

BOLETIN OFICIAL DE LA REPUBLICA ARGENTINA

Buenos Aires,
lunes 2
de septiembre de 2013

Año CXXI
Número 32.713

Precio \$ 3,00



Primera Sección Legislación y Avisos Oficiales

Los documentos que aparecen en el BOLETIN OFICIAL DE LA REPUBLICA ARGENTINA serán tenidos por auténticos y obligatorios por el efecto de esta publicación y por comunicados y suficientemente circulados dentro de todo el territorio nacional (Decreto N° 659/1947)

Sumario

DECRETOS

MINISTERIO DE DESARROLLO SOCIAL

Decreto 1236/2013
Designaciones en el Instituto Nacional de Asociativismo y Economía Social. 1

MINISTERIO DE ECONOMIA Y FINANZAS PUBLICAS

Decreto 1227/2013
Danse por prorrogadas designaciones en la Oficina Nacional de Crédito Público de la Subsecretaría de Financiamiento de la Secretaría de Finanzas. 2

Decreto 1225/2013

Danse por prorrogadas designaciones en la Subsecretaría de Presupuesto de la Secretaría de Hacienda. 3

MINISTERIO DE JUSTICIA Y DERECHOS HUMANOS

Decreto 1226/2013
Dase por prorrogada designación del Director de Administración de Recursos Humanos de la Dirección General de Recursos Humanos de la Subsecretaría de Coordinación. 3

Decreto 1232/2013

Dase por prorrogada designación en la Dirección de Planificación de Políticas de Transparencia de la Oficina Anticorrupción. 3

Decreto 1233/2013

Dase por prorrogada designación en la Subsecretaría de Coordinación y Control de Gestión Registral de la Secretaría de Asuntos Registrales. 4

MINISTERIO DE RELACIONES EXTERIORES Y CULTO

Decreto 1224/2013
Condecoración de la Orden de Mayo al Mérito. 4

MINISTERIO DE SALUD

Decreto 1237/2013
Dase por prorrogada designación de la Directora de Sumarios de la Secretaría de Coordinación. 4

MINISTERIO DE SEGURIDAD

Decreto 1234/2013
Dase por prorrogada designación. 4

MINISTERIO DE AGRICULTURA, GANADERIA Y PESCA

Decreto 1231/2013
Designación en la Dirección de Coordinación Federal de la Dirección Nacional de Coordinación Política de la Subsecretaría de Coordinación Política. 5

MINISTERIO DE TRABAJO, EMPLEO Y SEGURIDAD SOCIAL

Decreto 1235/2013
Designación en la Dirección de Programación Operativa de la Dirección Nacional de Fiscalización de la Subsecretaría de Fiscalización del Trabajo y de la Seguridad Social. 5

MINISTERIO DE AGRICULTURA, GANADERIA Y PESCA

Decreto 1230/2013
Inclúyese funcionaria dentro de las previsiones del Decreto N° 1.840/1986. 6

MINISTERIO DEL INTERIOR Y TRANSPORTE

Decreto 1221/2013
Dase por prorrogada designación en la Dirección Nacional de Migraciones. 6

Decreto 1222/2013

Danse por prorrogadas designaciones en la Agencia Nacional de Seguridad Vial. 7

Continúa en página 2

DECRETOS



MINISTERIO DE DESARROLLO SOCIAL

Decreto 1236/2013

Designaciones en el Instituto Nacional de Asociativismo y Economía Social.

Bs. As., 26/8/2013

VISTO el Expediente N° 15/2013, del registro del INSTITUTO NACIONAL DE ASOCIATIVISMO Y ECONOMIA SOCIAL, organismo descentralizado en la órbita del MINISTERIO DE DESARROLLO SOCIAL, la Ley N° 26.784, los Decretos N° 491 del 12 de marzo de 2002, N° 721 del 25 de agosto de 2000 y N° 2098 del 3 de diciembre de 2008, y

CONSIDERANDO:

Que por la citada Ley se aprobó el PRESUPUESTO DE LA ADMINISTRACION NACIONAL para el ejercicio 2013.

Que por el artículo 7° de la Ley N° 26.784 se dispuso el congelamiento de los cargos vacantes financiados existentes a la fecha de la sanción de la misma, en las Jurisdicciones y Entidades de la Administración Pública Nacional y de los que queden vacantes con posterioridad, salvo decisión fundada del Señor Jefe de Gabinete de Ministros o del PODER EJECUTIVO NACIONAL, en virtud de las disposiciones del artículo 10 de la citada Ley.

Que por el Decreto N° 491/02 se estableció, entre otros aspectos, que toda designación de personal en el ámbito de la Administración Pública Nacional centralizada y descentralizada, en cargos de planta permanente y no permanente, será efectuada por el PODER EJECUTIVO NACIONAL a propuesta de jurisdicción o entidad correspondiente.

Que mediante el Decreto N° 721/00 se aprobó la estructura organizativa del INSTITUTO NACIONAL DE ASOCIATIVISMO Y ECONOMIA SOCIAL organismo descentralizado en la órbita del MINISTERIO DE DESARROLLO SOCIAL.

Que por el Decreto N° 2098/08 se homologó el Convenio Colectivo de Trabajo Sectorial del Personal del Sistema Nacional de Empleo Público, el que rige a partir del 1° de diciembre de 2008.

Que mediante el Decreto N° 1567/09, fue designado transitoriamente en el cargo de Gerente de Intervenciones e Infracciones de la Secretaría de Contralor del INSTITUTO NACIONAL DE ASOCIATIVISMO Y ECONOMIA SOCIAL, organismo descentralizado en la órbita del MINISTERIO DE DESARROLLO SOCIAL, el Licenciado Adrián Gabriel BRIANZA (D.N.I. N° 25.544.816), cuya última prórroga fue efectuada por el Decreto N° 2078/12.

Que por el expediente citado en el Visto tramita la designación transitoria por el término de CIENTO OCHENTA (180) días hábiles, a partir del dictado del presente decreto, del mencionado funcionario, en el cargo de Gerente de Administración y Finanzas de la Secretaría de Registro Nacional de Cooperativas y Mutuales del referido Instituto Nacional, Nivel A, Grado 0, Función Ejecutiva Nivel III del Sistema Nacional de Empleo Público (SINEP), aprobado por el Convenio Colectivo de Trabajo Sectorial, homologado por el Decreto N° 2098/08, a cuyo efecto presenta su renuncia al cargo aludido en el considerando anterior, con el objeto de posibilitar la designación propuesta, para la que reúne los requisitos de experiencia e idoneidad necesarios para su desempeño.

Que asimismo resulta imprescindible proceder a la cobertura del cargo de Gerente de Intervenciones e Infracciones de la Secretaría de Contralor, Nivel A, Grado 0, Función Ejecutiva Nivel III, del mencionado Sistema Nacional, por el término de CIENTO OCHENTA (180) días hábiles, contados a partir del dictado del presente decreto, a fin de asegurar el normal desenvolvimiento operativo del citado Instituto Nacional.

Que el Licenciado Ezequiel Luis BORGOGNO (DNI N° 30.531.488), reúne los requisitos de experiencia e idoneidad, necesarios para el desempeño de dicho cargo.

Que tales requerimientos implican resolver las coberturas de los respectivos cargos como excepción a lo dispuesto en el artículo 7° de la Ley N° 26.784, y a las pautas generales de selección para el acceso a las funciones de que se trata, con autorización excepcional por no reunir los requisitos mínimos establecidos en el artículo 14 y a lo establecido, respectivamente, en

PRESIDENCIA DE LA NACION

SECRETARIA LEGAL Y TECNICA
DR. CARLOS ALBERTO ZANNINI
Secretario

DIRECCION NACIONAL DEL REGISTRO OFICIAL
DR. JORGE EDUARDO FEIJOÓ
Director Nacional

www.boletinoficial.gob.ar

e-mail: dnro@boletinoficial.gob.ar

Registro Nacional de la Propiedad Intelectual
N° 4.995.241

DOMICILIO LEGAL
Suipacha 767-C1008AAO
Ciudad Autónoma de Buenos Aires
Tel. y Fax 5218-8400 y líneas rotativas

DECISIONES ADMINISTRATIVAS

MINISTERIO DE AGRICULTURA, GANADERIA Y PESCA

Decisión Administrativa 648/2013

Contratación..... 7

Decisión Administrativa 649/2013

Contratación en la Subsecretaría de Pesca y Acuicultura de la Secretaría de Agricultura, Ganadería y Pesca..... 8

Decisión Administrativa 652/2013

Contratación en la Subsecretaría de Coordinación Técnica y Administrativa..... 8

MINISTERIO DE JUSTICIA Y DERECHOS HUMANOS

Decisión Administrativa 653/2013

Facúltase al Ministro de Justicia y Derechos Humanos a aprobar cargos de Conducción..... 9

MINISTERIO DEL INTERIOR Y TRANSPORTE

Decisión Administrativa 651/2013

Contrataciones en la Agencia Nacional de Seguridad Vial..... 9

RESOLUCIONES

ADUANAS

Resolución General 3524-AFIP

Premio a la Innovación Aduanera - "Cadenas logísticas mundiales eficientes, seguras, transparentes y resistentes". Su implementación..... 10

EXPORTACIONES

Resolución General 3523-AFIP

Cueros y pieles en bruto de la Partida 41.01 del Sistema Armonizado de Designación y Codificación de Mercancías. Aduanas especializadas..... 11

DISPOSICIONES

ADMINISTRACION PUBLICA NACIONAL

Disposición 3/2013-ONTI

Apruébase la "Política de Seguridad de la Información Modelo"..... 12

AVISOS OFICIALES

Nuevos..... 47

Anteriores..... 69

CONVENCIONES COLECTIVAS DE TRABAJO

Pág.

7

8

8

9

9

10

11

12

47

69

69

TA (180) días hábiles, contados a partir del dictado del presente, al Licenciado Adrián Gabriel BRIANZA (D.N.I. N° 25.544.816), en el cargo de Gerente de Administración y Finanzas de la Secretaría de Registro Nacional de Cooperativas y Mutuales, Nivel A, Grado 0, autorizándose el correspondiente pago de la Función Ejecutiva Nivel III del Sistema Nacional de Empleo Público (SINEP), aprobado por el Convenio Colectivo de Trabajo Sectorial homologado por el Decreto N° 2098/08, perteneciente al INSTITUTO NACIONAL DE ASOCIATIVISMO Y ECONOMIA SOCIAL, organismo descentralizado en la órbita del MINISTERIO DE DESARROLLO SOCIAL, con autorización excepcional por no reunir los requisitos mínimos establecidos en el artículo 14 del citado Convenio y con carácter de excepción a lo dispuesto por el artículo 7° de la Ley N° 26.784.

Art. 3° — Designase con carácter transitorio, por el término de CIENTO OCHENTA (180) días hábiles, contados a partir del dictado del presente, al Licenciado Ezequiel Luis BORGOGNO (DNI 30.531.488), en el cargo de Gerente de Intervenciones e Infracciones de la Secretaría de Contralor, Nivel A, Grado 0, autorizándose el correspondiente pago de la Función Ejecutiva Nivel III del Sistema Nacional de Empleo Público (SINEP), aprobado por el Convenio Colectivo de Trabajo Sectorial homologado por el Decreto N° 2098/08, perteneciente al INSTITUTO NACIONAL DE ASOCIATIVISMO Y ECONOMIA SOCIAL, organismo descentralizado en la órbita del MINISTERIO DE DESARROLLO SOCIAL, con autorización excepcional por no reunir los requisitos mínimos establecidos en el artículo 14 del citado Convenio y con carácter de excepción a lo dispuesto por el artículo 7° de la Ley N° 26.784.

Art. 4° — Los cargos involucrados en los artículos 2° y 3° de la presente medida, deberán ser cubiertos conforme los sistemas de selección vigentes y requisitos según lo establecido, respectivamente, en los Títulos II, Capítulos III, IV y VIII y IV del Convenio Colectivo de Trabajo Sectorial del Personal del Sistema Nacional de Empleo Público, homologado por el Decreto N° 2098/08, dentro del plazo de CIENTO OCHENTA (180) días hábiles contados a partir de la fecha del presente Decreto.

Art. 5° — El gasto que demande el cumplimiento de la presente medida será atendido con cargo a las partidas específicas del presupuesto del INSTITUTO NACIONAL DE ASOCIATIVISMO Y ECONOMIA SOCIAL - Entidad 114.

Art. 6° — Comuníquese, publíquese, dese a la Dirección Nacional del Registro Oficial y archívese. — FERNANDEZ DE KIRCHNER. — Juan M. Abal Medina. — Alicia M. Kirchner.

NOMIA Y FINANZAS PUBLICAS, prorrogándose dichas designaciones en último término mediante el Decreto N° 1.560 de fecha 3 de octubre de 2011.

Que razones operativas hacen necesario prorrogar las designaciones transitorias citadas en el primer considerando de la presente medida.

Que el Licenciado en Economía Don Paulo Enrico FARINA (M.I. N° 25.430.610) se desempeñó en el cargo de Coordinador de Estudios del Mercado Interno, hasta el 12 de septiembre de 2012, atento que a partir del 13 de septiembre de 2012 presentó su renuncia, y la Licenciada en Economía Doña Mariel Elizabeth CORETTI (M.I. N° 23.942.576) se desempeñó en el cargo de Director de Informaciones Financieras hasta el 28 de febrero de 2012, teniendo en cuenta que a partir del 29 de febrero de 2012 por la Resolución N° 33 de fecha 12 de abril de 2012 de la SECRETARIA DE FINANZAS DEL MINISTERIO DE ECONOMIA Y FINANZAS PUBLICAS, se le aceptó la renuncia a dicho cargo.

Que la Dirección General de Asuntos Jurídicos del MINISTERIO DE ECONOMIA Y FINANZAS PUBLICAS ha tomado la intervención que le compete.

Que la presente medida se dicta en virtud de las facultades conferidas por el Artículo 99, inciso 1 de la CONSTITUCION NACIONAL, y por el Artículo 1° del Decreto N° 491 de fecha 12 de marzo de 2002.

Por ello,

LA PRESIDENTA
DE LA NACION ARGENTINA
DECRETA:

Artículo 1° — Dase por prorrogada la designación transitoria, del Licenciado en Economía Don Paulo Enrico FARINA (M.I. N° 25.430.610), en el cargo de Coordinador de Estudios, del Mercado Interno de la OFICINA NACIONAL DE CREDITO PUBLICO de la SUBSECRETARIA DE FINANCIAMIENTO de la SECRETARIA DE FINANZAS del MINISTERIO DE ECONOMIA Y FINANZAS PUBLICAS, Nivel B, autorizándose el correspondiente pago del Suplemento por Función Ejecutiva Nivel III del SISTEMA NACIONAL DE EMPLEO PUBLICO (SI.N.E.P.), aprobado por el Convenio Colectivo de Trabajo Sectorial homologado por el Decreto N° 2.098 de fecha 3 de diciembre de 2008, por el término de CIENTO OCHENTA (180) días hábiles contados a partir del vencimiento establecido en el Artículo 1° del Decreto N° 1.560 de fecha 3 de octubre de 2011 y hasta el 12 de septiembre de 2012.

Art. 2° — Dase por prorrogada la designación transitoria, de la Licenciada en Economía Doña Mariel Elizabeth CORETTI (M.I. N° 23.942.576), en el cargo de Director de Informaciones Financieras de la OFICINA NACIONAL DE CREDITO PUBLICO de la SUBSECRETARIA DE FINANCIAMIENTO de la SECRETARIA DE FINANZAS del MINISTERIO DE ECONOMIA Y FINANZAS PUBLICAS, Nivel B, autorizándose el correspondiente pago del Suplemento por Función Ejecutiva Nivel III del SISTEMA NACIONAL DE EMPLEO PUBLICO (SI.N.E.P.), aprobado por el Convenio Colectivo de Trabajo Sectorial homologado por el Decreto N° 2.098 de fecha 3 de diciembre de 2008, a partir del vencimiento establecido en el Artículo 1° del Decreto N° 1.560 de fecha 3 de octubre de 2011 y hasta el 28 de febrero de 2012.

Art. 3° — El gasto que demandó el cumplimiento del presente decreto se atendió con cargo a las partidas específicas de la Jurisdicción 50 - MINISTERIO DE ECONOMIA Y FINANZAS PUBLICAS.

Art. 4° — Comuníquese, publíquese, dese a la Dirección Nacional del Registro Oficial y archívese. — FERNANDEZ DE KIRCHNER. — Juan M. Abal Medina. — Hernán G. Lorenzino.

los Títulos II, Capítulos III, IV y VIII y IV del Convenio Colectivo de Trabajo Sectorial del Personal del Sistema Nacional de Empleo Público, homologado por el Decreto N° 2098/08.

Que a dichos efectos, resulta procedente aceptar la renuncia presentada por el Lic. Adrián Gabriel BRIANZA, al cargo de Gerente de Intervenciones e Infracciones de la Secretaría de Contralor, y efectuar las designaciones correspondientes a fin de proceder a la cobertura transitoria de los mencionados cargos.

Que los cargos aludidos no constituyen asignación de recurso extraordinario alguno.

Que la Dirección General de Asuntos Jurídicos del MINISTERIO DE DESARROLLO SOCIAL ha tomado la intervención que le compete.

Que la presente medida se dicta en virtud de las atribuciones emergentes del artículo 99, inciso 1° de la CONSTITUCION

NACIONAL y de los artículos 7° y 10 de la Ley N° 26.784 y del artículo 1° del Decreto N° 491/02.

Por ello,

LA PRESIDENTA
DE LA NACION ARGENTINA
DECRETA:

Artículo 1° — Acéptase, a partir de la fecha del presente decreto, la renuncia presentada por el Licenciado Adrián Gabriel BRIANZA (D.N.I. N° 25.544.816) al cargo de Gerente de Intervenciones e Infracciones de la Secretaría de Contralor, Nivel A, Grado 0 Función Ejecutiva Nivel III, en el que fuera designado mediante el Decreto N° 1567/09, cuya última prórroga fue efectuada por el Decreto N° 2078/12, perteneciente al INSTITUTO NACIONAL DE ASOCIATIVISMO Y ECONOMIA SOCIAL, organismo descentralizado en la órbita del MINISTERIO DE DESARROLLO SOCIAL.

Art. 2° — Designase con carácter transitorio, por el término de CIENTO OCHEN-

MINISTERIO DE ECONOMIA Y FINANZAS PUBLICAS

Decreto 1227/2013

Danse por prorrogadas designaciones en la Oficina Nacional de Crédito Público de la Subsecretaría de Financiamiento de la Secretaría de Finanzas.

Bs. As., 26/8/2013

VISTO el Expediente N° S01:0454940/2011 del Registro del MINISTERIO DE ECONOMIA Y FINANZAS PUBLICAS, y

CONSIDERANDO:

Que mediante el Decreto N° 645 de fecha 10 de mayo de 2010, se designaron con carácter transitorio, a diversos profesionales en cargos vacantes de la SUBSECRETARIA DE FINANCIAMIENTO dependiente de la SECRETARIA DE FINANZAS del MINISTERIO DE ECO-

MINISTERIO DE ECONOMIA Y FINANZAS PUBLICAS**Decreto 1225/2013**

Danse por prorrogadas designaciones en la Subsecretaría de Presupuesto de la Secretaría de Hacienda.

Bs. As., 26/8/2013

VISTO el Expediente N° S01:0418651/2012 del Registro del MINISTERIO DE ECONOMIA Y FINANZAS PUBLICAS, y

CONSIDERANDO:

Que mediante los Decretos Nros. 1.306 de fecha 28 de septiembre de 2006, 259 de fecha 7 de abril de 2009, 659 de fecha 28 de mayo de 2009 y 1.517 de fecha 20 de octubre de 2009, se dispusieron las designaciones transitorias en cargos con Funciones Ejecutivas en el ámbito de la SUBSECRETARIA DE PRESUPUESTO dependiente de la SECRETARIA DE HACIENDA del MINISTERIO DE ECONOMIA Y FINANZAS PUBLICAS y se prorrogaron en último término por el Decreto N° 1.429 de fecha 14 de agosto de 2012.

Que encontrándose cumplido el plazo de CIENTO OCHENTA (180) días hábiles y no habiéndose efectuado la correspondiente convocatoria, conforme el proceso de selección previsto en el SISTEMA NACIONAL DE EMPLEO PUBLICO (S.I.N.E.P.), homologado por el Decreto N° 2.098 de fecha 3 de diciembre de 2008, razones operativas hacen necesario prorrogar dichas designaciones transitorias.

Que los profesionales a los que se hace referencia en el presente decreto se encuentran actualmente desempeñándose en los cargos en que fueron designados transitoriamente.

Que la Dirección General de Asuntos Jurídicos del MINISTERIO DE ECONOMIA Y FINANZAS PUBLICAS ha tomado la intervención que le compete.

Que la presente medida se dicta en virtud de las facultades conferidas por el Artículo 99, inciso 1 de la CONSTITUCION NACIONAL y el Artículo 1° del Decreto N° 491 de fecha 12 de marzo de 2002.

Por ello,

LA PRESIDENTA
DE LA NACION ARGENTINA
DECRETA:

Artículo 1° — Danse por prorrogadas las designaciones transitorias de los funcionarios que se designan en el Anexo que forma parte integrante de la presente medida, efectuadas por conducto de los Decretos Nros. 1.306 de fecha 28 de septiembre de 2006, 259 de fecha 7 de abril de 2009, 659 de fecha 28 de mayo de 2009 y 1.517 de fecha 20 de octubre de 2009, por el término de CIENTO OCHENTA (180) días hábiles contados a partir del vencimiento establecido en el Artículo 1° del Decreto N° 1.429 de fecha 14 de agosto de 2012, que se produjo el 15 de noviembre de 2012, pertenecientes a la SUBSECRETARIA DE PRESUPUESTO dependiente de la SECRETARIA DE HACIENDA del MINISTERIO DE ECONOMIA Y FINANZAS PUBLICAS, autorizándose el correspondiente pago del Suplemento por Función Ejecutiva del SISTEMA NACIONAL DE EMPLEO PUBLICO (S.I.N.E.P.), aprobado por el Convenio Colectivo de Trabajo Sectorial homologado por el Decreto N° 2.098 de fecha 3 de diciembre de 2008.

Art. 2° — Los cargos involucrados deberán ser cubiertos conforme los requisitos y sistemas de selección vigentes según lo establecido, respectivamente, en los Títulos II, Capítulos III, IV y VIII, y IV del SISTEMA NACIONAL DE EMPLEO PUBLICO (S.I.N.E.P.), dentro del plazo de CIENTO OCHENTA (180) días hábiles contados a partir del 15 de noviembre de 2012.

Art. 3° — El gasto que demande el cumplimiento del presente decreto se atenderá con cargo a las partidas específicas de la Jurisdicción 50 - MINISTERIO DE ECONOMIA Y FINANZAS PUBLICAS.

Art. 4° — Comuníquese, publíquese, dése a la Dirección Nacional del Registro Oficial y archívese. — FERNANDEZ DE KIRCHNER. — Juan M. Abal Medina. — Hernán G. Lorenzino.

ANEXO

MINISTERIO DE ECONOMIA Y FINANZAS PUBLICAS

SECRETARIA DE HACIENDA

SUBSECRETARIA DE PRESUPUESTO

APELLIDO Y NOMBRES	M.I. N°	NIVEL S.I.N.E.P.	NIVEL F.E.	CARGO
CANDAL, María Gabriela	20.410.440	A	II	Coordinador General de Actividades de Capacitación en Materia de Administración Financiera

OFICINA NACIONAL DE PRESUPUESTO

APELLIDO Y NOMBRES	M.I. N°	NIVEL S.I.N.E.P.	NIVEL F.E.	CARGO
RAJUAN, Luis Clemente	16.497.477	A	II	Subdirector de la Oficina Nacional de Presupuesto

CONTADURIA GENERAL DE LA NACION

APELLIDO Y NOMBRES	M.I. N°	NIVEL S.I.N.E.P.	NIVEL F.E.	CARGO
GENOVESI, Verónica Rosana	23.100.688	C	IV	Coordinador de Auditoría de Sistemas Administrativos Contables

TESORERIA GENERAL DE LA NACION

APELLIDO Y NOMBRES	M.I. N°	NIVEL S.I.N.E.P.	NIVEL F.E.	CARGO
LEMUS, Miriam Noemí	14.927.814	B	IV	Coordinador de Normas y Supervisión Tesorerías Jurisdiccionales

MINISTERIO DE JUSTICIA Y DERECHOS HUMANOS**Decreto 1226/2013**

Dase por prorrogada designación del Director de Administración de Recursos Humanos de la Dirección General de Coordinación.

Bs. As., 26/8/2013

VISTO el Expediente N° S04:0004560/2011 del registro del MINISTERIO DE JUSTICIA Y DERECHOS HUMANOS, los Decretos Nros. 491 del 12 de marzo de 2002, 2098 del 3 de diciembre de 2008, 1770 del 16 de noviembre de 2009, 1318 del 14 de septiembre de 2010, 666 del 26 de mayo de 2011, 268 del 23 de febrero de 2012 y 1989 del 19 de octubre de 2012, y

CONSIDERANDO:

Que por el Decreto N° 1770/09, prorrogado por sus similares Nros. 1318/10, 666/11, 268/12 y 1989/12, se designó transitoriamente al contador público Pablo Ariel VICENTE (D.N.I. N° 21.897.586), en un cargo Nivel B - Grado 0 del Convenio Colectivo de Trabajo Sectorial del personal del SISTEMA NACIONAL DE EMPLEO PUBLICO (SINEP), homologado por el Decreto N° 2098/08, de la planta permanente de la DIRECCION GENERAL DE RECURSOS HUMANOS dependiente de la SUBSECRETARIA DE COORDINACION del MINISTERIO DE JUSTICIA Y DERECHOS HUMANOS, para cumplir funciones de Director de Administración de Recursos Humanos —Función Ejecutiva de Nivel II—.

Que por razones de índole operativa no se ha podido tramitar el proceso de selección para la cobertura del cargo en cuestión, motivo por el cual el citado Ministerio solicita una nueva prórroga de la designación transitoria aludida.

Que a los efectos de implementar la prórroga de la designación transitoria del contador público Pablo Ariel VICENTE, resulta necesario disponer la cobertura del cargo con carácter de excepción a los requisitos mínimos de acceso al Nivel B establecidos en el artículo 14 del Convenio Colectivo de Trabajo Sectorial del personal del SISTEMA NACIONAL DE EMPLEO PUBLICO (SINEP), homologado por el Decreto N° 2098/08.

Que la presente medida tiene por objeto asegurar el cumplimiento de los objetivos asignados a la citada Dirección General.

Que la cobertura del cargo en cuestión no constituye asignación de recurso extraordinario alguno toda vez que se cuenta con el crédito necesario en el presupuesto del MINISTERIO DE JUSTICIA Y DERECHOS HUMANOS para atender el gasto resultante de la medida que se aprueba por el presente.

Que ha tomado intervención el servicio permanente de asesoramiento jurídico del citado Ministerio.

Que la presente medida se dicta en virtud de las atribuciones emergentes del artículo 99, inciso 1 de la CONSTITUCION NACIONAL y del artículo 1° del Decreto N° 491/02.

Por ello,

LA PRESIDENTA
DE LA NACION ARGENTINA
DECRETA:

Artículo 1° — Dase por prorrogada, a partir del 26 de marzo de 2013 —fecha de su vencimiento— y por el término de CIENTO OCHENTA (180) días hábiles, la designación transitoria del contador público Pablo Ariel VICENTE (D.N.I. N° 21.897.586), dispuesta por conducto del Decreto N° 1770/09, prorrogado por sus similares Nros. 1318/10, 666/11, 268/12 y 1989/12, en un cargo Nivel B - Grado 0 del Convenio Colectivo de Trabajo Sectorial del personal del SISTEMA NACIONAL DE EMPLEO PUBLICO (SINEP), homologado por el Decreto N° 2098/08, de la

planta permanente de la DIRECCION GENERAL DE RECURSOS HUMANOS dependiente de la SUBSECRETARIA DE COORDINACION del MINISTERIO DE JUSTICIA Y DERECHOS HUMANOS, para cumplir funciones de Director de Administración de Recursos Humanos, autorizándose el correspondiente pago de la Función Ejecutiva de Nivel II del Convenio Colectivo de Trabajo Sectorial del personal del SISTEMA NACIONAL DE EMPLEO PUBLICO (SINEP), homologado por el Decreto N° 2098/08, con carácter de excepción a los requisitos mínimos de acceso al Nivel B establecidos en el artículo 14 del citado Convenio.

Art. 2° — El cargo involucrado en este acto deberá ser cubierto conforme los requisitos y sistemas de selección vigentes, según lo establecido, respectivamente, en los Títulos II, Capítulos III, IV y VIII, y IV del Convenio Colectivo de Trabajo Sectorial del personal del SISTEMA NACIONAL DE EMPLEO PUBLICO (SINEP), homologado por Decreto N° 2098/08, dentro del plazo de CIENTO OCHENTA (180) días hábiles contados a partir del 26 de marzo de 2013.

Art. 3° — El gasto que demande el cumplimiento de la presente medida será atendido con los créditos asignados a la Jurisdicción 40 - MINISTERIO DE JUSTICIA Y DERECHOS HUMANOS.

Art. 4° — Comuníquese, publíquese, dése a la Dirección Nacional del Registro Oficial y archívese. — FERNANDEZ DE KIRCHNER. — Juan M. Abal Medina. — Julio C. Alak.

MINISTERIO DE JUSTICIA Y DERECHOS HUMANOS**Decreto 1232/2013**

Dase por prorrogada designación en la Dirección de Planificación de Políticas de Transparencia de la Oficina Anticorrupción.

Bs. As., 26/8/2013

VISTO el Expediente N° S04:0013388/2011 del registro del MINISTERIO DE JUSTICIA Y DERECHOS HUMANOS, los Decretos Nros. 491 del 12 de marzo de 2002, 2098 del 3 de diciembre de 2008, 2106 del 4 de diciembre de 2008, 749 del 17 de junio de 2009, 2178 del 28 de diciembre de 2009, 1838 del 30 de noviembre de 2010, 882 del 30 de junio de 2011 y 1101 del 5 de julio de 2012, y

CONSIDERANDO:

Que por el Decreto N° 2106/08, prorrogado por sus similares Nros. 749/09, 2178/09, 1838/10, 882/11 y 1101/12, se efectuó la designación transitoria de doctora Laura GELER, en un cargo Nivel B - Grado 0 de la planta permanente de la DIRECCION DE PLANIFICACION DE POLITICAS DE TRANSPARENCIA dependiente de la OFICINA ANTICORRUPCION del MINISTERIO DE JUSTICIA Y DERECHOS HUMANOS, para cumplir funciones de Analista Principal.

Que por razones de índole operativa no se ha podido tramitar el proceso de selección para la cobertura del cargo en cuestión, razón por la cual el MINISTERIO DE JUSTICIA Y DERECHOS HUMANOS solicita una nueva prórroga de la designación transitoria.

Que la presente medida tiene por objeto asegurar el cumplimiento de los objetivos asignados a la DIRECCION DE PLANIFICACION DE POLITICAS DE TRANSPARENCIA dependiente de la OFICINA ANTICORRUPCION del citado Ministerio.

Que se cuenta con el crédito necesario en el presupuesto del MINISTERIO DE JUSTICIA Y DERECHOS HUMANOS para atender el gasto resultante de la medida que se aprueba por el presente.

Que ha tomado intervención el servicio de asesoramiento jurídico del MINISTERIO DE JUSTICIA Y DERECHOS HUMANOS.

Que la presente medida se dicta en virtud de las atribuciones emergentes del artículo 99, inciso 1 de la CONSTITUCION NACIONAL y del artículo 1° del Decreto N° 491/02.

Por ello,

LA PRESIDENTA
DE LA NACION ARGENTINA
DECRETA:

Artículo 1° — Dase por prorrogada a partir del 21 de marzo de 2013 —fecha de su vencimiento— y por el término de CIENTO OCHENTA (180) días hábiles, la designación transitoria de la doctora Laura GELER (D.N.I. N° 26.281.641), en un cargo Nivel B - Grado 0 del Convenio Colectivo de Trabajo Sectorial del personal del SISTEMA NACIONAL DE EMPLEO PUBLICO (SINEP), homologado por el Decreto N° 2098/08, de la planta permanente de la DIRECCION DE PLANIFICACION DE POLITICAS DE TRANSPARENCIA dependiente de la OFICINA ANTICORRUPCION del MINISTERIO DE JUSTICIA Y DERECHOS HUMANOS efectuada por conducto del Decreto N° 2106/08, prorrogada por sus similares Nros. 749/09, 2178/09, 1838/10, 882/11 y 1101/12, para cumplir funciones de Analista Principal.

Art. 2° — El cargo involucrado en este acto deberá ser cubierto de conformidad con los requisitos y sistemas de selección vigentes, según lo establecido, respectivamente, en los Títulos II, Capítulos III y IV, y IV del Convenio Colectivo de Trabajo Sectorial del personal del SISTEMA NACIONAL DE EMPLEO PUBLICO, homologado por el Decreto N° 2098/08, dentro del plazo de CIENTO OCHENTA (180) días hábiles contados a partir del 21 de marzo de 2013.

Art. 3° — El gasto que demande el cumplimiento de este acto será atendido con cargo a las partidas específicas del presupuesto de la Jurisdicción 40 MINISTERIO DE JUSTICIA Y DERECHOS HUMANOS.

Art. 4° — Comuníquese, publíquese, dese a la Dirección Nacional del Registro Oficial y archívese. — FERNANDEZ DE KIRCHNER. — Juan M. Abal Medina. — Julio C. Alak.

MINISTERIO DE JUSTICIA Y DERECHOS HUMANOS

Decreto 1233/2013

Dase por prorrogada designación en la Subsecretaría de Coordinación y Control de Gestión Registral de la Secretaría de Asuntos Registrales.

Bs. As., 26/8/2013

VISTO el Expediente N° S04:0050949/2011 del registro del MINISTERIO DE JUSTICIA Y DERECHOS HUMANOS, los Decretos Nros. 491 del 12 de marzo de 2002, 2098 del 3 de diciembre de 2008 y 1170 del 13 de julio de 2012, y

CONSIDERANDO:

Que por el Decreto N° 1170/12 se designó transitoriamente a la señora Catalina DIVASTO (D.N.I. N° 34.323.761), en un cargo Nivel D - Grado 0 del Convenio Colectivo de Trabajo Sectorial del Personal del SISTEMA NACIONAL DE EMPLEO PUBLICO (SINEP) homologado por el Decreto N° 2098/08 de la planta permanente de la SUBSECRETARIA DE COORDINACION Y CONTROL DE GESTION REGISTRAL de la SECRETARIA DE ASUNTOS REGISTRALES del MINISTERIO DE JUSTICIA Y DERECHOS HUMANOS, para cumplir funciones de Secretaria - Asistente Administrativa.

Que por razones de índole operativa no se ha podido tramitar el proceso de selección para la cobertura del cargo en cuestión, razón por la cual el citado Ministerio solicita la prórroga de la designación transitoria aludida.

Que la presente medida tiene por objeto asegurar el cumplimiento de los objetivos asignados a la mencionada Subsecretaría.

Que ha tomado intervención el servicio permanente de asesoramiento jurídico del MINISTERIO DE JUSTICIA Y DERECHOS HUMANOS.

Que la presente, medida se dicta en virtud de las atribuciones emergentes del artículo 99, inciso 1 de la CONSTITUCION NACIONAL y del artículo 1° del Decreto N° 491/02.

Por ello,

LA PRESIDENTA
DE LA NACION ARGENTINA
DECRETA:

Artículo 1° — Dase por prorrogada, a partir del 28 de marzo de 2013 —fecha de su vencimiento— y por el término de CIENTO OCHENTA (180) días hábiles, la designación transitoria dispuesta por conducto del Decreto N° 1170/12, de la señora Catalina DIVASTO (D.N.I. N° 34.323.761), en un cargo Nivel D - Grado 0 del Convenio Colectivo de Trabajo Sectorial del personal del SISTEMA NACIONAL DE EMPLEO PUBLICO (SINEP) homologado por el Decreto N° 2098/08 de la planta permanente de la SUBSECRETARIA DE COORDINACION Y CONTROL DE GESTION REGISTRAL de la SECRETARIA DE ASUNTOS REGISTRALES del MINISTERIO DE JUSTICIA Y DERECHOS HUMANOS, para cumplir funciones de Secretaria - Asistente Administrativa.

Art. 2° — El cargo involucrado en la presente medida deberá ser cubierto de conformidad con los requisitos y sistemas de selección vigentes, según lo establecido, respectivamente, en los Títulos II, Capítulos III y IV, y IV del Convenio Colectivo de Trabajo Sectorial del personal del SISTEMA NACIONAL DE EMPLEO PUBLICO (SINEP), homologado por el Decreto N° 2098/08, dentro del plazo de CIENTO OCHENTA (180) días hábiles contados a partir del 28 de marzo de 2013.

Art. 3° — El gasto que demande el cumplimiento del presente será atendido con los créditos asignados a la Jurisdicción 40 - MINISTERIO DE JUSTICIA Y DERECHOS HUMANOS.

Art. 4° — Comuníquese, publíquese, dese a la Dirección Nacional del Registro Oficial y archívese. — FERNANDEZ DE KIRCHNER. — Juan M. Abal Medina. — Julio C. Alak.

MINISTERIO DE RELACIONES EXTERIORES Y CULTO

Decreto 1224/2013

Condecoración de la Orden de Mayo al Mérito.

Bs. As., 26/8/2013

VISTO lo establecido por el Decreto Ley N° 16.629 de fecha 17 de diciembre de 1957, ratificado por la Ley N° 14.467, por el que se creó la ORDEN DE MAYO, y

CONSIDERANDO:

Que el Consejo de la Orden ha prestado acuerdo a la propuesta de la señora Embajadora de la República en la REPUBLICA DE EL SALVADOR de condecorar a los señores D. Pedro Angel CALDERON, D. Oscar Antonio MARTINEZ CALDERON y D. Daniel VAZQUEZ QUINTANILLA, empleados locales de la Embajada de la República en la REPUBLICA DE EL SALVADOR, quienes han prestado allí funciones durante VEINTICINCO (25) años, con dedicación, esmero, confiabilidad y lealtad a la República, por lo que se han hecho acreedores al honor y reconocimiento de la Nación.

Que compete al PODER EJECUTIVO NACIONAL dictar la medida aprobatoria complementaria prevista en el Artículo 6° del Decreto Ley N° 16.629 de fecha 17 de diciembre de 1957, ratificado por Ley N° 14.467.

Por ello,

LA PRESIDENTA
DE LA NACION ARGENTINA
DECRETA:

Artículo 1° — Apruébase el Acta del Consejo de la ORDEN DE MAYO, suscripta el 4 de julio de 2013, mediante la cual se acuerda la condecoración de la ORDEN DE MAYO AL MERITO, en el grado de CABALLERO, a los señores D. Pedro Angel CALDERON, D. Oscar Antonio MARTINEZ CALDERON y D. Daniel VAZQUEZ QUINTANILLA, empleados locales de la Embajada de la República en la REPUBLICA DE EL SALVADOR.

Art. 2° — Extiéndanse los correspondientes diplomas, de acuerdo con lo estipulado por el Artículo 19 de la Reglamentación de la ORDEN DE MAYO, aprobada por el Decreto N° 16.644 de fecha 18 de diciembre de 1957 y conforme a lo dispuesto en el Artículo 1° del Decreto N° 220 de fecha 8 de febrero de 2010.

Art. 3° — Comuníquese, publíquese, dese a la Dirección Nacional del Registro Oficial y archívese. — FERNANDEZ DE KIRCHNER. — Héctor M. Timerman.

MINISTERIO DE SALUD

Decreto 1237/2013

Dase por prorrogada designación de la Directora de Sumarios de la Secretaría de Coordinación.

Bs. As., 26/8/2013

VISTO los Decretos Nros. 828 del 10 de abril de 2003, 441 del 6 de abril de 2004, 300 del 8 de abril de 2005, 1650 del 27 de diciembre de 2005, 456 del 18 de abril de 2006, 1985 del 28 de diciembre de 2006, 1341 del 4 de octubre de 2007, 2005 del 24 de noviembre de 2008, 1642 del 2 de noviembre de 2009, 491 del 12 de marzo de 2002, 2098 del 3 de diciembre de 2008, 1830 del 29 de noviembre de 2010, 487 del 25 de abril de 2011, 2017 del 5 de diciembre de 2011, 789 del 23 de mayo de 2012 y 2797 del 28 de diciembre de 2012, lo propuesto por el MINISTERIO DE SALUD y el Expediente N° 1-2002-1454/03-1 del registro del citado Ministerio, y

CONSIDERANDO:

Que por el Decreto N° 491/02 el PODER EJECUTIVO NACIONAL, reasumió el control directo de todas las designaciones de personal, en el ámbito de la Administración Pública Nacional, en los cargos de planta permanente y no permanente.

Que por el Decreto N° 828/03 se designó con carácter transitorio por el término de CIENTO OCHENTA (180) días hábiles, como Directora de Sumarios dependiente de la ex SUBSECRETARIA DE COORDINACION del MINISTERIO DE SALUD, Nivel B - Grado 8, Función Ejecutiva de Nivel III, a la doctora Da. Susana Graciela SOUZA ALEXANDRE (D.N.I. N° 6.044.408).

Que el plazo precedentemente señalado fue prorrogado sucesivamente y por igual término por los Decretos Nros. 441/04, 300/05, 1650/05, 456/06, 1985/06, 1341/07, 2005/08 1642/09, 1830/10, 487/11, 2017/11, 789/12 y 2797/12 y se encuentra actualmente vencido.

Que el procedimiento de selección correspondiente no se ha instrumentado hasta el presente y no resulta factible concretarlo en lo inmediato, motivo por el cual, teniendo en cuenta la naturaleza del cargo involucrado y a efectos de contribuir al normal cumplimiento de las acciones que tiene asignadas la Dirección de Sumarios, resulta necesario disponer la prórroga por igual período del plazo precedentemente señalado.

Que la DIRECCION GENERAL DE ASUNTOS JURIDICOS del MINISTERIO DE SALUD ha tomado la intervención de su competencia.

Que la presente medida se dicta en uso de las facultades conferidas por el artículo 99, inciso 1°) de la CONSTITUCION NACIONAL y el Decreto N° 491/02, artículo 1°.

Por ello,

LA PRESIDENTA
DE LA NACION ARGENTINA
DECRETA:

Artículo 1° — Dase por prorrogada a partir del 5 de junio de 2013 y por el término de CIENTO OCHENTA (180) días hábiles, la designación transitoria efectuada en los términos del Decreto N° 828/03 y cuya última prórroga operó por el Decreto N° 2797/12 de la doctora Da. Susana Graciela SOUZA ALEXANDRE (D.N.I. N° 6.044.408), Nivel B - Grado 8, en el cargo de Directora de Sumarios dependiente de la SECRETARIA DE COORDINACION del MINISTERIO DE SALUD, autorizándose el correspondiente pago de la Función Ejecutiva de Nivel III del CONVENIO COLECTIVO DE TRABAJO SECTORIAL DEL PERSONAL DEL SISTEMA NACIONAL DE EMPLEO PUBLICO (SINEP), homologado por el Decreto N° 2098/08.

Art. 2° — El cargo involucrado en el artículo 1° deberá ser cubierto conforme los requisitos y sistemas de selección vigentes según lo establecido, respectivamente, en los Títulos II —Capítulos III, IV y VIII— y IV del CONVENIO COLECTIVO DE TRABAJO SECTORIAL DEL PERSONAL DEL SISTEMA NACIONAL DE EMPLEO PUBLICO homologado por Decreto N° 2098/08, dentro del plazo de CIENTO OCHENTA (180) días hábiles contados a partir de la fecha mencionada en el artículo 1° del presente Decreto.

Art. 3° — El gasto que demande el cumplimiento de la presente medida será atendido con cargo a las partidas específicas del presupuesto vigente de la jurisdicción 80 - del MINISTERIO DE SALUD.

Art. 4° — Comuníquese, publíquese, dese a la DIRECCION NACIONAL DEL REGISTRO OFICIAL y archívese. — FERNANDEZ DE KIRCHNER. — Juan M. Abal Medina. — Juan L. Manzur.

MINISTERIO DE SEGURIDAD

Decreto 1234/2013

Dase por prorrogada designación.

Bs. As., 26/8/2013

VISTO el Expediente N° 23561/2012 del registro del MINISTERIO DE SEGURIDAD, los Decretos Nros. 491 del 12 de marzo de 2002, 2098 del 3 de diciembre de 2008, 1597 del 2 de octubre de 2008, 708 del 11 de junio de 2009, 2226 del 28 de diciembre de 2009, 8 del 6 de enero de 2011 y 1261 del 17 de agosto de 2011, y

CONSIDERANDO:

Que mediante el Decreto N° 1597/08 se designó transitoriamente a Don Roberto Juan CAMPOS (D.N.I. N° 13.452.441), en un cargo Nivel B - Grado 0 del Convenio Colectivo de Trabajo Sectorial del personal del SISTEMA NACIONAL DE EMPLEO PUBLICO (SINEP), homologado por el Decreto N° 2098/08, correspondiente a la planta permanente de la ex SECRETARIA DE SEGURIDAD INTERIOR del entonces MINISTERIO DE JUSTICIA, SEGURIDAD Y DERECHOS HUMANOS, para cumplir funciones como Coordinador de Proyectos.

Que por los Decretos Nros. 708/09, 2226/09 y 1261/11 se prorrogó la designación transitoria mencionada en el párrafo precedente.

Que mediante el artículo 6° del Decreto N° 8/11 se transfirió al MINISTERIO DE SEGURIDAD la dotación de la ex SECRETARIA DE SEGURIDAD INTERIOR del entonces MINISTERIO DE JUSTICIA, SEGURIDAD Y DERECHOS HUMANOS y sus unidades dependientes, manteniendo el

personal transferido sus respectivos cargos, niveles, grados de revista escalafonarios, funciones ejecutivas, adicionales y suplementos.

Que por razones de índole operativa no se ha podido tramitar el proceso de selección para la cobertura del cargo en cuestión, razón por la cual el MINISTERIO DE SEGURIDAD solicita la prórroga de la designación transitoria aludida.

Que mediante el Decreto N° 491/02 se estableció, entre otros aspectos, que toda designación de personal, en el ámbito de la Administración Pública, centralizada y descentralizada, en cargos de planta permanente, y no permanente, será efectuada por el PODER EJECUTIVO NACIONAL a propuesta de la jurisdicción correspondiente.

Que el Decreto N° 601 de fecha 11 de abril de 2002, en su artículo 6°, establece que los proyectos de decretos que propicien designaciones, contrataciones que no impliquen renovación o prórroga y reincorporación de personal en el ámbito de la Administración Pública Nacional deberán ser acompañados por la documentación detallada en la Circular del Secretario Legal y Técnico de la PRESIDENCIA DE LA NACION N° 4 de fecha 15 de marzo de 2002.

Que el agente involucrado en la presente medida se encuentra exceptuado de lo establecido en el referido artículo 6° del Decreto N° 601/02 reglamentario del Decreto N° 491/02 por haber dado cumplimiento oportunamente.

Que la presente medida no implica un exceso en los créditos asignados ni constituye asignación de recurso extraordinario alguno.

Que se cuenta con el crédito necesario en el presupuesto del MINISTERIO DE SEGURIDAD para atender el gasto resultante de la medida que se aprueba por el presente.

Que ha tomado intervención la DIRECCION GENERAL DE ASUNTOS JURIDICOS del MINISTERIO DE SEGURIDAD.

Que la presente medida se dicta en virtud de las atribuciones emergentes del artículo 99, inciso 1 de la CONSTITUCION NACIONAL y a tenor de lo dispuesto por el artículo 1° del Decreto N° 491/02.

Por ello,

LA PRESIDENTA
DE LA NACION ARGENTINA
DECRETA:

Artículo 1° — Dase por prorrogada, a partir del 20 de mayo de 2011 —fecha de su vencimiento— y por el término de CIENTO OCHENTA (180) días hábiles a partir de la fecha de la presente medida, la designación transitoria oportunamente dispuesta por el Decreto N° 1597/08 y prorrogada por sus similares Nros. 708/09, 2226/09 y 1261/11, de Don Roberto Juan CAMPOS (D.N.I. N° 13.452.441), en UN (1) cargo Nivel B - Grado 0 del Convenio Colectivo de Trabajo Sectorial del personal del SISTEMA NACIONAL DE EMPLEO PUBLICO (SINEP), homologado por Decreto N° 2098/08, correspondiente a la planta permanente del MINISTERIO DE SEGURIDAD, para cumplir funciones como Coordinador de Proyectos, con autorización excepcional por no reunir los requisitos mínimos de acceso al nivel indicado, establecidos en el artículo 14 del mencionado Convenio.

Art. 2° — El cargo involucrado deberá ser cubierto conforme los requisitos y sistemas de selección vigentes según lo establecido, respectivamente, en los Títulos II, Capítulos III y IV, y IV del CONVENIO COLECTIVO DE TRABAJO SECTORIAL DEL PERSONAL DEL SISTEMA NACIONAL DE EMPLEO PUBLICO (SINEP), homologado por Decreto N° 2098/08, dentro del plazo de CIENTO OCHENTA (180) días hábiles contados a partir de la fecha del presente Decreto.

Art. 3° — El gasto que demande el cumplimiento de lo dispuesto precedentemente se imputará con cargo a las partidas específicas del presupuesto vigente de la Jurisdicción 41 - MINISTERIO DE SEGURIDAD.

Art. 4° — Comuníquese, publíquese, dese a la DIRECCION NACIONAL DEL REGISTRO OFICIAL y archívese. — FERNANDEZ DE KIRCHNER. — Juan M. Abal Medina. — Arturo A. Puricelli.

MINISTERIO DE AGRICULTURA, GANADERIA Y PESCA

Decreto 1231/2013

Designación en la Dirección de Coordinación Federal de la Dirección Nacional de Coordinación Política de la Subsecretaría de Coordinación Política.

Bs. As., 26/8/2013

VISTO el Expediente N° S01:0440823/2012 del Registro del MINISTERIO DE AGRICULTURA, GANADERIA Y PESCA, el Presupuesto General de la Administración Nacional para los Ejercicios 2012 y 2013 aprobado por las Leyes Nros. 26.728 y 26.784, respectivamente, los Decretos Nros. 1.840 de fecha 10 de octubre de 1986, sus modificatorios y complementarios, 491 de fecha 12 de marzo de 2002, 2.098 de fecha 3 de diciembre de 2008 y 168 de fecha 3 de febrero de 2012, la Decisión Administrativa N° 175 de fecha 9 de abril de 2010, las Resoluciones Nros. 395 de fecha 5 de octubre de 2010 y 1.091 de fecha 26 de octubre de 2012 ambas del citado Ministerio, y

CONSIDERANDO:

Que por el Artículo 7° del Presupuesto General de la Administración Nacional para los Ejercicios 2012 y 2013 aprobado por las Leyes Nros. 26.728 y 26.784, respectivamente, se dispuso el congelamiento de los cargos vacantes financiados existentes a la fecha de la sanción de las referidas normas, en las Jurisdicciones y Entidades de la Administración Nacional y de los que queden vacantes con posterioridad a dicha fecha, salvo decisión fundada del señor Jefe de Gabinete de Ministros o del PODER EJECUTIVO NACIONAL, en virtud de la disposición del Artículo 10 de las citadas leyes.

Que el Decreto N° 491 de fecha 12 de marzo de 2002 dispuso, entre otros aspectos, que toda designación de personal en el ámbito de la Administración Pública, centralizada y descentralizada, en cargos de planta permanente y no permanente, será efectuada por el PODER EJECUTIVO NACIONAL, a propuesta de la Jurisdicción o Entidad correspondiente.

Que por el Artículo 1° de la Decisión Administrativa N° 175 de fecha 9 de abril de 2010, se aprobó la estructura organizativa del primer nivel operativo de la SECRETARIA DE AGRICULTURA, GANADERIA Y PESCA, de la SECRETARIA DE DESARROLLO RURAL Y AGRICULTURA FAMILIAR y de la ex- SECRETARIA DE RELACIONES INSTITUCIONALES, todas pertenecientes al MINISTERIO DE AGRICULTURA, GANADERIA Y PESCA.

Que asimismo, mediante la Resolución N° 395 de fecha 5 de octubre de 2010 del citado Ministerio, se aprobaron las aperturas estructurales inferiores de las mencionadas Secretarías.

Que por el Decreto N° 168 de fecha 3 de febrero de 2012 se modificó el organigrama de aplicación del MINISTERIO DE AGRICULTURA, GANADERIA Y PESCA incorporando la SECRETARIA DE COORDINACION POLITICO - INSTITUCIONAL Y EMERGENCIA AGROPECUARIA al citado Ministerio.

Que por el Artículo 1° de la Resolución N° 1.091 de fecha 26 de octubre de 2012 del MINISTERIO DE AGRICULTURA, GANADERIA Y PESCA, se aprobaron las segundas aperturas de la estructura organizativa para las Secretarías citadas, estableciendo a la Dirección de Coordinación Federal dependiente de la Dirección Nacio-

nal de Coordinación Política de la SUBSECRETARIA DE COORDINACION POLITICA de la SECRETARIA DE COORDINACION POLITICO - INSTITUCIONAL Y EMERGENCIA AGROPECUARIA del citado Ministerio.

Que en virtud de específicas razones de servicio de la SECRETARIA DE COORDINACION POLITICO - INSTITUCIONAL Y EMERGENCIA AGROPECUARIA del MINISTERIO DE AGRICULTURA, GANADERIA Y PESCA, se considera imprescindible la cobertura de UN (1) cargo vacante Nivel B, Función Ejecutiva III, correspondiente al titular de la Dirección de Coordinación Federal.

Que para cubrir dicho cargo se propone al Abogado D. Hugo Marcelo PONCE DE LEON (M.I. N° 17.678.519).

Que si bien el agente que se propone posee condiciones de experiencia e idoneidad para cubrir dicho cargo, debe ser exceptuado de los requisitos establecidos en el Artículo 14 del SISTEMA NACIONAL DE EMPLEO PUBLICO (S.I.N.E.P.), aprobado por el Convenio Colectivo de Trabajo Sectorial homologado por el Decreto N° 2.098 de fecha 3 de diciembre de 2008.

Que el Decreto N° 1.840 de fecha 10 de octubre de 1986, sus modificatorios y complementarios, establece, entre otras medidas, un régimen especial de compensación de los mayores gastos en que incurran los funcionarios convocados por el PODER EJECUTIVO NACIONAL para cumplir funciones políticas, cuando su residencia sea permanente y se encuentre a una distancia superior a los CIENTO KILOMETROS (100 km) de la sede de los respectivos organismos que revistan.

Que el agente citado precedentemente tiene su residencia permanente en la Ciudad de Corrientes, Provincia de CORRIENTES, conforme lo acreditado con la documentación pertinente.

Que ello implica resolver la cobertura de dicho cargo mediante una excepción a las limitaciones establecidas por el Artículo 7° del Presupuesto General de la Administración Nacional para los Ejercicios 2012 y 2013 aprobado por las Leyes Nros. 26.728 y 26.784, respectivamente.

Que el cargo aludido no constituye asignación de recurso extraordinario alguno para el ESTADO NACIONAL.

Que se ha dado cumplimiento a la Circular N° 4 de fecha 15 de marzo de 2002 de la SECRETARIA LEGAL Y TECNICA de la PRESIDENCIA DE LA NACION.

Que la Dirección General de Asuntos Jurídicos del MINISTERIO DE AGRICULTURA, GANADERIA Y PESCA ha tomado la debida intervención.

Que la presente medida se dicta en virtud de las facultades conferidas por los Artículos 99, incisos 1 y 7 de la CONSTITUCION NACIONAL, 7° y 10 del Presupuesto General de la Administración Nacional para los Ejercicios 2012 y 2013 aprobado por las Leyes Nros. 26.728 y 26.784, respectivamente, y 1° del citado Decreto N° 491/02.

Por ello,

LA PRESIDENTA
DE LA NACION ARGENTINA
DECRETA:

Artículo 1° — Dase por designado transitoriamente a partir del 28 de diciembre de 2012 y por el término de CIENTO OCHENTA (180) días hábiles contados a partir del dictado del presente decreto, en UN (1) cargo vacante Nivel B, Función Ejecutiva III, como titular de la Dirección de Coordinación Federal dependiente de la Dirección Nacional de Coordinación Política de la SUBSECRETARIA DE COORDINACION POLITICA de la SECRETARIA DE COORDINACION POLITICO - INSTITUCIONAL Y EMERGENCIA AGROPECUARIA del MINISTERIO DE AGRICULTURA, GANADERIA Y PESCA, al Abogado D. Hugo Marcelo PONCE DE LEON (M.I. N° 17.678.519), autorizándose el correspondiente pago de Función Ejecutiva del

SISTEMA NACIONAL DE EMPLEO PUBLICO (S.I.N.E.P.) aprobado por el Convenio Colectivo de Trabajo Sectorial homologado por el Decreto N° 2.098 de fecha 3 de diciembre de 2008 y con autorización excepcional por no reunir los requisitos mínimos establecidos en el Artículo 14 del Anexo del mencionado Decreto N° 2.098/08 y con carácter de excepción a lo dispuesto por el Artículo 7° del Presupuesto General de la Administración Nacional para los Ejercicios 2012 y 2013 aprobado por las Leyes Nros. 26.728 y 26.784, respectivamente.

Art. 2° — El cargo involucrado deberá ser cubierto conforme los requisitos y sistemas de selección vigentes según lo establecido, respectivamente, en los Títulos II, Capítulos III, IV y VIII, y IV del Convenio Colectivo de Trabajo Sectorial del Personal del SISTEMA NACIONAL DE EMPLEO PUBLICO (S.I.N.E.P.), homologado por el citado Decreto N° 2.098/08, dentro del plazo de CIENTO OCHENTA (180) días hábiles, contados a partir del dictado del presente decreto.

Art. 3° — Inclúyese con carácter de excepción y mientras su residencia permanente se encuentre a una distancia superior a los CIENTO KILOMETROS (100 km) de la CIUDAD AUTONOMA DE BUENOS AIRES, dentro de las previsiones del Decreto N° 1.840 de fecha 10 de octubre de 1986, sus modificatorios y complementarios, al Abogado D. Hugo Marcelo PONCE DE LEON (M.I. N° 17.678.519), a partir del primer día hábil del mes siguiente al de la fecha de dictado del presente decreto.

Art. 4° — El gasto que demande el cumplimiento de la presente medida será atendido con cargo a las partidas específicas de la Jurisdicción 52 - MINISTERIO DE AGRICULTURA, GANADERIA Y PESCA.

Art. 5° — Comuníquese, publíquese, dese a la Dirección Nacional del Registro Oficial y archívese. — FERNANDEZ DE KIRCHNER. — Juan M. Abal Medina. — Norberto G. Yauhar.

MINISTERIO DE TRABAJO, EMPLEO Y SEGURIDAD SOCIAL

Decreto 1235/2013

Designación en la Dirección de Programación Operativa de la Dirección Nacional de Fiscalización de la Subsecretaría de Fiscalización del Trabajo y de la Seguridad Social.

Bs. As., 26/8/2013

VISTO el Expediente N° 1.533.335/12 del Registro del MINISTERIO DE TRABAJO, EMPLEO Y SEGURIDAD SOCIAL, las Leyes Nros. 26.728 y 26.784, los Decretos Nros. 491 del 12 de marzo de 2002, 628 del 13 de junio de 2005 y sus modificatorios y 2.098 del 3 de diciembre de 2008 y sus modificatorios, la Decisión Administrativa N° 917 del 28 de diciembre de 2010 y sus modificatorias, las Resoluciones del MINISTERIO DE TRABAJO, EMPLEO Y SEGURIDAD SOCIAL Nros. 99 del 27 de enero de 2012, 260 del 18 de marzo de 2011 y 921 del 26 de octubre de 2012, y

CONSIDERANDO:

Que por las Leyes Nros. 26.728 y 26.784 se aprobaron los Presupuestos Generales de la Administración Nacional para los Ejercicios 2012 y 2013.

Que mediante el Decreto N° 491 del 12 de marzo de 2002 se estableció que toda designación, asignación de funciones, promoción y reincorporación de personal, en el ámbito de la Administración Pública, centralizada y descentralizada, en cargos de planta permanente y no permanente será efectuada por el PODER EJECUTIVO NACIONAL, a propuesta de la Jurisdicción correspondiente.

Que por el artículo 7° de las Leyes Nros. 26.728 y 26.784, se dispuso el congelamiento de los cargos vacantes financiados existentes a la fecha de sanción de las mismas, en las Jurisdicciones y Entidades

de la Administración Nacional y de los que queden vacantes con posterioridad, salvo decisión fundada del señor Jefe de Gabinete de Ministros.

Que por el artículo 10 de las Leyes Nros. 26.728 y 26.784, se dispuso que las facultades otorgadas por dichas leyes al señor Jefe de Gabinete de Ministros podrán ser asumidas por el PODER EJECUTIVO NACIONAL, en su carácter de responsable político de la Administración General del país y en función de lo dispuesto por el inciso 10 del artículo 99 de la CONSTITUCION NACIONAL.

Que por el Decreto N° 628 del 13 de junio de 2005 y sus modificatorios y la Decisión Administrativa N° 917 del 28 de diciembre de 2010 y sus modificatorias, se aprobó la estructura organizativa de primer nivel operativo del MINISTERIO DE TRABAJO, EMPLEO Y SEGURIDAD SOCIAL.

Que por la Resolución del MINISTERIO DE TRABAJO, EMPLEO Y SEGURIDAD SOCIAL N° 260 del 18 de marzo de 2011 se aprobaron las aperturas inferiores al primer nivel operativo de la estructura organizativa del MINISTERIO DE TRABAJO, EMPLEO Y SEGURIDAD SOCIAL.

Que por la Resolución del MINISTERIO DE TRABAJO, EMPLEO Y SEGURIDAD SOCIAL N° 99 del 27 de enero de 2012 se aprobaron las aperturas inferiores correspondientes a los niveles de departamento y división de la SECRETARIA DE TRABAJO de esa Jurisdicción.

Que mediante la Resolución del MINISTERIO DE TRABAJO, EMPLEO Y SEGURIDAD SOCIAL N° 921 del 26 de octubre de 2012 se sustituyó el Anexo III —Dotación— al artículo 1° de la Resolución del MINISTERIO DE TRABAJO, EMPLEO Y SEGURIDAD SOCIAL N° 99/12.

Que en el ámbito del MINISTERIO DE TRABAJO, EMPLEO Y SEGURIDAD SOCIAL se encuentra vacante el cargo de Nivel B, Grado 0, Jefe de Departamento de Registros y Bases de Datos dependiente de la Dirección de Programación Operativa de la Dirección Nacional de Fiscalización de la SUBSECRETARIA DE FISCALIZACION DEL TRABAJO Y DE LA SEGURIDAD SOCIAL de la SECRETARIA DE TRABAJO.

Que por la particular naturaleza de las tareas asignadas a la mencionada Unidad Organizativa, resulta necesario proceder a su inmediata cobertura y con carácter transitorio, exceptuándola a tal efecto de lo dispuesto en el artículo 7° de las Leyes Nros. 26.728 y 26.784 y de lo establecido, respectivamente en los Títulos II, Capítulos III y IV; y IV del CONVENIO COLECTIVO DE TRABAJO SECTORIAL DEL PERSONAL DEL SISTEMA NACIONAL DE EMPLEO PUBLICO (SINEP), homologado por el Decreto N° 2.098/08.

Que por el Decreto N° 2.098 del 3 de diciembre de 2008, se homologó el CONVENIO COLECTIVO DE TRABAJO SECTORIAL DEL PERSONAL DEL SISTEMA NACIONAL DE EMPLEO PUBLICO (SINEP), concertado entre el Estado Empleador y los Sectores Gremiales mediante el Acta Acuerdo de fecha 5 de septiembre de 2008.

Que el cargo involucrado deberá ser cubierto de conformidad con los requisitos y sistemas de selección vigentes según lo establecido, respectivamente en los Títulos II, Capítulos III y IV; y IV del CONVENIO COLECTIVO DE TRABAJO SECTORIAL DEL PERSONAL DEL SISTEMA NACIONAL DE EMPLEO PUBLICO (SINEP), homologado por el Decreto N° 2.098/08, dentro del plazo de CIENTO OCHENTA (180) días hábiles contados a partir de la fecha de la presente medida.

Que la persona propuesta reúne las condiciones de experiencia e idoneidad necesarias para desempeñar el cargo que se encuentra vacante.

Que el cargo aludido no constituye asignación de recurso extraordinario alguno para el ESTADO NACIONAL.

Que se encuentran reunidos los requisitos exigidos en la Circular N° 4 de fecha 15 de marzo de 2002 de la SECRETARIA LEGAL Y TECNICA de la PRESIDENCIA DE LA NACION.

Que la Dirección General de Asuntos Jurídicos del MINISTERIO DE TRABAJO, EMPLEO Y SEGURIDAD SOCIAL ha tomado la intervención que le compete.

Que la presente medida se dicta en virtud de las atribuciones emergentes del artículo 99, incisos 1 y 7 de la CONSTITUCION NACIONAL, de los artículos 7° y 10 de las Leyes Nros. 26.728 y 26.784 y del artículo 1° del Decreto N° 491/02.

Por ello,

LA PRESIDENTA
DE LA NACION ARGENTINA
DECRETA:

Artículo 1° — Dase por designada transitoriamente, a partir del 1° de noviembre de 2012 y por el término de CIENTO OCHENTA (180) días hábiles contados desde la fecha de la presente medida, en el cargo Nivel B, Grado 0, Jefa de Departamento de Registros y Bases de Datos dependiente de la Dirección de Programación Operativa de la Dirección Nacional de Fiscalización de la SUBSECRETARIA DE FISCALIZACION DEL TRABAJO Y DE LA SEGURIDAD SOCIAL de la SECRETARIA DE TRABAJO del MINISTERIO DE TRABAJO, EMPLEO Y SEGURIDAD SOCIAL, a la Lic. Julia Verónica SOSA (M.I. N° 25.676.758) con carácter de excepción a lo dispuesto por el artículo 7° de las Leyes Nros. 26.728 y 26.784.

Art. 2° — El cargo involucrado deberá ser cubierto de conformidad con los requisitos y sistemas de selección vigentes según lo establecido, respectivamente, en los Títulos II, Capítulos III y IV; y IV del CONVENIO COLECTIVO DE TRABAJO SECTORIAL DEL PERSONAL DEL SISTEMA NACIONAL DE EMPLEO PUBLICO (SINEP) homologado por el Decreto N° 2.098/08, dentro del plazo de CIENTO OCHENTA (180) días hábiles contados a partir de la fecha de la presente medida.

Art. 3° — El gasto que demande el cumplimiento del presente decreto será atendido con cargo a las partidas específicas del presupuesto vigente de la Jurisdicción 75 - MINISTERIO DE TRABAJO, EMPLEO Y SEGURIDAD SOCIAL.

Art. 4° — Comuníquese, publíquese, dese a la Dirección Nacional del Registro Oficial y archívese. — FERNANDEZ DE KIRCHNER. — Juan M. Abal Medina. — Carlos A. Tomada.

MINISTERIO DE AGRICULTURA, GANADERIA Y PESCA

Decreto 1230/2013

Inclúyese funcionaria dentro de las previsiones del Decreto N° 1.840/1986.

Bs. As., 26/8/2013

VISTO el Expediente N° S05:0517905/2013 del Registro del MINISTERIO DE AGRICULTURA, GANADERIA Y PESCA, el Presupuesto General de la Administración Nacional para el Ejercicio 2013 aprobado por la Ley N° 26.784, los Decretos Nros. 1.840 de fecha 10 de octubre de 1986, sus modificatorios y complementarios, y 2.753 de fecha 28 de diciembre de 2012, y

CONSIDERANDO:

Que por el Decreto N° 2.753 de fecha 28 de diciembre de 2012 se aprobó la designación transitoria, a partir del 30 de octubre de 2012, como Directora Nacional de Tierras y Unidades Agropecuarias dependiente de la SUBSECRETARIA DE COORDINACION POLITICA de la SECRETARIA DE COORDINACION POLITICO - INSTITUCIONAL Y EMERGENCIA AGROPECUARIA del MINISTERIO DE AGRICULTURA, GANADERIA Y PESCA, de la Abogada Da. Mariana Raquel URIA (M.I. N° 23.715.210).

Que el Decreto N° 1.840 de fecha 10 de octubre de 1986, sus modificatorios y complementarios establece, entre otras medidas, un régimen especial de compensación de los mayores gastos en que incurran los funcionarios convocados por el PODER EJECUTIVO NACIONAL para cumplir funciones políticas, cuando su residencia sea permanente y se encuentre a una distancia superior a los CIEN KILOMETROS (100 km) de la sede de los respectivos organismos que revistan.

Que la funcionaria citada precedentemente tiene su residencia permanente en la Ciudad de La Rioja, Provincia de LA RIOJA, conforme lo acreditado con la documentación pertinente, por lo tanto corresponde proceder a incluirla, con carácter de excepción, dentro de las previsiones del Decreto N° 1.840/86.

Que la Dirección General de Asuntos Jurídicos del MINISTERIO DE AGRICULTURA, GANADERIA Y PESCA ha tomado la intervención que le compete.

Que la presente medida se dicta en virtud de las facultades conferidas por el Artículo 99, inciso 1 de la CONSTITUCION NACIONAL.

Por ello,

LA PRESIDENTA
DE LA NACION ARGENTINA
DECRETA:

Artículo 1° — Inclúyese con carácter de excepción y mientras su residencia permanente se encuentre a una distancia superior a los CIEN KILOMETROS (100 km) de la CIUDAD AUTONOMA DE BUENOS AIRES, dentro de las previsiones del Decreto N° 1.840 de fecha 10 de octubre de 1986, sus modificatorios y complementarios, a la Directora Nacional de Tierras y Unidades Agropecuarias dependiente de la SUBSECRETARIA DE COORDINACION POLITICA de la SECRETARIA DE COORDINACION POLITICO - INSTITUCIONAL Y EMERGENCIA AGROPECUARIA del MINISTERIO DE AGRICULTURA, GANADERIA Y PESCA, Abogada Da. Mariana Raquel URIA (M.I. N° 23.715.210), a partir del primer día del mes siguiente al de la fecha de dictado del presente decreto.

Art. 2° — El gasto que demande el cumplimiento de la presente medida será atendido con cargo a las partidas específicas de la Jurisdicción 52 - MINISTERIO DE AGRICULTURA, GANADERIA Y PESCA.

Art. 3° — Comuníquese, publíquese, dese a la Dirección Nacional del Registro Oficial y archívese. — FERNANDEZ DE KIRCHNER. — Juan M. Abal Medina. — Norberto G. Yauhar.

MINISTERIO DEL INTERIOR Y TRANSPORTE

Decreto 1221/2013

Dase por prorrogada designación en la Dirección Nacional de Migraciones.

Bs. As., 26/8/2013

VISTO el Expediente N° S02:0018301/2012 del registro de la DIRECCION NACIONAL DE MIGRACIONES, organismo descentralizado actuante en la órbita del MINISTERIO DEL INTERIOR Y TRANSPORTE, las Leyes N° 26.728 y N° 26.784 y los Decretos N° 491 del 12 de marzo de 2002, N° 1338 del 15 de septiembre de 2010 y N° 110 del 17 de enero de 2012, y

CONSIDERANDO:

Que mediante el Decreto N° 491/02 se estableció, entre otros aspectos, que toda designación de personal en el ámbito de la Administración Pública Nacional, centralizada y descentralizada, en cargos de planta permanente y no permanente, incluyendo en estos últimos al personal transitorio y contratado, cualquiera fuere su modalidad y fuente de financiamiento, será efectuada

por el PODER EJECUTIVO NACIONAL a propuesta de la jurisdicción o entidad correspondiente.

Que mediante el Decreto N° 1338/10 se ha designado transitoriamente en la Planta Permanente, a la señora Irene Miriam BÖSCH (DNI N° 11.191.793) Nivel B - Grado 0, con carácter de excepción a lo establecido por el Título II, Capítulo III, artículo 14 del SISTEMA NACIONAL DE EMPLEO PUBLICO (SINEP) aprobado por el CONVENIO COLECTIVO DE TRABAJO SECTORIAL homologado por el Decreto N° 2098 del 3 de diciembre de 2008, en el cargo de Delegada de la DELEGACION POSADAS dependiente de la DIRECCION NACIONAL DE MIGRACIONES.

Que mediante el Decreto N° 110/12 se prorrogó por el término de CIENTO OCHENTA (180) días hábiles el plazo de la designación transitoria aprobada por el Decreto N° 1338/10.

Que por razones operativas no ha sido posible cumplimentar la cobertura del cargo en el plazo establecido, por lo que resulta indispensable prorrogar la mencionada designación por el término de CIENTO OCHENTA (180) días hábiles, contados a partir del dictado de la presente medida.

Que asimismo, a través de la Ley N° 26.784, se aprobó el Presupuesto General de la Administración Nacional para el Ejercicio 2013.

Que la DIRECCION GENERAL DE ASUNTOS JURIDICOS del MINISTERIO DEL INTERIOR Y TRANSPORTE ha tomado la intervención que le compete.

Que la presente medida se dicta en ejercicio de las atribuciones emergentes del artículo 99 inciso 1 de la CONSTITUCION NACIONAL y a tenor de lo establecido por el artículo 1° del Decreto N° 491 del 12 de marzo de 2002.

Por ello,

LA PRESIDENTA
DE LA NACION ARGENTINA
DECRETA:

Artículo 1° — Dase por prorrogado a partir del 16 de octubre de 2012 y por el término de CIENTO OCHENTA (180) días hábiles, contados a partir del dictado de la presente medida, el plazo establecido por el Decreto N° 1338 del 15 de septiembre de 2010 que fuera prorrogado por el Decreto N° 110 del 17 de enero de 2012, con relación a la designación transitoria en la Planta Permanente de la señora Irene Miriam BÖSCH (DNI N° 11.191.793), en el cargo de Delegada de la DELEGACION POSADAS dependiente de la DIRECCION NACIONAL DE MIGRACIONES, organismo descentralizado actuante en la órbita del MINISTERIO DEL INTERIOR Y TRANSPORTE, Nivel B - Grado 0 y con autorización excepcional por no reunir los requisitos mínimos establecidos en el artículo 14 del SISTEMA NACIONAL DE EMPLEO PUBLICO (SINEP), aprobado por el CONVENIO COLECTIVO DE TRABAJO SECTORIAL homologado por el Decreto N° 2098 del 3 de diciembre de 2008.

Art. 2° — El cargo involucrado, deberá ser cubierto conforme los requisitos y sistemas de selección vigentes, según lo establecido, respectivamente, en los Títulos II, Capítulos III y IV, y IV del SISTEMA NACIONAL DE EMPLEO PUBLICO (SINEP), dentro del plazo de CIENTO OCHENTA (180) días hábiles contados a partir del dictado de la presente medida.

Art. 3° — El gasto que demande el cumplimiento del presente será atendido con cargo a las partidas específicas del Presupuesto vigente para el corriente ejercicio, correspondiente a la Jurisdicción 30 - MINISTERIO DEL INTERIOR Y TRANSPORTE - O.D. 201 - DIRECCION NACIONAL DE MIGRACIONES.

Art. 4° — Comuníquese, publíquese, dese a la DIRECCION NACIONAL DEL REGISTRO OFICIAL y archívese. — FERNANDEZ DE KIRCHNER. — Juan M. Abal Medina. — Aníbal F. Randazzo.

MINISTERIO DEL INTERIOR Y TRANSPORTE

Decreto 1222/2013

Danse por prorrogadas designaciones en la Agencia Nacional de Seguridad Vial.

Bs. As., 26/8/2013

VISTO el Expediente N° S02:0011642/2013 del registro de la AGENCIA NACIONAL DE SEGURIDAD VIAL, Organismo Descentralizado actuante en la órbita del MINISTERIO DEL INTERIOR Y TRANSPORTE, la Ley N° 26.784, los Decretos N° 491 del 12 de marzo de 2002, N° 2098 del 3 de diciembre de 2008, N° 466 del 27 de marzo de 2012, y

CONSIDERANDO:

Que mediante el Decreto N° 491/02 se estableció, entre otros aspectos, que toda designación de personal, en el ámbito de la Administración Pública, centralizada y descentralizada, en cargos de planta permanente y no permanente será efectuada por el PODER EJECUTIVO NACIONAL a propuesta de la jurisdicción correspondiente.

Que por el Decreto N° 466/12 se han designado transitoriamente en la Planta Permanente de la AGENCIA NACIONAL DE SEGURIDAD VIAL al personal aludido en la presente medida.

Que resulta necesario prorrogar las mencionadas designaciones transitorias por el término de CIENTO OCHENTA (180) días hábiles, toda vez que aún no se han realizado los procesos de selección previstos.

Que han tomado la intervención que les compete la DIRECCION DE ASUNTOS LEGALES Y JURIDICOS de la AGENCIA NACIONAL DE SEGURIDAD VIAL y la DIRECCION GENERAL DE ASUNTOS JURIDICOS del MINISTERIO DEL INTERIOR Y TRANSPORTE.

Que la presente medida se dicta en uso de las atribuciones emergentes del artículo 99, inciso 1 de la CONSTITUCION NACIONAL, y a tenor de lo establecido por el artículo 1° del Decreto N° 491 del 12 de marzo de 2002.

Por ello,

LA PRESIDENTA
DE LA NACION ARGENTINA
DECRETA:

Artículo 1° — Dase por prorrogado a partir del 17 de diciembre de 2012 y por el término de CIENTO OCHENTA (180) días hábiles computados a partir del presente decreto, el plazo establecido por el Decreto N° 466 del 27 de marzo de 2012, con relación a las designaciones con carácter transitorio en la Planta Permanente de la AGENCIA NACIONAL DE SEGURIDAD VIAL, Organismo Descentralizado actuante en la órbita del MINISTERIO DEL INTERIOR Y TRANSPORTE, de los agentes que se detallan en el Anexo I de la presente medida, en el Nivel y Grado y en las funciones que se detallan en cada caso.

Art. 2° — Los cargos involucrados en el artículo 1° deberán ser cubiertos conforme a los sistemas de selección vigentes y requisitos según lo establecido, respectivamente, en los Títulos II, Capítulos III y IV, y IV del SISTEMA NACIONAL DE EMPLEO PUBLICO (SINEP), aprobado por el Convenio Colectivo de Trabajo Sectorial homologado por el Decreto N° 2098/08, en el término de CIENTO OCHENTA (180) días hábiles computados a partir del dictado del presente decreto.

Art. 3° — El gasto que demande el cumplimiento de la presente medida será atendido con cargo a las partidas específicas del presupuesto vigente de la Jurisdicción 30 - MINISTERIO DEL INTERIOR Y TRANSPORTE - O.D. 203 - AGENCIA NACIONAL DE SEGURIDAD VIAL.

Art. 4° — Comuníquese, publíquese, dése a la DIRECCION NACIONAL DEL REGISTRO OFICIAL y archívese. — FERNANDEZ DE KIRCHNER. — Juan M. Abal Medina. — Aníbal F. Randazzo.

ANEXO I

AGENCIA NACIONAL DE SEGURIDAD VIAL

PLANTA PERMANENTE

EXPEDIENTE N° 11642/2013

Apellido	Nombre	Tipo	Número	Unidad de Revista	Función	Nivel	Grado
CARABAS	Nicolás	DNI	26.429.345	Dirección de Coordinación del Control y Fiscalización Vial	Asistente Fiscalizador	D	0
DIAZ	Carlos Claudio	DNI	22.865.279	Dirección de Coordinación del Control y Fiscalización Vial	Asistente Fiscalizador	D	0
GONZALEZ	Lucas Felipe	DNI	32.312.707	Dirección de Coordinación del Control y Fiscalización Vial	Asistente Fiscalizador	D	0
LATCOVICH	Walter Leonardo	DNI	16.733.464	Dirección de Coordinación del Control y Fiscalización Vial	Asistente Fiscalizador	D	0
LOPEZ SAWLAN	Ezequiel Nicolás	DNI	27.620.447	Dirección de Coordinación del Control y Fiscalización Vial	Asistente Fiscalizador	D	0
PEREZ	Néstor Arturo	DNI	14.723.517	Dirección de Coordinación del Control y Fiscalización Vial	Asistente Fiscalizador	D	0
PIETRA RISSOTTO	Eduardo André	DNI	18.868.320	Dirección de Coordinación del Control y Fiscalización Vial	Asistente Fiscalizador	D	0
SERRA	Diego Sebastián	DNI	30.777.206	Dirección de Coordinación del Control y Fiscalización Vial	Asistente Fiscalizador	D	0
TROMBINI	Pablo Ricardo	DNI	25.790.822	Dirección de Coordinación del Control y Fiscalización Vial	Asistente Fiscalizador	D	0

DECISIONES ADMINISTRATIVAS


MINISTERIO DE AGRICULTURA, GANADERIA Y PESCA

Decisión Administrativa 648/2013

Contratación.

Bs. As., 23/8/2013

VISTO el Expediente N° S01:0172999/2012 del Registro del MINISTERIO DE AGRICULTURA, GANADERIA Y PESCA, la Ley N° 25.164, el Decreto N° 1.421 de fecha 8 de agosto de 2002, la Decisión Administrativa N° 3 de fecha 21 de enero de 2004 y sus modificatorias Nros. 1.151 de fecha 28 de diciembre de 2006 y 52 de fecha 6 de marzo de 2009, la Resolución N° 48 de fecha 30 de diciembre de 2002 de la ex - SUBSECRETARIA DE LA GESTION PUBLICA de la JEFATURA DE GABINETE DE MINISTROS y sus modificatorias, y

CONSIDERANDO:

Que por el expediente citado en el Visto tramita la propuesta de aprobación de la contratación de la persona que se detalla en el Anexo que forma parte integrante de la presente medida, a celebrarse bajo el régimen del Artículo 9° del Anexo a la Ley Marco de Regulación de Empleo Público Nacional N° 25.164 y su reglamentación, destinada al ámbito del MINISTERIO DE AGRICULTURA, GANADERIA Y PESCA con el objeto de fortalecer y complementar su labor, asegurando de tal modo su eficaz desenvolvimiento operativo.

Que el Convenio Colectivo de Trabajo Sectorial del Personal del SISTEMA NACIONAL DE EMPLEO PUBLICO (SI.N.E.P.), homologado por el Decreto N° 2.098 de fecha 3 de diciembre de 2008, establece los requisitos mínimos para el acceso a los distintos niveles escalafonarios.

Que el último párrafo del Artículo 9° del Anexo I del Decreto N° 1.421 de fecha 8 de agosto de 2002, establece que el señor Jefe de Gabinete de Ministros podrá autorizar excepciones al punto II) del inciso c) del citado artículo, mediante decisión fundada y a requerimiento del titular de la jurisdicción u organismo descentralizado, en los casos de funciones que posean una especialidad crítica en el mercado laboral.

Que los antecedentes curriculares de la persona mencionada en el Anexo que forma parte integrante de la presente medida, acreditan acabadamente la idoneidad necesaria para la realización de las tareas asignadas y el nivel escalafonario propuesto.

Que consecuentemente y dada la especialidad crítica en el mercado laboral de las funciones que se pretenden cubrir, corresponde exceptuar a la persona que se detalla en el Anexo que forma parte integrante de la presente medida, de los requisitos establecidos en el punto II) del inciso c) del Artículo 9° del Anexo I del Decreto N° 1.421/02, al sólo efecto de posibilitar su contratación en el MINISTERIO DE AGRICULTURA, GANADERIA Y PESCA.

Que resulta necesario entonces, dar por exceptuada a la persona propuesta del requisito establecido en el Artículo 14 inciso b) del Anexo al Decreto N° 2.098/08, para el Nivel B.

Que los Artículos 7° y 9° del Anexo a la Ley N° 25.164, reglamentada por el Decreto N° 1.421/02 y la Resolución N° 48 de fecha 30 de diciembre de 2002 de la ex - SUBSECRETARIA DE LA GESTION PUBLICA de la JEFATURA DE GABINETE DE MINISTROS y sus modificatorias, norman respecto de la naturaleza y características de la relación de empleo del personal que revista en el régimen de contrataciones para la prestación de servicios de carácter no permanente, el que será equiparado en los niveles y grados de la planta permanente.

Que se han cumplimentado, en lo pertinente, las previsiones contenidas en los Artículos 9° y 14 del Anexo I del Decreto N° 1.421/02, asimismo, las pautas para la aplicación del régimen de contrataciones del personal aprobadas por la citada Resolución N° 48/02 y sus modificatorias y las prescripciones referidas a la asignación de grado contenidas en la Decisión Administrativa N° 3 de fecha 21 de enero de 2004 y sus modificatorias Nros. 1.151 de fecha 28 de diciembre de 2006 y 52 de fecha 6 de marzo de 2009.

Que la persona indicada en el Anexo que integra la presente medida ha dado cumplimiento a los requisitos establecidos en la Circular N° 4 de fecha 15 de marzo de 2002 de la SECRETARIA LEGAL Y TECNICA de la PRESIDENCIA DE LA NACION.

Que la Dirección General de Recursos Humanos dependiente de la SUBSECRETARIA DE COORDINACION TECNICA Y ADMINISTRATIVA del MINISTERIO DE AGRICULTURA, GANADERIA Y PESCA ha tomado la intervención que le compete.

Que la Dirección General de Asuntos Jurídicos del MINISTERIO DE AGRICULTURA, GANADERIA Y PESCA ha tomado la intervención que le compete.

Que la presente medida se dicta en uso de las atribuciones conferidas por el Artículo 100, inciso 2 de la CONSTITUCION NACIONAL y por el último párrafo del Artículo 9° del Anexo I del Decreto N° 1.421/02.

Por ello,

EL JEFE
DE GABINETE DE MINISTROS
DECIDE:

Artículo 1° — Dase por exceptuada a la persona que se detalla en el Anexo que forma parte integrante de la presente medida, de las restricciones establecidas en el punto II) del inciso c) del Artículo 9° del Anexo I del Decreto N° 1.421 de fecha 8 de agosto de 2002, reglamentario de la Ley Marco de Regulación de Empleo Público Nacional N° 25.164 al sólo efecto de posibilitar su contratación, en el nivel y grado del Convenio Colectivo de Trabajo Sectorial del Personal del SISTEMA NACIONAL DE EMPLEO PUBLICO (SI.N.E.P.), homologado por el Decreto N° 2.098 de fecha 3 de diciembre de 2008 y plazo consignados en el Anexo de la presente decisión administrativa, bajo el régimen del Artículo 9° del Anexo de la ley precitada, en el ámbito del MINISTERIO DE AGRICULTURA, GANADERIA Y PESCA.

Art. 2° — Comuníquese, publíquese, dése a la Dirección Nacional del Registro Oficial y archívese. — Juan M. Abal Medina. — Norberto G. Yauhar.

ANEXO

Modalidad de Contratación: LEY 25.164

Nombre del Proyecto: 0000001052 INDIVIDUALES DEL MINISTERIO DE AGRICULTURA, GANADERIA Y PESCA

Código de Control: 0000017696

Listado de Contrataciones

N°	Apellido	Nombre	Tipo y N° Doc.	NyG	Desde	Hasta	Prog.	Act.	Dedic.
1	BALDELLI	ALEJANDRA VERONICA	D.N.I. 30367867	B0	01/05/2012	31/12/2012	1	1	100%

Cantidad de Contratos Listados: 1

Imputación Presupuestaria: 1 81 Proyecto: 0 Fuente: 11 Ubic. Geo.: 2 Jurisdicción: 52

MINISTERIO DE AGRICULTURA, GANADERIA Y PESCA

Decisión Administrativa 649/2013

Contratación en la Subsecretaría de Pesca y Acuicultura de la Secretaría de Agricultura, Ganadería y Pesca.

Bs. As., 23/8/2013

VISTO el Expediente N° S01:0445581/2012 del Registro del MINISTERIO DE AGRICULTURA, GANADERIA Y PESCA, la Ley N° 25.164, el Decreto N° 1.421 de fecha 8 de agosto de 2002, la Decisión Administrativa N° 3 de fecha 21 de enero de 2004, sus modificatorias Nros. 1.151 de fecha 28 de diciembre de 2006 y 52 de fecha 6 de marzo de 2009, la Resolución N° 48 de fecha 30 de diciembre de 2002 de la ex - SUBSECRETARIA DE LA GESTION PUBLICA de la JEFATURA DE GABINETE DE MINISTROS y sus modificatorias, y

CONSIDERANDO:

Que por el expediente citado en el Visto tramita la propuesta de aprobación de la contratación de la persona que se detalla en el Anexo que forma parte integrante de la presente medida, a celebrarse bajo el régimen del Artículo 9° del Anexo a la Ley Marco de Regulación de Empleo Público Nacional N° 25.164 y su reglamentación, destinada al ámbito de la SUBSECRETARIA DE PESCA Y ACUICULTURA de la SECRETARIA DE AGRICULTURA, GANADERIA Y PESCA del MINISTERIO DE AGRICULTURA, GANADERIA Y PESCA con el objeto de fortalecer y complementar su labor, asegurando de tal modo su eficaz desenvolvimiento operativo.

Que el Convenio Colectivo de Trabajo Sectorial del Personal del SISTEMA NACIONAL DE EMPLEO PUBLICO (SI.N.E.P.), homologado por el Decreto N° 2.098 de fecha 3 de diciembre de 2008, establece los requisitos mínimos para el acceso a los distintos niveles escalafonarios.

Que el último párrafo del Artículo 9° del Anexo I del Decreto N° 1.421 de fecha 8 de agosto de 2002, establece que el señor Jefe de Gabinete de Ministros podrá autorizar excepciones al punto II) del inciso c) del citado artículo, mediante decisión fundada y a requerimiento del titular de la jurisdicción u organismo descentralizado, en los casos de funciones que posean una especialidad crítica en el mercado laboral.

Que los antecedentes curriculares de la persona mencionada en el Anexo que forma parte integrante de la presente medida, acreditan acabadamente la idoneidad necesaria para la realización de las tareas asignadas y el nivel escalafonario propuesto.

Que consecuentemente y dada la especialidad crítica en el mercado laboral de las funciones que se pretenden cubrir, corresponde exceptuar a la persona que se detalla en el Anexo que forma parte integrante de la presente medida, de los requisitos establecidos en el punto II) del inciso c) del Artículo 9° del Anexo I del Decreto N° 1.421/02, al sólo efecto de posibilitar su contratación en el MINISTERIO DE AGRICULTURA, GANADERIA Y PESCA.

Que resulta necesario entonces, dar por exceptuada a la persona propuesta de las requisitos establecidos en el Artículo 14 del inciso a) del Anexo al Decreto N° 2.098/08, para el Nivel E.

Que los Artículos 7° y 9° del Anexo a la Ley N° 25.164, reglamentada por el Decreto N° 1.421/02 y la Resolución N° 48 de fecha 30 de diciembre de 2002 de la ex - SUBSECRETARIA DE LA GESTION PUBLICA de la JEFATURA DE GABINETE DE MINISTROS y sus modificatorias, norman respecto de la naturaleza y características de la relación de empleo del personal que revista en el régimen de contrataciones para la prestación de servicios de carácter no permanente, el que será equiparado en los niveles y grados de la planta permanente.

Que se han cumplimentado, en lo pertinente, las previsiones contenidas en los Artículos 9° y 14 del Anexo I del Decreto N° 1.421/02, asimismo, las pautas para la aplicación del régimen de contrataciones del personal aprobadas por la citada Resolución N° 48/02 y sus modificatorias, y las prescripciones referidas a la asignación de grado contenidas en la Decisión Administrativa N° 3 de fecha 21 de enero de 2004 y sus modificatorias Nros. 1.151 de fecha 28 de diciembre de 2006 y 52 de fecha 6 de marzo de 2009.

Que la persona indicada en el Anexo que integra la presente medida ha dado cumplimiento a los requisitos establecidos en la Circular N° 4 de fecha 15 de marzo de 2002 de la SECRETARIA LEGAL Y TECNICA de la PRESIDENCIA DE LA NACION.

Que la Dirección General de Recursos Humanos dependiente de la SUBSECRETARIA DE COORDINACION TECNICA Y ADMINISTRATIVA del MINISTERIO DE AGRICULTURA, GANADERIA Y PESCA ha tomado la intervención que le compete.

Que la Dirección General de Asuntos Jurídicos del MINISTERIO DE AGRICULTURA, GANADERIA Y PESCA ha tomado la intervención que le compete.

Que la presente medida se dicta en uso de las atribuciones conferidas por el Artículo 100, inciso 2 de la CONSTITUCION NACIONAL, y por el último párrafo del Artículo 9° del Anexo I del Decreto N° 1.421/02.

Por ello,

EL JEFE
DE GABINETE DE MINISTROS
DECIDE:

Artículo 1° — Dase por exceptuada a la persona que se detalla en el Anexo que forma parte integrante de la presente medida, de las restricciones establecidas en el punto II) del inciso c) del Artículo 9° del Anexo I del Decreto N° 1.421 de fecha 8 de agosto de 2002, reglamentario de la Ley Marco de Regulación de Empleo Público Nacional N° 25.164, al sólo efecto de posibilitar su contratación, en el nivel y grado del Convenio Colectivo de Trabajo Sectorial del Personal del SISTEMA NACIONAL DE EMPLEO PUBLICO (SI.N.E.P.), homologado por el Decreto N° 2.098 de fecha 3 de diciembre de 2008 y plazo consignados en el Anexo que forma parte de la presente decisión administrativa, bajo el régimen del Artículo 9° del Anexo de la ley precitada, en el ámbito de la SUBSECRETARIA DE PESCA Y ACUICULTURA de la SECRETARIA DE AGRICULTURA, GANADERIA Y PESCA del MINISTERIO DE AGRICULTURA, GANADERIA Y PESCA.

Art. 2° — Comuníquese, publíquese, dése a la Dirección Nacional del Registro Oficial y archívese. — Juan M. Abal Medina. — Norberto G. Yauhar.

ANEXO

Modalidad de Contratación: LEY 25.164

Nombre del Proyecto: 0000001233 INDIVIDUALES DE LA SUBSECRETARIA DE PESCA Y ACUICULTURA

Código de Control: 0000018354

Listado de Contrataciones

N°	Apellido	Nombre	Tipo y N° Doc.	NyG	Desde	Hasta	Prog.	Act.	Dedic.
1	MISSART	FLORENCIA SOLEDAD	D.N.I. 37162393	E0	01/08/2012	31/12/2012	1	1	100%

Cantidad de Contratos Listados: 1

Imputación Presupuestaria: 1 81 Proyecto: 0 Fuente: 11 Ubic. Geo.: 2 Jurisdicción: 52

MINISTERIO DE AGRICULTURA, GANADERIA Y PESCA

Decisión Administrativa 652/2013

Contratación en la Subsecretaría de Coordinación Técnica y Administrativa.

Bs. As., 26/8/2013

VISTO el Expediente N° S01:0112446/2012 del Registro del MINISTERIO DE AGRICULTURA, GANADERIA Y PESCA, la Ley N° 25.164, el Decreto N° 1.421 de fecha 8 de agosto de 2002, la Decisión Administrativa N° 3 de fecha 21 de enero de 2004, sus modificatorias Nros. 1.151 de fecha 28 de diciembre de 2006 y 52 de fecha 6 de marzo de 2009, la Resolución N° 48 de fecha 30 de diciembre de 2002 de la ex - SUBSECRETARIA DE LA GESTION PUBLICA de la JEFATURA DE GABINETE DE MINISTROS y sus modificatorias, y

CONSIDERANDO:

Que por el expediente citado en el Visto tramita la propuesta de aprobación de la contratación de la persona que se detalla en el Anexo que forma parte integrante de la presente medida, a celebrarse bajo el régimen del Artículo 9° del Anexo a la Ley Marco de Regulación de Empleo Público Nacional N° 25.164 y su reglamentación, destinada al ámbito de la SUBSECRETARIA DE COORDINACION TECNICA Y ADMINISTRATIVA del MINISTERIO DE AGRICULTURA GANADERIA Y PESCA con el objeto de fortalecer y complementar su labor, asegurando de tal modo su eficaz desenvolvimiento operativo.

Que el Convenio Colectivo de Trabajo Sectorial del Personal del SISTEMA NACIONAL DE EMPLEO PUBLICO (SI.N.E.P.), homologado por el Decreto N° 2.098 de fecha 3 de diciembre de 2008, establece los requisitos mínimos para el acceso a los distintos niveles escalafonarios.

Que el último párrafo del Artículo 9° del Anexo I del Decreto N° 1.421 de fecha 8 de agosto de 2002, establece que el señor Jefe de Gabinete de Ministros podrá autorizar excepciones al punto II) del inciso c) del citado artículo, mediante decisión fundada y a requerimiento del titular de la jurisdicción u organismo descentralizado, en los casos de funciones que posean una especialidad crítica en el mercado laboral.

Que los antecedentes curriculares de la persona mencionada en el Anexo que forma parte integrante de la presente medida, acreditan acabadamente la idoneidad necesaria para la realización de las tareas asignadas y el nivel escalafonario propuesto.

Que consecuentemente y dada la especialidad crítica en el mercado laboral de las funciones que se pretenden cubrir, corresponde exceptuar a la persona que se detalla en el Anexo que forma parte integrante de la presente medida, de los requisitos establecidos en el punto II) del inciso c) del Artículo 9° del Anexo I del Decreto N° 1.421/02, al solo efecto de posibilitar su contratación en el MINISTERIO DE AGRICULTURA, GANADERIA Y PESCA.

Que resulta necesario entonces dar por exceptuada a la persona propuesta de los requisitos establecidos en el Artículo 14, inciso a) del Anexo al Decreto N° 2.098/08, para el Nivel B.

Que los Artículos 7° y 9° del Anexo a la Ley N° 25.164, reglamentada por el Decreto N° 1.421/02 y la Resolución N° 48 de fecha 30 de diciembre de 2009 de la ex SUBSE-

CRETARIA DE LA GESTION PUBLICA de la JEFATURA DE GABINETE DE MINISTROS y sus modificatorias, norman respecto de la naturaleza y características de la relación de empleo del personal que revista en el régimen de contrataciones para la prestación de servicios de carácter no permanente, el que será equiparado en los niveles y grados de la planta permanente.

Que se han cumplimentado, en lo pertinente, las previsiones contenidas en los Artículos 9° y 14 del Anexo I del Decreto N° 1.421/02, asimismo, las pautas para la aplicación del régimen de contrataciones del personal aprobadas por la citada Resolución N° 48/02 y sus modificatorias, y las prescripciones referidas a la asignación de grado contenidas en la Decisión Administrativa N° 3 de fecha 21 de enero de 2004 y sus modificatorias Nros. 1.151 de fecha 28 de diciembre de 2006 y 52 de fecha 6 de marzo de 2009.

Que la persona indicada en el Anexo que integra la presente medida ha dado cumplimiento a los requisitos establecidos en la Circular N° 4 de fecha 15 de marzo de 2002 de la SECRETARIA LEGAL Y TECNICA de la PRESIDENCIA DE LA NACION.

Que la Dirección General de Recursos Humanos dependiente de la SUBSECRETARIA DE COORDINACION TECNICA Y ADMINISTRATIVA del MINISTERIO DE AGRICULTURA, GANADERIA Y PESCA ha tomado la intervención que le compete.

Que la Dirección General de Asuntos Jurídicos del MINISTERIO DE AGRICULTURA, GANADERIA Y PESCA ha tomado la intervención que le compete,

Que la presente medida se dicta en uso de las atribuciones conferidas por el Artículo 100, inciso 2 de la CONSTITUCION NACIONAL, y por el último párrafo del Artículo 9° del Anexo I del Decreto N° 1.421/02.

Por ello,

EL JEFE
DE GABINETE DE MINISTROS
DECIDE:

Artículo 1° — Dase por exceptuada a la persona que se detalla en el Anexo que forma parte integrante de la presente medida, de las restricciones establecidas en el punto II) del inciso c) del Artículo 9° del Anexo I del Decreto N° 1.421 de fecha 8 de agosto de 2002, reglamentario de la Ley Marco de Regulación de Empleo Público Nacional N° 25.164, al solo efecto de posibilitar su contratación, en el nivel y grado del Convenio Colectivo de Trabajo Sectorial del Personal del SISTEMA NACIONAL DE EMPLEO PUBLICO (S.I.N.E.P.), homologado por el Decreto N° 2098 de fecha 3 de diciembre de 2008 y plazo consignados en el Anexo que forma parte de la presente decisión administrativa, bajo el régimen del Artículo 9° del Anexo de la ley precitada, en el ámbito de la SUBSECRETARIA DE COORDINACION TECNICA Y ADMINISTRATIVA del MINISTERIO DE AGRICULTURA, GANADERIA Y PESCA.

Art. 2° — Comuníquese, publíquese, dése a la Dirección Nacional del Registro Oficial y archívese. — Juan M. Abal Medina. — Norberto G. Yauhar.

ANEXO

Modalidad de Contratación: LEY 25.164

Nombre del Proyecto: 0000001180 INDIVIDUALES DE LA SUBSECRETARIA DE COORDINACION TECNICA Y ADMINISTRATIVA

Código de Control: 0000017898

Listado de Contrataciones

N°	Apellido	Nombre	Tipo y N° Doc.	NyG	Desde	Hasta	Prog.	Act.	Dedic.
1	ROMERO	LUISA GRACIELA	DNI 12472383	B4	01/03/2012	31/12/2012	1	1	100%

Cantidad de Contratos Listados: 1

Imputación Presupuestaria: 1 81 Proyecto: 0 Fuente: 11 Ubic. Geo.: 2 Jurisdicción: 52

MINISTERIO DE JUSTICIA Y DERECHOS HUMANOS

Decisión Administrativa 653/2013

Facúltase al Ministro de Justicia y Derechos Humanos a aprobar cargos de Conducción.

Bs. As., 26/8/2013

VISTO el Expediente N° S04:0064734/2012 del registro del MINISTERIO DE JUSTICIA Y DERECHOS HUMANOS, los Decretos Nros. 1755 del 23 de octubre de 2008 y modificatorios, 936 del 5 de julio de 2011 y 1486 del 23 de setiembre de 2011 y sus modificatorios, la Resolución M.J. y D.H. N° 731 del 4 de mayo de 2012, y

CONSIDERANDO:

Que por el Decreto N° 1486/11 y sus modificatorios se aprobó la estructura organizativa de primer nivel operativo del MINISTERIO DE JUSTICIA Y DERECHOS HUMANOS.

Que de acuerdo a lo establecido en el artículo 2° del citado Decreto, mantiene su vigencia las unidades organizativas de segundo nivel operativo aprobadas por el Decreto N° 1755/08 y modificatorios.

Que a efectos de fortalecer institucionalmente las tareas llevadas a cabo por la OFICINA DE MONITOREO DE PUBLICACION DE AVISOS DE OFERTA DE COMERCIO SEXUAL, creada por el Decreto N° 936/11, y por el PROGRAMA NACIONAL DE RESCATE Y ACOMPAÑAMIENTO A LAS PERSONAS DAMNIFICADAS POR EL DELITO DE TRATA, creado por Resolución M.J. y D.H. N° 731/12, resulta conveniente la creación de DOS (2) cargos de conducción en la estructura organizativa del citado Ministerio.

Que el fortalecimiento de las citadas áreas, ambas dependientes de la SUBSECRETARIA DE POLITICA CRIMINAL de la SECRETARIA DE JUSTICIA del MINISTERIO DE JUSTICIA Y DERECHOS HUMANOS, responde a la necesidad de dar respuesta en forma sistemática y coordinada a los temas referidos a la trata de personas, en el marco de las acciones

emprendidas por el Gobierno Nacional en la materia, para llevar adelante tanto acciones de prevención como de rescate y acompañamiento a las personas víctimas de ese delito.

Que, por otra parte, deviene necesaria la creación de un cargo de conducción en el ámbito de la SECRETARIA DE DERECHOS HUMANOS del MINISTERIO DE JUSTICIA Y DERECHOS HUMANOS con el objeto de profundizar todas aquellas manifestaciones culturales tendientes a la promoción de los Derechos Humanos, como así también el desarrollo de recursos de exposición y difusión que permitan la comprensión, por parte del público, de la importancia del desarrollo de las políticas de Derechos Humanos, Memoria, Verdad y Justicia en sus aspectos históricos, culturales, políticos y sociales.

Que la medida propiciada contribuirá a lograr un adecuado cumplimiento de los criterios de eficacia y eficiencia necesarios para el logro de los objetivos estratégicos establecidos para el MINISTERIO DE JUSTICIA Y DERECHOS HUMANOS.

Que, en consecuencia, resulta necesaria la creación de DOS (2) cargos de conducción en la estructura organizativa de nivel inferior al primer nivel operativo, en el ámbito de SUBSECRETARIA DE POLITICA CRIMINAL de la SECRETARIA DE JUSTICIA Y UN (1) cargo de conducción en el ámbito de la SUBSECRETARIA DE PROMOCION DE DERECHOS HUMANOS de la SECRETARIA DE DERECHOS HUMANOS, ambas del MINISTERIO DE JUSTICIA Y DERECHOS HUMANOS.

Que con ello se propende a aumentar la capacidad de respuesta de la mencionada cartera ministerial a las demandas que la sociedad produce.

Que la DIRECCION GENERAL DE ASUNTOS JURIDICOS del MINISTERIO DE

JUSTICIA Y DERECHOS HUMANOS y la OFICINA NACIONAL DE INNOVACION DE GESTION de la SUBSECRETARIA DE GESTION Y EMPLEO PUBLICO de la SECRETARIA DE GABINETE Y COORDINACION ADMINISTRATIVA de la JEFATURA DE GABINETE DE MINISTROS han tomado la intervención que les compete.

Que la SECRETARIA LEGAL Y TECNICA de la PRESIDENCIA DE LA NACION ha tomado la intervención de su competencia.

Que la presente medida se dicta en ejercicio de las facultades conferidas por el artículo 100, inciso 1) de la CONSTITUCION NACIONAL, el artículo 16, inciso 12) de la Ley de Ministerios N° 22.520 (texto ordenado por Decreto N° 438/92) y sus modificatorias y el artículo 7° del Decreto N° 21 del 10 de diciembre de 2007.

Por ello,

EL JEFE
DE GABINETE DE MINISTROS
DECIDE:

Artículo 1° — Facúltase al señor Ministro de Justicia y Derechos Humanos a aprobar DOS (2) cargos de conducción en el ámbito de la SUBSECRETARIA DE POLITICA CRIMINAL de la SECRETARIA DE JUSTICIA y UN (1) cargo de conducción en el ámbito de la SUBSECRETARIA DE PROMOCION DE DERECHOS HUMANOS de la SECRETARIA DE DERECHOS HUMANOS, ambas del MINISTERIO DE JUSTICIA Y DERECHOS HUMANOS.

Art. 2° — El gasto que demande la presente medida será atendido con los créditos presupuestarios de la Jurisdicción 40 - MINISTERIO DE JUSTICIA Y DERECHOS HUMANOS.

Art. 3° — Comuníquese, publíquese, dése a la DIRECCION NACIONAL DEL REGISTRO OFICIAL y archívese. — Juan M. Abal Medina. — Julio C. Alak.

MINISTERIO DEL INTERIOR Y TRANSPORTE

Decisión Administrativa 651/2013

Contrataciones en la Agencia Nacional de Seguridad Vial.

Bs. As., 26/8/2013

VISTO el Expediente N° S02:0039395/2012 del registro de la AGENCIA NACIONAL DE SEGURIDAD VIAL, Organismo Descentralizado actuante en la órbita del MINISTERIO DEL INTERIOR Y TRANSPORTE, la Ley Marco de Regulación de Empleo Público Nacional N° 25.164, la Ley N° 26.784, los Decretos N° 1421 del 8 de agosto de 2002 y N° 2098 del 3 de diciembre de 2008, las Decisiones Administrativas N° 3 del 21 de enero de 2004 y sus modificatorias, y N° 1 del 10 de enero de 2012, y la Resolución N° 48 del 30 de diciembre de 2002, de la entonces SUBSECRETARIA DE LA GESTION PUBLICA de la JEFATURA DE GABINETE DE MINISTROS y sus modificatorias, y

CONSIDERANDO:

Que mediante las actuaciones citadas en el Visto, la AGENCIA NACIONAL DE SEGURIDAD VIAL solicita la excepción prevista en el último párrafo del artículo 9°, del Anexo I al Decreto N° 1421/02, reglamentario de la Ley Marco de Regulación de Empleo Público Nacional N° 25.164, a efectos de contratar a las personas que se detallan en el Anexo I adjunto a la presente.

Que el último párrafo del artículo 9° del Anexo I al Decreto N° 1421/02 prevé que el Jefe de Gabinete de Ministros podrá autorizar excepciones a los requisitos mínimos previstos para la equiparación escalafonaria mediante decisión fundada y a requerimiento del titular de la Jurisdicción u Organismo Descentralizado.

Que la creciente complejidad de las misiones y funciones de la AGENCIA NACIONAL DE SEGURIDAD VIAL, hace aconsejable fortalecer y complementar la labor que desarrolla dicho Organismo, resultando necesario celebrar las contrataciones que se propician.

Que las personas involucradas en la presente medida resultan imprescindibles para la consecución de tales fines y misiones, reuniendo los requisitos de idoneidad necesarios para cumplir las tareas que la operatoria del citado Organismo requiere.

Que el artículo 1° de la Decisión Administrativa N° 3/04 establece que el personal contratado percibirá una remuneración mensual equivalente al nivel o categoría del régimen escalafonario aplicable al personal de Planta Permanente de la Jurisdicción u Organismo Descentralizado contratante al que corresponde equipararlo según el tipo de funciones a desarrollar.

Que la financiación de los contratos que se aprueban por la presente, será atendida con cargo a las partidas específicas de los créditos presupuestarios de la Jurisdicción 30

- MINISTERIO DEL INTERIOR Y TRANSPORTE - O.D. 203 - AGENCIA NACIONAL DE SEGURIDAD VIAL, de conformidad con la Ley N° 26.784.

Que han tomado la intervención de su competencia la DIRECCION DE ASUNTOS LEGALES Y JURIDICOS de la AGENCIA NACIONAL DE SEGURIDAD VIAL y la DIRECCION GENERAL DE ASUNTOS JURIDICOS del MINISTERIO DEL INTERIOR Y TRANSPORTE.

Que la presente se dicta en ejercicio de las facultades conferidas por el artículo 100, inciso 2 de la CONSTITUCION NACIONAL y el último párrafo del artículo 9° del Anexo I al Decreto N° 1421/02, reglamentario de la Ley Marco de Regulación de Empleo Público Nacional N° 25.164.

Por ello,

EL JEFE
DE GABINETE DE MINISTROS
DECIDE:

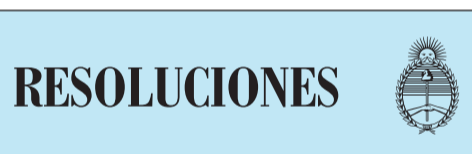
Artículo 1° — Exceptúanse a las personas incluidas en el Anexo I, que forma parte integrante de la presente, de lo establecido en el inciso c), punto II del artículo 9° del Anexo I al Decreto N° 1421 del 8 de agosto de 2002, reglamentario de la Ley Marco de Regulación de Empleo Público Nacional N° 25.164, al solo efecto de posibilitar su contratación en el ámbito de la AGENCIA NACIONAL DE SEGURIDAD VIAL, Organismo Descentralizado actuante en la órbita del MINISTERIO DEL INTERIOR Y TRANSPORTE, equiparándolas por el período y al Nivel y Grado del SISTEMA NACIONAL DE EMPLEO PUBLICO (SINEP), aprobado por Decreto N° 2098 del 3 de diciembre de 2008, conforme el régimen previsto en el artículo 9° del Anexo a la Ley N° 25.164, de acuerdo con el detalle obrante en el Anexo I de la presente.

Art. 2° — Comuníquese, publíquese, dése a la DIRECCION NACIONAL DEL REGISTRO OFICIAL y archívese. — Juan M. Abal Medina. — Aníbal F. Randazzo.

ANEXO I

TIEMPO DETERMINADO: Desde las fechas que en cada caso se consignan hasta el 31 de diciembre de 2012.

APELLIDO	NOMBRES	TD	N°	NIVEL	GRADO	TIEMPO DETERMINADO DESDE:
ARROYO	MATIAS NICOLAS	DNI	26.485.719	D	0	14 de diciembre de 2012
CIPOLLONI	DARIO OMAR	DNI	32.686.160	D	0	12 de diciembre de 2012
TABOADA	MARTIN RAFAEL	DNI	18.380.039	C	0	12 de diciembre de 2012
YNSFRAN	OSMAR ALBERTO	DNI	18.299.343	D	0	12 de diciembre de 2012



Administración Federal
de Ingresos Públicos

ADUANAS

Resolución General 3524

Premio a la Innovación Aduanera - "Cadenas logísticas mundiales eficientes, seguras, transparentes y resistentes". Su implementación.

Bs. As., 28/8/2013

VISTO la Actuación SIGEA N° 12048-763-2013 del Registro de esta Administración Federal, y

CONSIDERANDO:

Que esta Administración Federal de Ingresos Públicos es anfitriona del 4to. Foro de Innovación y Tecnología a realizarse —por primera vez en el continente americano— del 12 al 14 de noviembre del corriente año en la Ciudad Autónoma de Buenos Aires de la República Argentina.

Que, en esta edición, la temática del Foro se centra en el aprovechamiento de la tecnología para construir cadenas logísticas mundiales eficientes, seguras, transparentes y resistentes.

Que la temática abordada concuerda con el lema de la Organización Mundial de Aduanas (OMA) para este año, "Innovación para el progreso aduanero".

Que resulta propicia la oportunidad para generar un espacio de reflexión sobre los desafíos y riesgos evolutivos y emergentes que enfrenta la gestión aduanera y

buscar alternativas creativas e innovadoras para abordar esa realidad compleja y dinámica.

Que la implementación de este premio es un reconocimiento que esta Administración Federal efectúa al valor innovación, afirmando el compromiso estratégico de fortalecer los intercambios internacionales de ideas, experiencias y casos exitosos en el ámbito aduanero.

Que han tomado la intervención que les compete la Dirección de Legislación, la Subdirección General de Asuntos Jurídicos y la Dirección General de Aduanas.

Que la presente se dicta en ejercicio de las facultades conferidas por el Artículo 7° del Decreto N° 618 del 10 de julio de 1997, sus modificatorios y sus complementarios.

Por ello,

EL ADMINISTRADOR FEDERAL
DE LA ADMINISTRACION FEDERAL
DE INGRESOS PUBLICOS
RESUELVE:

Artículo 1° — Institúyese el "Premio a la Innovación Aduanera - Cadenas logísticas mundiales eficientes, seguras, transparentes y resistentes", a efectos de fomentar espacios creativos donde tenga lugar el surgimiento de nuevas formas de hacer, ser un catalizador para la innovación y promover el intercambio de ideas, experiencias y casos exitosos que resulten originales en el contexto del control aduanero.

Art. 2° — Las bases y condiciones generales del premio y los requisitos para la presentación de la "Propuesta Premio a la Innovación Aduanera" se consignan, respectivamente, en los

Anexos I y II que se aprueban y forman parte de la presente.

Art. 3° — A efectos de la implementación operativa de este premio deberán intervenir, en coordinación con la Dirección General de Aduanas y en el ámbito de sus respectivas competencias, las siguientes áreas:

a) Dirección de Asuntos Internacionales, Dirección de Secretaría General y División Fortalecimiento, todas ellas de la Subdirección General de Coordinación Técnico Institucional.

b) Subdirección General de Sistemas y Telecomunicaciones.

Art. 4° — La presente entrará en vigencia a partir del día hábil administrativo inmediato siguiente al de su publicación en el Boletín Oficial, inclusive.

Art. 5° — Regístrese y dése a la Dirección Nacional del Registro Oficial para su publicación. Remítase copia a la Secretaría Administrativa del MERCOSUR -Sección Nacional-, a la Secretaría del Convenio Multilateral sobre Cooperación y Asistencia Mutua entre las Direcciones de Aduanas de América Latina, España y Portugal (México D.F.), a la Secretaría de la Organización Mundial de Aduanas y a la Vicepresidencia Regional de las Américas y el Caribe (OMA). Cumplido, archívese. — Ricardo Echegaray.

ANEXO I (Artículo 2°)

BASES Y CONDICIONES GENERALES

"PREMIO A LA INNOVACION ADUANERA"

CADENAS LOGISTICAS MUNDIALES
EFICIENTES, SEGURAS, TRANSPARENTES
Y RESISTENTES

I.- INTRODUCCION

La Administración Federal de Ingresos Públicos es anfitriona del 4to. Foro de Innovación y Tecnología a realizarse —por primera vez en el continente americano— del 12 al 14 de noviembre del corriente año en la Ciudad Autónoma de Buenos Aires de la República Argentina.

La temática del Foro de esta edición se centra en el aprovechamiento de la tecnología para construir cadenas logísticas mundiales eficientes, seguras, transparentes y resistentes, en línea con el lema de la Organización Mundial de Aduanas (OMA) para este año, "Innovación para el progreso aduanero".

Esta oportunidad resulta propicia para generar un espacio de reflexión sobre los desafíos y riesgos evolutivos y emergentes que enfrenta la gestión aduanera y cómo buscar alternativas creativas e innovadoras para abordar esa realidad compleja y dinámica.

En este sentido, el Premio a la Innovación Aduanera nace con el propósito de fomentar espacios creativos donde tenga lugar el surgimiento de nuevas formas de hacer, ser un catalizador para la innovación y promover el intercambio de ideas, experiencias y casos exitosos que resulten originales en el contexto del control aduanero.

La innovación como motor del progreso aduanero es un activo clave que hay que estimular para lograr respuestas más eficaces y eficientes, alcanzar los resultados esperados y los impactos positivos, aumentar la productividad y el rendimiento de los recursos disponibles y fortalecer las capacidades de las administraciones a través de un proceso de mejora continua.

Este premio refleja el reconocimiento del valor de la innovación por parte de esta Administración Federal y el compromiso con fortalecer los intercambios internacionales como factor clave para el aprovechamiento de la innovación y su mayor rendimiento a través de la unificación de esfuerzos.

II.- PARTICIPANTES

- Universidades extranjeras que tengan carreras afines al comercio exterior y la tecnología en su oferta académica.

- Organismos extranjeros con los que esta Administración Federal lleva adelante una gestión coordinada de frontera.

III.- FORMA DE PARTICIPAR

Se deberá presentar un trabajo sobre el tema general de "innovación en la cadena de suministros" el cual puede referirse de manera amplia a cualquier aspecto y proceso relacionado a la gestión de cadenas logísticas seguras, eficientes, transparentes y resistentes, siendo este el requisito excluyente.

Podrán seleccionarse procesos internos de la administración o aquellos que involucren alianzas estratégicas con el sector privado, académico y gubernamental así como con otras aduanas y organismos con los cuales se desarrolla una gestión coordinada de fronteras.

Las áreas temáticas para seleccionar son amplias, pudiendo involucrar cuestiones legales, procedimentales, de uso e intercambio de la información, de tecnología aplicada al control, de sistemas de información, de gestión y procesos de trabajo, de gestión del riesgo, de administración de recursos, entre otros.

El trabajo deberá referirse a innovaciones implementadas que hayan demostrado cambios en la gestión de la cadena logística con resultados e impactos positivos demostrables que puedan reflejarse en mediciones cualitativas y cuantitativas a partir de la implementación (históricas si se ha implementado o esperadas si es a futuro).

El trabajo debe cumplir con el formato del Anexo "Propuesta Premio a la Innovación Aduanera" en formato PDF. El mismo podrá presentarse en idioma español o inglés.

IV.- PRESENTACION DE LOS TRABAJOS.

Las propuestas serán recibidas hasta antes de las CERO HORAS (00:00 hs) del 21/09/2013, por correo electrónico a: fortalecimiento@afip.gob.ar indicando en el asunto: "Propuesta para el Premio a la Innovación Aduanera".

V.- EVALUACION Y SELECCION DE GANADORES.

La evaluación de los trabajos será realizada por un Comité Evaluador que estará compuesto por un representante de la Subdirección General de Sistemas y Telecomunicaciones de la Administración Federal de Ingresos Públicos, de la Dirección General de Aduanas y del Consejo Consultivo Aduanero (CDA).

El eje de la evaluación estará sobre aquellas innovaciones que reporten mayor valor agregado a la gestión de la cadena logística. Por ello, serán variables importantes la evaluación de los impactos y resultados positivos alcanzados que pueden ser demostrados cualitativa y cuantitativamente, los costos asumidos y la sustentabilidad de la iniciativa así como el potencial de mayores desarrollos.

Los resultados serán notificados en la semana del 7 al 11 de octubre del corriente año.

VI.- PREMIO PARA EL GANADOR. El premio consistirá en:

- Inscripción al Foro (equivalente a TRES-CIENTOS EUROS (€ 300.-)) para asistir al 4to. Foro de Innovación y Tecnología de la OMA.

- Pasajes aéreos internacionales.

- Alojamiento en la República Argentina durante los días en que se desarrolle el Foro.

- El trabajo ganador será publicado para su difusión y conocimiento.

ANEXO II (Artículo 2°)

REQUISITOS PARA LA PRESENTACION

"Propuesta Premio a la Innovación Aduanera"

Universidad/ Organismo que representa:

Título del trabajo:

Tema seleccionado:

Fecha de implementación:

Autor/res y datos de contacto:

1. Breve presentación de la innovación describiendo la sustancia de la innovación y su importancia (50 palabras máximo).

2. Descripción de la innovación (500 palabras máximo).

2.1. Problemas/oportunidades a los que está dirigida: ¿Cuál es el problema/oportunidad que dio origen a la iniciativa innovadora?

2.2. ¿En qué consiste precisamente la innovación?

2.3. Destacar lo original de la propuesta, su vinculación con los objetivos que persigue y el diagnóstico inicial (problemas/oportunidades).

3. Presentación de los resultados, logros e impactos más significativos alcanzados mediante la implementación de la innovación (250 palabras máximo).

3.1. Descripción del tipo de resultado y logros alcanzados.

3.2. Presentación precisa de los resultados y logros verificables cualitativa y cuantitativamente.

Administración Federal de Ingresos Públicos

EXPORTACIONES

Resolución General 3523

Cueros y pieles en bruto de la Partida 41.01 del Sistema Armonizado de Designación y Codificación de Mercancías. Aduanas especializadas.

Bs. As., 28/8/2013

VISTO la Resolución General N° 1.399, y

CONSIDERANDO:

Que la citada resolución general aprobó las normas relativas a la participación presencial de entidades privadas en la verificación efectuada por el servicio aduanero en las destinaciones de exportación de cueros.

Que representantes del sector privado, incluidos en la nómina prevista en el Anexo III de la aludida Resolución General N° 1.399, efectuaron determinados planteos con relación al incremento de las exportaciones de cueros salados sin procesamiento industrial.

Que en virtud del análisis realizado y en concordancia con las pautas establecidas por la Organización Mundial de Aduanas (OMA) se estima conveniente adoptar medidas relativas a las destinaciones de exportación que involucren mercaderías consideradas escasas y sensibles, evitando producir demoras injustificadas en la cadena logística del comercio exterior.

Que han tomado la intervención que les compete la Dirección de Legislación, las Subdirecciones Generales de Asuntos Jurídicos, Técnico Legal Aduanera, de Recaudación y de Sistemas y Telecomunicaciones y la Dirección General de Aduanas.

Que la presente se dicta en ejercicio de las facultades conferidas por el Artículo 7° del Decreto N° 618 del 10 de julio de 1997, sus modificatorios y sus complementarios.

Por ello,

EL ADMINISTRADOR FEDERAL DE LA ADMINISTRACION FEDERAL DE INGRESOS PUBLICOS RESUELVE:

Artículo 1° — Las destinaciones de exportación de las mercaderías comprendidas en la Partida 41.01 del Sistema Armonizado de Designación y Codificación de Mercancías deberán ser oficializadas y controladas con carácter obligatorio en las aduanas consignadas en el Anexo que se aprueba y forma parte de la presente, a efectos de permitir al servicio aduanero y demás organismos competentes efectuar los controles pertinentes conforme a la normativa vigente.

Art. 2° — Lo dispuesto en el artículo precedente será de aplicación para las solicitudes de destinaciones de exportación que se oficialicen a partir del décimo día hábil administrativo, inclusive, posterior al de publicación de la presente en el Boletín Oficial.

Art. 3° — Regístrese, dése a la Dirección Nacional del Registro Oficial para su publicación y publíquese en el Boletín de la Dirección General de Aduanas. Cumplido, archívese. — Ricardo Echegaray.

ANEXO (Artículo 1°)

NOMINA DE ADUANAS

Código	Aduanas
001	BUENOS AIRES
016	CONCORDIA
017	CORDOBA
073	EZEIZA



BOLETIN OFICIAL DE LA REPUBLICA ARGENTINA

SUSCRÍBASE ANUALMENTE

Edición Gráfica



Primera Sección **\$670**
Legislación y Avisos Oficiales

Segunda Sección **\$950**
Contratos sobre Personas Jurídicas, Convocatorias y Avisos Comerciales, Edictos Judiciales, Partidos Políticos, Información y Cultura

Tercera Sección **\$980**
Contrataciones del Estado

CENTRO DE ATENCIÓN AL CLIENTE
0810-345-BORA (2672)

www.boletinoficial.gob.ar

Ventas / Ciudad Autónoma de Buenos Aires

Sede Central: Suipacha 767 (9:30 a 16:00hs.) Tel.: (011) 5218-8400.

Delegación Tribunales: Libertad 469 (8:30 a 14:30 hs.) Tel.: (011) 4379-1979.

Delegación Colegio Público de Abogados: Av. Corrientes 1441. Entrepiso (10:00 a 15:45 hs.) Tel.: (011) 4379-8700 (int. 236).

Delegación Inspección General de Justicia: Moreno 251 (8.30 a 11.30 hs.) Tel.: (011) 4343-0732/2419/0947 (int. 6074).

Delegación Consejo Profesional de Ciencias Económicas: Viamonte 1549. Planta Baja (12:00 a 17:00 hs.) Tel.: (011) 5382-9535.

DISPOSICIONES



Política de
Seguridad de la Información
Modelo

Oficina Nacional de Tecnologías de Información

ADMINISTRACION PUBLICA NACIONAL

Disposición 3/2013

Apruébase la "Política de Seguridad de la Información Modelo".

Bs. As., 27/8/2013

VISTO el Expediente CUDAP: EXP-JGM: 50449/2011 del Registro de la JEFATURA DE GABINETE DE MINISTROS, el Decreto N° 378 del 27 de abril de 2005, la Decisión Administrativa N° 669 del 20 de diciembre de 2004 de la JEFATURA DE GABINETE DE MINISTROS, la Resolución N° 45 de fecha 24 de junio de 2005 de la entonces SUBSECRETARIA DE LA GESTION PUBLICA, la Disposición N° 6 de fecha 8 de agosto de 2005 de la OFICINA DE TECNOLOGIAS DE INFORMACION, y

CONSIDERANDO:

Que el Decreto N° 378/05 aprobó los Lineamientos Estratégicos que deberán regir el Plan Nacional de Gobierno Electrónico y los Planes Sectoriales de Gobierno Electrónico de los Organismos de la ADMINISTRACION PUBLICA NACIONAL a fin de promover el empleo eficiente y coordinado de los recursos de las Tecnologías de la Información y las Comunicaciones.

Que la Decisión Administrativa N° 669/04 de la JEFATURA DE GABINETE DE MINISTROS estableció en su artículo 1° que los organismos del Sector Público Nacional comprendidos en el artículo 7° de la citada medida deberán dictar o bien adecuar sus políticas de seguridad de la información conforme a la Política de Seguridad Modelo a dictarse dentro del plazo de CIENTO OCHENTA (180) días de aprobada dicha Política de Seguridad Modelo.

Que el artículo 8° de la mencionada Decisión Administrativa, facultó al entonces señor SUBSECRETARIO DE LA GESTION PUBLICA de la JEFATURA DE GABINETE DE MINISTROS a aprobar la Política de Seguridad Modelo y a dictar las normas aclaratorias y complementarias de la citada medida, pudiendo dicha autoridad delegar en el DIRECTOR NACIONAL DE LA OFICINA NACIONAL DE TECNOLOGIAS DE INFORMACION las facultades aludidas.

Que consecuentemente el artículo 1° de la Resolución de la ex SUBSECRETARIA DE GESTION PUBLICA N° 45/05 de la JEFATURA DE GABINETE DE MINISTROS facultó al señor DIRECTOR NACIONAL de la OFICINA NACIONAL DE TECNOLOGIAS DE INFORMACION a aprobar la Política de Seguridad de la Información Modelo y dictar las normas aclaratorias y complementarias que requiera la aplicación de la Decisión Administrativa JGM N° 669/2004.

Que la Disposición N° 6/05 de la OFICINA NACIONAL DE TECNOLOGIAS DE INFORMACION de la SUBSECRETARIA DE TECNOLOGIAS DE GESTION de la SECRETARIA DE GABINETE Y COORDINACION ADMINISTRATIVA de la JEFATURA DE GABINETE DE MINISTROS en su artículo 1° aprobó la "Política de Seguridad de la Información Modelo" ordenada por la Decisión Administrativa JGM N° 669/04, y que sirve como base para la elaboración de las respectivas políticas a dictarse por cada organismo alcanzado por la citada norma.

Que atento al incremento en cantidad y variedad de amenazas y vulnerabilidades que rodean a los activos de información, la "Política de Seguridad Modelo" oportunamente aprobada requiere ser actualizada a fin de mantener su vigencia y nivel de eficacia.

Que la mera elaboración por parte de los organismos de políticas de seguridad no es suficiente para garantizar la seguridad de la información, la que permite a su vez, garantizar la prestación continua e ininterrumpida de los diversos servicios públicos prestados por dichos organismos.

Que sólo a través de la efectiva implementación de las medidas contempladas en dichas políticas se podrá proteger acabadamente los recursos de información de los organismos como así también la tecnología utilizada para su procesamiento.

Que ha tomado la intervención de su competencia la DIRECCION GENERAL DE ASUNTOS JURIDICOS de la SUBSECRETARIA DE COORDINACION ADMINISTRATIVA de la SECRETARIA DE GABINETE y COORDINACION ADMINISTRATIVA de la JEFATURA DE GABINETE DE MINISTROS.

Que la presente medida se dicta en ejercicio de las facultades conferidas por el artículo 1° de la Resolución de la ex SUBSECRETARIA DE GESTION PUBLICA N° 45/05.

Por ello,

EL DIRECTOR NACIONAL
DE LA OFICINA NACIONAL DE TECNOLOGIAS DE INFORMACION
DISPONE:

Artículo 1° — Apruébase la "Política de Seguridad de la Información Modelo", que reemplaza a los mismos fines a la aprobada por Disposición ONTI N° 6/2005, que como Anexo I forma parte integrante de la presente.

Art. 2° — Las disposiciones de la Política de Seguridad de la Información Modelo servirán como base para la elaboración de las respectivas políticas a dictarse por cada organismo alcanzado por la Decisión Administrativa N° 669/2004, debiendo ser interpretada como un compendio de mejores prácticas en materia de seguridad de la información para las entidades, públicas y adaptada a la realidad y recursos de cada organismo.

Art. 3° — Las funciones a las que hace alusión la Política de Seguridad Modelo deberán ser asignadas de acuerdo a las particularidades y operatoria de cada organismo. Dicha asignación deberá realizarse evitándose la duplicación de tareas y asegurando la segregación de funciones incompatibles siempre que sea posible, o bien mediante la implementación de controles para mitigar dicho riesgo.

Art. 4° — Comuníquese, publíquese, dése a la Dirección Nacional del Registro Oficial y archívese. — Pedro Janices.

INDICE

Tabla de contenido

- 1 Introducción
 - 1.1 Alcance
 - 1.2 Qué es seguridad de la información?
 - 1.3 ¿Por qué es necesario?
 - 1.4 Requerimientos de seguridad
 - 1.5 Evaluación de los riesgos de seguridad
 - 1.6 Selección de controles
 - 1.7 ¿Cómo empezar?
 - 1.8 Factores críticos de éxito
- 2 Términos y Definiciones
 - 2.1 Seguridad de la Información
 - 2.2 Evaluación de Riesgos
 - 2.2 Tratamiento de Riesgos
 - 2.3 Gestión de Riesgos
 - 2.4 Comité de Seguridad de la Información
 - 2.5 Responsable de Seguridad de la Información
 - 2.6 Incidente de Seguridad
 - 2.8 Riesgo
 - 2.9 Amenaza
 - 2.10 Vulnerabilidad
 - 2.11 Control
3. Estructura de la política Modelo
4. Evaluación y tratamiento de riesgos
 - 4.1 Evaluación de los riesgos de seguridad
 - 4.2 Tratamiento de riesgos de seguridad
5. Cláusula: Política de Seguridad de la Información
 - 5.1 Categoría: Política de Seguridad de la información
 - 5.1.1 Control: Documento de la política de seguridad de la información
 - 5-1-2 Control: Revisión de la política de seguridad de la información
6. Cláusula: Organización
 - 6.1 Categoría: Organización interna
 - 6.1.1 Control: Compromiso de la dirección con la seguridad de la información
 - 6-1-2 Control: Coordinación de la seguridad de la información
 - 6-1-3 Control: Asignación de responsabilidades de la seguridad de la información
 - 6-1-4 Control: Autorización para Instalaciones de Procesamiento de Información
 - 6-1-5 Control: Acuerdos de confidencialidad
 - 6-1-6 Control: Contacto con otros organismos
 - 6-1-7 Control: Contacto con grupos de interés especial
 - 6-1-8 Control: Revisión independiente de la seguridad de la información
 - 6.2 Categoría: Grupos o personas externas
 - 6.2.1 Control: Identificación de los riesgos relacionados con grupos externos
 - 6-2-2 Control: Puntos de seguridad de la información a considerar en Contratos o Acuerdos con terceros
 - 6-2-3 Control: Puntos de Seguridad de la Información a ser considerados en acuerdos con terceros
7. Cláusula: Gestión de Activos
 - 7.1 Categoría: Responsabilidad sobre los activos
 - 7.1.1 Control: Inventario de activos
 - 7.1.2 Control: Propiedad de los activos
 - 7.1.3 Control: Uso aceptable de los activos
 - 7.2 Categoría: Clasificación de la información
 - 7.2.1 Control: Directrices de clasificación
 - 7.2.2 Control: Etiquetado y manipulado de la información
8. Cláusula: Recursos Humanos
 - 8.1 Categoría: Antes del empleo
 - 8.1.1 Control: Funciones y responsabilidades
 - 8.1.2 Control: Investigación de antecedentes
 - 8.1.3 Control: Términos y condiciones de contratación
 - 8.2 Categoría: Durante el empleo
 - 8.2.1 Control: Responsabilidad de la dirección
 - 8.2.2 Control: Concientización, formación y capacitación en seguridad de la información
 - 8.2.3 Control: Proceso disciplinario
 - 8.3 Categoría: Cese del empleo o cambio de puesto de trabajo
 - 8.3.1 Control: Responsabilidad del cese o cambio
 - 8.3.2 Control: Devolución de activos
 - 8.3.3 Control: Retiro de los derechos de acceso
9. Cláusula: Física y Ambiental
 - 9.1 Categoría: Areas Seguras
 - 9.1.1 Control: Perímetro de seguridad física
 - 9.1.2 Control: Controles físicos de entrada
 - 9.1.3 Control: Seguridad de oficinas, despachos, instalaciones
 - 9.1.4 Control: Protección contra amenazas externas y de origen ambiental
 - 9.1.5 Control: Trabajo en áreas seguras
 - 9.1.6 Control: Areas de acceso público, de carga y descarga
 - 9.2 Categoría: Seguridad de los equipos
 - 9.2.1 Control: emplazamiento y protección de equipos
 - 9.2.2 Control: Instalaciones de suministro
 - 9.2.3 Control: Seguridad del cableado
 - 9.2.4 Control: Mantenimiento de los equipos
 - 9.2.5 Control: Seguridad de los equipos fuera de las instalaciones
 - 9.2.6 Control: Reutilización o retiro seguro de equipos
 - 9.2.7 Control: Retirada de materiales propiedad de la empresa
 - 9.2.8 Políticas de Escritorios y Pantallas Limpias

10. Cláusula: Gestión de Comunicaciones y Operaciones
- 10.1 Categoría: Procedimientos y Responsabilidades Operativas
- 10.1.1 Control: Documentación de los Procedimientos Operativos
- 10.1.2 Control: Cambios en las Operaciones
- 10.1.3 Control: Separación de Funciones
- 10.1.4 Control: Separación entre Instalaciones de Desarrollo e Instalaciones Operativas
- 10.2 Categoría: Gestión de Provisión de Servicios
- 10.2.1 Control: Provisión de servicio
- 10.2.2 Control: Seguimiento y revisión de los servicios de las terceras partes
- 10.2.3 Control: Gestión del cambio de los servicios de terceras partes
- 10.3 Categoría: Planificación y Aprobación de Sistemas
- 10.3.1 Control: Planificación de la Capacidad
- 10.3.2 Control: Aprobación del Sistema
- 10.4 Categoría: Protección Contra Código Malicioso
- 10.4.1 Control: Código Malicioso
- 10.4.2 Control: Código Móvil
- 10.5 Categoría: Respaldo o Back-up
- 10.5.1 Control: Resguardo de la Información
- 10.5.2 Control: Registro de Actividades del Personal Operativo
- 10.5.3 Control: Registro de Fallas
- 10.6 Categoría: Gestión de la Red
- 10.6.1 Control: Redes
- 10.7 Categoría: Administración y Seguridad de los medios de almacenamiento
- 10.7.1 Control: Administración de Medios Informáticos Removibles
- 10.7.2 Control: Eliminación de Medios de Información
- 10.7.3 Control: Procedimientos de Manejo de la Información
- 10.7.4 Control: Seguridad de la Documentación del Sistema
- 10.8 Categoría: Intercambios de Información y Software
- 10.8.1 Control: Procedimientos y controles de intercambio de la información
- 10.8.2 Control: Acuerdos de Intercambio de Información y Software
- 10.8.3 Control: Seguridad de los Medios en Tránsito
- 10.8.4 Control: Seguridad de los la Mensajería
- 10.8.5 Control: Seguridad del Gobierno Electrónico
- 10.9 Categoría: Seguridad del Correo Electrónico
- 10.9.1 Control: Riesgos de Seguridad
- 10.9.2 Control: Política de Correo Electrónico
- 10.9.3 Control: Seguridad de los Sistemas Electrónicos de Oficina
- 10.9.4 Control: Sistemas de Acceso Público
- 10.9.5 Control: Otras Formas de Intercambio de Información
- 10.10 Categoría: Seguimiento y control
- 10.10.1 Control: Registro de auditoría
- 10.10.2 Control: Protección de los registros
- 10.10.3 Control: Registro de actividad de administrador y operador
- 10.10.4 Control: Sincronización de Relojes

11. Cláusula: Gestión de Accesos
- 11.1 Categoría: Requerimientos para el Control de Acceso
- 11.1.1 Control: Política de Control de Accesos
- 11.1.2 Control: Reglas de Control de Acceso
- 11.2 Categoría: Administración de Accesos de Usuarios
- 11.2.1 Control: Registración de Usuarios
- 11.2.2 Control: Gestión de Privilegios
- 11.2.3 Control: Gestión de Contraseñas de Usuario
- 11.2.4 Control: Administración de Contraseñas Críticas
- 11.2.5 Revisión de Derechos de Acceso de Usuarios
- 11.3 Categoría: Responsabilidades del Usuario
- 11.3.1 Control: Uso de Contraseñas
- 11.3.2 Control: Equipos Desatendidos en Areas de Usuarios
- 11.4 Categoría: Control de Acceso a la Red
- 11.4.1 Control: Política de Utilización de los Servicios de Red
- 11.4.2 Control: Camino Forzado
- 11.4.3 Control: Autenticación de Usuarios para Conexiones Externas
- 11.4.4 Control: Autenticación de Nodos
- 11.4.5 Control: Protección de los Puertos (Ports) de Diagnóstico Remoto
- 11.4.6 Control: Subdivisión de Redes
- 11.4.7 Control: Acceso a Internet
- 11.4.8 Control: Conexión a la Red
- 11.4.9 Control: Ruteo de Red
- 11.4.10 Control: Seguridad de los Servicios de Red
- 11.5 Categoría: Control de Acceso al Sistema Operativo
- 11.5.1 Control: Identificación Automática de Terminales
- 11.5.2 Control: Procedimientos de Conexión de Terminales
- 11.5.3 Control: Identificación y Autenticación de los Usuarios
- 11.5.4 Control: Sistema de Administración de Contraseñas
- 11.5.5 Control: Uso de Utilitarios de Sistema
- 11.5.6 Control: Alarmas Silenciosas para la Protección de los Usuarios
- 11.5.7 Control: Desconexión de Terminales por Tiempo Muerto
- 11.5.8 Control: Limitación del Horario de Conexión
- 11.6 Categoría: Control de Acceso a las Aplicaciones
- 11.6.1 Control: Restricción del Acceso a la Información
- 11.6.2 Control: Aislamiento de los Sistemas Sensibles
- 11.7 Categoría: Monitoreo del Acceso y Uso de los Sistemas
- 11.7.1 Control: Registro de Eventos
- 11.7.2 Control: Procedimientos y Areas de Riesgo
- 11.8 Categoría: Dispositivos Móviles y Trabajo Remoto
- 11.8.1 Control: Computación Móvil
- 11.8.2 Control: Trabajo Remoto

12. Cláusula: Adquisición, desarrollo y mantenimiento de sistemas
- 12.1 Categoría: Requerimientos de Seguridad de los Sistemas
- 12.1.1 Control: Análisis y Especificaciones de los Requerimientos de seguridad
- 12.2 Categoría: Seguridad en los Sistemas de Aplicación
- 12.2.1 Validación de Datos de Entrada
- 12.2.2 Control: Controles de Procesamiento Interno
- 12.2.3 Control: Autenticación de Mensajes
- 12.2.4 Control: Validación de Datos de Salidas
- 12.3 Categoría: Controles Criptográficos
- 12.3.1 Control: Política de Utilización de Controles Criptográficos
- 12.3.2 Control: Cifrado
- 12.3.4 Control: Firma Digital
- 12.3.5 Control: Servicios de No Repudio
- 12.3.6 Control: Protección de claves criptográficas
- 12.3.7 Control: Protección de Claves criptográficas: Normas y procedimientos

- 12.4 Categoría: Seguridad de los Archivos del Sistema
- 12.4.1 Control: Software Operativo
- 12.4.2 Control: Protección de los Datos de Prueba del Sistema
- 12.4.3 Control: Cambios a Datos Operativos
- 12.4.4 Control: Acceso a las Bibliotecas de Programas fuentes
- 12.5 Categoría: Seguridad de los Procesos de Desarrollo y Soporte
- 12.5.1 Control Procedimiento de Control de Cambios
- 12.5.2 Control: Revisión Técnica de los Cambios en el sistema Operativo
- 12.5.3 control: Restricción del Cambio de Paquetes de Software
- 12.5.4 Control: Canales Ocultos y Código Malicioso
- 12.5.6 Control: Desarrollo Externo de Software
- 12.6 Categoría: Gestión de vulnerabilidades técnicas
- 12.6.1 Control: Vulnerabilidades técnicas

13. Cláusula: Gestión de Incidentes de Seguridad
- 13.1 Categoría: Informe de los eventos y debilidades de la seguridad
- 13.1.1 Reporte de los eventos de la seguridad de información
- 13.1.2 Reporte de las debilidades de la seguridad
- 13.1.3 Comunicación de Anomalías del Software
- 13.2 Categoría: Gestión de los Incidentes y mejoras de la seguridad
- 13.2.1 Control: Responsabilidades y procedimientos
- 13.2.2 Aprendiendo a partir de los incidentes de la seguridad de la información
- 13.2.3 Procesos Disciplinarios

14. Cláusula: Gestión de la Continuidad
- 14.1 Categoría: Gestión de continuidad del Organismo
- 14.1.1 Control: Proceso de Administración de la continuidad del Organismo
- 14.1.2 Control: Continuidad de las Actividades y Análisis de los impactos
- 14.1.3 Control: Elaboración e implementación de os planes de continuidad de las Actividades del Organismo
- 14.1.4 Control: Marco para la Planificación de la continuidad de las Actividades del Organismo
- 14.1.5 Control: Ensayo, Mantenimiento y Reevaluación de los Planes de continuidad del Organismo

15. Cláusula: Cumplimiento
- 15.1 Categoría: Cumplimiento de Requisitos Legales
- 15.1.1 Control: Identificación de la Legislación Aplicable
- 15.1.2 Control: Derechos de Propiedad Intelectual
- 15.1.3 Control: Protección de los Registros del Organismo
- 15.1.3 Control: Protección de Datos y Privacidad de la Información Personal
- 15.1.4 Control: Prevención del Uso Inadecuado de los Recursos de Procesamiento de Información
- 15.1.6 Regulación de Controles para el Uso de Criptografía
- 15.1.7 Recolección de Evidencia
- 15.1.8 Delitos Informáticos
- 15.2 Categoría: Revisiones de la Política de Seguridad y la Compatibilidad
- 15.2.1 Control: Cumplimiento de la Política de Seguridad
- 15.2.2 Verificación de la Compatibilidad Técnica
- 15.3 Consideraciones de Auditorías de Sistemas
- 15.3.1 Controles de Auditoría de Sistemas
- 15.3.2 Protección de los Elementos Utilizados por la Auditoría de Sistemas
- 15.3.3 Sanciones Previstas por Incumplimiento

1 Introducción

En diciembre de 2004, la DA N° 669/2004 de la Jefatura de Gabinete de Ministros estableció la obligatoriedad para los organismos del Sector Público Nacional (comprendidos en los incisos a) y c) del artículo 8° de la Ley N° 24.156 y sus modificatorias) de:

- Dictar una política de Seguridad de la Información conforme la Política de Seguridad Modelo, o adecuar sus Políticas de Seguridad conforme al Modelo aprobado.
- Conformar un Comité de Seguridad en la Información.
- Designar un coordinador del Comité de Seguridad de la Información.
- Establecer las funciones del Comité de Seguridad de la Información.

En 2005 mediante la Disposición N° 6/2005 de la Oficina Nacional de Tecnologías de Información se aprueba la primera "Política de Seguridad de la Información Modelo" y en septiembre del 2011 se procedió a realizar la actualización de aquel Modelo, en base a las actualizaciones sufridas por la norma ISO/IEC 27002 y la incorporación de temas como los que se mencionan a continuación:

Los aspectos clave de esta actualización son:

Fundamentales

- Compromiso y apoyo de la Dirección de la organización.
- Definición clara de un alcance apropiado.
- concientización y formación del personal.
- Evaluación de riesgos exhaustiva y adecuada a la organización.
- Compromiso de mejora continua.
- Establecimiento de políticas y normas.

- Organización y comunicación.

- Inclusión de la cláusula o dominio gestión de incidentes de seguridad

Factores críticos de éxito

- La concientización del empleado por la seguridad. Principal objetivo a conseguir.
- Realización de comités de dirección con descubrimiento continuo de no conformidades o acciones de mejora.
- Creación de un sistema de gestión de incidentes que recoja notificaciones continuas por parte de los usuarios (los incidentes de seguridad deben ser reportados y analizados).

- La seguridad absoluta no existe, se trata de reducir el riesgo a niveles asumibles.
- La seguridad no es un producto, es un proceso.
- La seguridad no es un proyecto, es una actividad continua y el programa de protección requiere el soporte de la organización para tener éxito.

- La seguridad debe ser inherente a los procesos de información y de la organización.

Riesgos

- Temor ante el cambio: resistencia de las personas.
- Discrepancias en los comités de dirección.
- Delegación de todas las responsabilidades en departamentos técnicos.
- No asumir que la seguridad de la información es inherente a los procesos de la organización.
- Planes de formación y concientización inadecuados.
- Definición poco clara del alcance.
- Exceso de medidas técnicas en detrimento de la formación, concientización y medidas de tipo organizativo.
- Falta de comunicación de los progresos al personal de la organización.

Se hace saber que queda expresamente prohibido el uso para fines comerciales del presente documento. Asimismo, las personas autorizadas para usar la "Política Modelo" podrán copiarla, modificarla y reproducirla únicamente para aquellos fines a los cuales está destinada.

El presente modelo podrá sufrir modificaciones futuras, de acuerdo a las novedades que se registren en la materia que trata, las cuales serán debidamente aprobadas y comunicadas.

1.1 Alcance

La presente Política de Seguridad de la Información se dicta en cumplimiento de las disposiciones legales vigentes, con el objeto de gestionar adecuadamente la seguridad de la información, los sistemas informáticos y el ambiente tecnológico del Organismo.

Debe ser conocida y cumplida por toda la planta de personal del Organismo, tanto se trate de funcionarios políticos como técnicos, y sea cual fuere su nivel jerárquico y su situación de revista.

1.2 Qué es seguridad de la información?

La información es un activo que, como otros activos importantes, es esencial y en consecuencia necesita ser protegido adecuadamente.

La información puede existir en muchas formas. Puede estar impresa o escrita en un papel, almacenada electrónicamente, transmitida por correo o utilizando medios electrónicos, mostrada en películas o hablada en una conversación. Cualquiera que sea la forma que tome la información, o medio por el cual sea almacenada o compartida, siempre debiera estar apropiadamente protegida.

La seguridad de la información es la protección de la información de un rango amplio de amenazas para poder asegurar la continuidad del negocio, minimizar el riesgo de la operación y la operación normal del organismo.

La seguridad de la información se logra implementando un adecuado conjunto de controles; incluyendo políticas, procesos, procedimientos, estructuras organizacionales y funciones de software y hardware. Se necesitan establecer, implementar, monitorear, revisar y mejorar estos controles cuando sea necesario para asegurar que se cumplan los objetivos de seguridad y comerciales específicos. Esto se debiera realizar en conjunción con otros procesos de gestión del organismo.

1.3 ¿Por qué es necesario?

La información y los procesos, sistemas y redes de apoyo son activos importantes. Definir, lograr, mantener y mejorar la seguridad de la información puede ser esencial para mantener una eficacia en la operación de las actividades del organismo, observancia legal e imagen.

Las organizaciones y sus sistemas y redes de información enfrentan amenazas de seguridad de un amplio rango de fuentes; incluyendo fraude por computadora, espionaje, sabotaje, vandalismo, fuego o inundación. Las causas de daño como código malicioso, piratería computarizada o negación de ataques de servicio se hacen cada vez más comunes, más ambiciosas y cada vez más sofisticadas.

La seguridad de la información es importante tanto para negocios del sector público como privado, y para proteger las infraestructuras críticas. En ambos sectores, la seguridad de la información funcionará como un facilitador; por ejemplo para lograr e-gobierno o e-negocio, para evitar o reducir los riesgos relevantes. La interconexión de redes públicas y privadas y el intercambio de fuentes de información incrementan la dificultad de lograr un control del acceso. La tendencia a la computación distribuida también ha debilitado la efectividad de un control central y especializado.

Muchos sistemas de información no han sido diseñados para ser seguros. La seguridad que se puede lograr a través de medios técnicos es limitada, y debiera ser apoyada por la gestión y los procedimientos adecuados. Identificar qué controles establecer requiere de un planeamiento cuidadoso y prestar atención a los detalles. La gestión de la seguridad de la información requiere, como mínimo, la participación de los diferentes grupos de interés, proveedores, terceros, clientes u otros grupos externos. También se puede requerir asesoría especializada de organizaciones externas.

1.4 Requerimientos de seguridad

Todo comienza con identificar los requerimientos de seguridad. Existen tres fuentes principales de requerimientos de seguridad, Una fuente se deriva de evaluar los riesgos para la organización, tomando en cuenta la estrategia general y los objetivos del organismo.

A través de la evaluación del riesgo, se identifican las amenazas para los activos, se evalúa la vulnerabilidad y la probabilidad de ocurrencia y se calcula el impacto potencial.

Otra fuente son los requerimientos legales, reguladores, estatutarios y contractuales que tienen que satisfacer una organización, sus socios comerciales, contratistas y proveedores de servicio; y su ambiente socio-cultural.

Otra fuente es el conjunto particular de principios, objetivos y requerimientos funcionales para el procesamiento de la información que una organización ha desarrollado para sostener sus operaciones.

1.5 Evaluación de los riesgos de seguridad

Los requerimientos de seguridad se identifican mediante una evaluación metódica de los riesgos de seguridad. El gasto en controles debiera ser equilibrado con el daño operacional probable resultado de fallas en la seguridad.

Los resultados de la evaluación del riesgo ayudarán a guiar y determinar la acción de gestión apropiada y las prioridades para manejar los riesgos de seguridad de la información, e implementar los controles seleccionados para protegerse contra esos riesgos.

La evaluación del riesgo se debiera repetir periódicamente para tratar cualquier cambio que podría influir en los resultados de la evaluación del riesgo.

Se puede encontrar más información de la evaluación de los riesgos de seguridad en la cláusula 4.1 "Evaluando los riesgos de la seguridad".

1.6 Selección de controles

Una vez que se han identificado los requerimientos y los riesgos de seguridad y se han tomado las decisiones para el tratamiento de los riesgos, se debieran seleccionar los controles apropiados y se debieran implementar para asegurar que los riesgos se reduzcan a un nivel aceptable.

La selección de los controles de seguridad depende de las decisiones organizacionales basadas en el criterio de aceptación del riesgo, opciones de tratamiento del riesgo y el enfoque general para la gestión del riesgo aplicado a la organización, y también debieran estar sujetas a todas las regulaciones y legislación nacionales e internacionales aplicables.

1.7 ¿Cómo empezar?

Se pueden considerar un número de controles como un buen punto de inicio para la implementación de la seguridad de la información. Estos se basan en requerimientos legales esenciales o pueden ser considerados como una práctica común para la seguridad de la información.

Los controles considerados como esenciales para una organización desde el punto de vista legislativo incluyen, dependiendo de la legislación aplicable:

- protección de datos y privacidad de la información personal
- protección de los registros organizacionales
- derechos de propiedad intelectual

Los controles considerados práctica común para la seguridad de la información incluyen:

- documento de la política de seguridad de la información
- asignación de responsabilidades de la seguridad de la información
- conocimiento, educación y capacitación en seguridad de la información
- procesamiento correcto en las aplicaciones
- gestión de la vulnerabilidad técnica
- gestión de la continuidad operacional
- gestión de los incidentes y mejoras de la seguridad de la información

Estos controles se aplican a la mayoría de las organizaciones y en la mayoría de los escenarios.

Se debiera notar que aunque los controles en esta política son importantes y debieran ser considerados, se debiera determinar la relevancia de cualquier control a la luz de los riesgos específicos que enfrenta la organización. Por lo tanto, aunque el enfoque arriba mencionado es considerado como un buen punto de inicio, no reemplaza la selección de controles basada en la evaluación del riesgo.

1.8 Factores críticos de éxito

La experiencia ha demostrado que los siguientes factores con frecuencia son críticos para una exitosa implementación de la seguridad de la información dentro de una organización:

- política, objetivos y actividades de seguridad de información que reflejan los objetivos del organismo;
- un enfoque y marco referencial para implementar, mantener, monitorear y mejorar la seguridad de la información que sea consistente con la cultura organizacional;
- soporte visible y compromiso de todos los niveles de gestión;
- un buen entendimiento de los requerimientos de seguridad de la información, evaluación del riesgo y gestión del riesgo;
- comunicación efectiva de la seguridad de la información con todo los directores, empleados y otras partes para lograr conciencia sobre el tema;
- distribución de lineamientos sobre la política y los estándares de seguridad de la información para todos los directores, empleados y otras partes involucradas;
- provisión para el financiamiento de las actividades de gestión de la seguridad de la información;
- proveer el conocimiento, capacitación y educación apropiados;
- establecer un proceso de gestión de incidentes de seguridad de la información;
- implementación de un sistema de medición: que se utiliza para evaluar el desempeño en la gestión de la seguridad de la información y retroalimentación de sugerencias para el mejoramiento.

2 Términos y Definiciones

2.1 Seguridad de la Información

La seguridad de la información se entiende como la preservación de las siguientes características:

- **Confidencialidad:** se garantiza que la información sea accesible sólo a aquellas personas autorizadas a tener acceso a la misma.

- **Integridad:** se salvaguarda la exactitud y totalidad de la información y los métodos de procesamiento.

- **Disponibilidad:** se garantiza que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con la misma, toda vez que lo requieran.

Adicionalmente, deben considerarse los conceptos de:

- **Autenticidad:** busca asegurar la validez de la información en tiempo, forma y distribución. Asimismo, se garantiza el origen de la información, validando el emisor para evitar suplantación de identidades.

- **Auditabilidad:** define que todos los eventos de un sistema deben poder ser registrados para su control posterior.

- **Protección a la duplicación:** consiste en asegurar que una transacción sólo se realiza una vez, a menos que se especifique lo contrario. Impedir que se grabe una transacción para luego reproducirla, con el objeto de simular múltiples peticiones del mismo remitente original.

- **No repudio:** se refiere a evitar que una entidad que haya enviado o recibido información alegue ante terceros que no la envió o recibió.

- **Legalidad:** referido al cumplimiento de las leyes, normas, reglamentaciones o disposiciones a las que está sujeto el Organismo.

- **Confiable de la Información:** es decir, que la información generada sea adecuada para sustentar la toma de decisiones y la ejecución de las misiones y funciones.

A los efectos de una correcta interpretación de la presente Política, se realizan las siguientes definiciones:

- **Información:** Se refiere a toda comunicación o representación de conocimiento como datos, en cualquier forma, con inclusión de formas textuales, numéricas, gráficas, cartográficas, narrativas o audiovisuales, y en cualquier medio, ya sea magnético, en papel, en pantallas de computadoras, audiovisual u otro.

- **Sistema de Información:** Se refiere a un conjunto independiente de recursos de información organizados para la recopilación, procesamiento, mantenimiento, transmisión y difusión de información según determinados procedimientos, tanto automatizados como manuales.

- **Tecnología de la Información:** Se refiere al hardware y software operados por el Organismo o por un tercero que procese información en su nombre, para llevar a cabo una función propia del Organismo, sin tener en cuenta la tecnología utilizada, ya se trate de computación de datos, telecomunicaciones u otro tipo.

2.2 Evaluación de Riesgos

Se entiende por evaluación de riesgos a la evaluación de las amenazas y vulnerabilidades relativas a la información y a las instalaciones de procesamiento de la misma, la probabilidad de que ocurran y su potencial impacto en la operatoria del Organismo.

2.2 Tratamiento de Riesgos

Proceso de selección e implementación de medidas para modificar el riesgo.

2.3 Gestión de Riesgos

Actividades coordinadas para dirigir y controlar una organización en lo que concierne al riesgo.

NOTA. La gestión de riesgos usualmente incluye la evaluación de riesgos, el tratamiento de riesgos, la aceptación de riesgos y la comunicación de riesgos.

2.4 Comité de Seguridad de la Información

El Comité de Seguridad de la Información, es un cuerpo integrado por representantes de todas las áreas sustantivas del Organismo, destinado a garantizar el apoyo manifiesto de las autoridades a las iniciativas de seguridad.

2.5 Responsable de Seguridad de la Información

Es la persona que cumple la función de supervisar el cumplimiento de la presente Política y de asesorar en materia de seguridad de la información a los integrantes del Organismo que así lo requieran.

2.6 Incidente de Seguridad

Un incidente de seguridad es un evento adverso en un sistema de computadoras, o red de computadoras, que puede comprometer o compromete la confidencialidad, integridad y/o disponibilidad de la información. Puede ser causado mediante la explotación de alguna vulnerabilidad o un intento o amenaza de romper los mecanismos de seguridad existentes.

2.8 Riesgo

Combinación de la probabilidad de ocurrencia de un evento y sus consecuencias o impacto.

2.9 Amenaza

Una causa potencial de un incidente no deseado, el cual puede ocasionar daños a un sistema u organización.

2.10 Vulnerabilidad

Una debilidad de un activo o grupo de activos que puede ser aprovechada por una amenaza.

2.11 Control

Medio para gestionar el riesgo, incluyendo políticas, procedimientos, directrices, prácticas o estructuras organizacionales, las cuales pueden ser de naturaleza administrativa, técnica, de gestión, o legal.

NOTA. Control es también utilizado como sinónimo de salvaguarda o de contramedida.

3. Estructura de la política Modelo

Este modelo que se divide en dos partes, y guarda la siguiente estructura:

- Cuatro capítulos introductorios, con los términos generales y el establecimiento de la Evaluación y el Tratamiento de los riesgos.

- Once capítulos que abarcan las diferentes cláusulas, aspectos o dominios de la seguridad de la información. Se presentan de manera sistemática y consistente.



Cada **cláusula** contiene un número de **categorías** o grupo de controles de seguridad principales. Las diez cláusulas (acompañadas por el número de categorías de seguridad principales incluidas dentro de cada cláusula) son:

- Política de Seguridad (1);
- Organización (2);
- Gestión de Activos (2);
- Recursos Humanos (3);
- Seguridad Física y Ambiental (2);
- Gestión de Comunicaciones y Operaciones (10);
- Gestión de Accesos (7);
- Adquisición, Desarrollo y Mantenimiento de Sistemas (6);
- Gestión de Incidentes de seguridad (2)
- Gestión de la Continuidad (1);
- Cumplimiento (3).

Por último, por cada **categoría**, se establece un **objetivo** y contiene uno o más **controles** a realizar.

A modo de síntesis se enuncia a continuación la estructura de cada uno de los capítulos de cada cláusula:

- Capítulo de la cláusula o dominio

- Generalidades
- Objetivos
- Alcance
- Responsabilidades
- Política
 - Categorías
 - Objetivos
 - Controles

Las once cláusulas o dominios son:

- Cláusulas
- Política de seguridad

- Organización
- Gestión de activos
- Recursos humanos
- Física ambiental
- Gestión de comunicaciones y operaciones
- Gestión de Accesos
- Adquisición, desarrollo y mantenimiento de sistemas
- Gestión de Incidentes de seguridad
- Gestión de continuidad
- Cumplimiento

4. Evaluación y tratamiento de riesgos

Generalidades

Todo Organismo se encuentra expuesto a riesgos en materia de seguridad de la información. No existe la seguridad completa, por lo que es necesario conocer cuál es el mapa de riesgos al cual se enfrenta el organismo y tomar acciones tendientes a minimizar los posibles efectos negativos de la materialización de dichos riesgos.

Es por ello que resulta imprescindible gestionar los riesgos del Organismo, como pilar fundamental para la gestión de seguridad.

Objetivo

Conocer los riesgos a los que se expone el Organismo en materia de seguridad de la información.

Generar información de utilidad para la toma de decisiones en materia de controles de seguridad.

Alcance

Esta Política se aplica a toda la información administrada en el Organismo, cualquiera sea el soporte en que se encuentre.

Responsabilidad

El Comité de Seguridad de la Información será responsable de que se gestionen los riesgos de seguridad de la información, brindando su apoyo para el desarrollo de dicho proceso y su mantenimiento en el tiempo.

El Responsable de Seguridad de la Información junto con los Titulares de Unidades Organizativas serán responsables del desarrollo del proceso de gestión de riesgos de seguridad de la información.

Política

4.1 Evaluación de los riesgos de seguridad

El Organismo evaluará sus riesgos identificándolos, cuantificándolos y priorizándolos en función de los criterios de aceptación de riesgos y de los objetivos de control relevantes para el mismo. Los resultados guiarán y determinarán la apropiada acción de la dirección y las prioridades para gestionar los riesgos de seguridad de la información y para la implementación de controles seleccionados para protegerse contra estos riesgos.

Se debe efectuar la evaluación de riesgos periódicamente, para tratar con los cambios en los requerimientos de seguridad y en las situaciones de riesgo, por ejemplo: cambios producidos en activos, amenazas, vulnerabilidades, impactos, valoración de riesgos. Asimismo, se debe efectuar la evaluación cada vez que ocurran cambios significativos. Es conveniente que estas evaluaciones de riesgos se lleven a cabo de una manera metódica capaz de producir resultados comparables y reproducibles.

El alcance de una evaluación de riesgos puede incluir a todo el Organismo, una parte, un sistema de información particular, componentes específicos de un sistema, o servicios. Resulta recomendable seguir una metodología de evaluación de riesgos para llevar a cabo el proceso.

4.2 Tratamiento de riesgos de seguridad

Antes de considerar el tratamiento de un riesgo, el Organismo debe decidir los criterios para determinar si los riesgos pueden, o no, ser aceptados. Los riesgos pueden ser aceptados si por ejemplo: se evaluó que el riesgo es bajo o que el costo del tratamiento no es económicamente viable para la organización. Tales decisiones deben ser tomadas por las autoridades y debidamente documentadas.

Para cada uno de los riesgos identificados durante la evaluación de riesgos, se necesita tomar una decisión para su tratamiento. Las posibles opciones para el tratamiento de riesgos incluyen:

- a) Mitigar los riesgos mediante la aplicación de controles apropiados para reducir los riesgos;
- b) Aceptar los riesgos de manera objetiva y consciente, siempre y cuando éstos satisfagan claramente la política y los criterios de aceptación de riesgos del Organismo;
- c) Evitar los riesgos, eliminando las acciones que dan origen a la ocurrencia de éstos;
- d) Transferir los riesgos asociados a otras partes interesadas, por ejemplo: compañías de seguro o proveedores.

Para aquellos riesgos donde la decisión ha sido la mitigación, se buscará reducir los riesgos a un nivel aceptable mediante la implementación de controles, teniendo en cuenta lo siguiente:

- a) requerimientos y restricciones de legislaciones y regulaciones nacionales e internacionales;
- b) objetivos organizacionales;

c) requerimientos y restricciones operativos;

d) costo de implementación y operación en relación directa a los riesgos reducidos, y proporcionales a los requerimientos y restricciones del Organismo;

e) la necesidad de equilibrar las inversiones en la implementación y operación de los controles contra el daño que podría resultar de las fallas de seguridad.

Los controles a implementar pueden ser seleccionados del contenido de los capítulos de esta política, o se pueden establecer nuevos controles para satisfacer necesidades específicas del Organismo. Es necesario reconocer que algunos controles pueden no ser aplicables a todo sistema de información o a su ambiente, y podrían no ser aplicables en todos los Organismos.

Se debe recordar que ningún conjunto de controles puede alcanzar la seguridad absoluta. Los controles implementados deben ser evaluados permanentemente para que puedan ser mejorados en eficiencia y efectividad.

5. Cláusula: Política de Seguridad de la Información



Generalidades

La información es un recurso que, como el resto de los activos, tiene valor para el Organismo y por consiguiente debe ser debidamente protegida.

Las Políticas de Seguridad de la Información protegen a la misma de una amplia gama de amenazas, a fin de garantizar la continuidad de los sistemas de información y de la operación del Organismo, minimizar los riesgos de daño y asegurar el eficiente cumplimiento de los objetivos del Organismo.

Es importante que los principios de la Política de Seguridad sean parte de la cultura organizacional.

Para esto, se debe asegurar un compromiso manifiesto de las máximas Autoridades del Organismo y de los titulares de Unidades Organizativas para la difusión, consolidación y cumplimiento de la presente Política.

Objetivo

Proteger los recursos de información del Organismo y la tecnología utilizada para su procesamiento, frente a amenazas, internas o externas, deliberadas o accidentales, con el fin de asegurar el cumplimiento de la confidencialidad, integridad, disponibilidad, legalidad y confiabilidad de la información.

Asegurar la implementación de las medidas de seguridad comprendidas en esta Política, identificando los recursos y las partidas presupuestarias correspondientes, sin que ello implique necesariamente la asignación de partidas adicionales.

Mantener la Política de Seguridad del Organismo actualizada, a efectos de asegurar su vigencia y nivel de eficacia.

Alcance

Esta Política se aplica en todo el ámbito del Organismo, a sus recursos y a la totalidad de los procesos, ya sean internos o externos vinculados a la entidad a través de contratos o acuerdos con terceros.

Responsabilidad

Todos los Directores Nacionales o Generales, Gerentes o equivalentes, titulares de Unidades Organizativas, tanto se trate de autoridades políticas o personal técnico y sea cual fuere su nivel jerárquico son responsables de la implementación de esta Política de Seguridad de la Información dentro de sus áreas de responsabilidad, así como del cumplimiento de dicha Política por parte de su equipo de trabajo.

La Política de Seguridad de la Información es de aplicación obligatoria para todo el personal del Organismo, cualquiera sea su situación de revista, el área a la cual se encuentre afectado y cualquiera sea el nivel de las tareas que desempeñe.

Las máximas autoridades del Organismo aprueban esta Política y son responsables de la autorización de sus modificaciones.

El Comité de Seguridad de la Información del Organismo,

- procederá a revisar y proponer a la máxima autoridad del Organismo para su aprobación la Política de Seguridad de la Información y las funciones generales en materia de seguridad de la información;
- monitorear cambios significativos en los riesgos que afectan a los recursos de información frente a las amenazas más importantes;
- tomar conocimiento y supervisar la investigación y monitoreo de los incidentes relativos a la seguridad;
- aprobar las principales iniciativas para incrementar la seguridad de la información, de acuerdo a las competencias y responsabilidades asignadas a cada área¹, así como acordar y aprobar metodologías y procesos específicos relativos a seguridad de la información;

¹ Se refiere a dar curso a las propuestas presentadas por parte de las áreas de acuerdo a sus competencias, elevándolas a la máxima autoridad, a través del Comité de Seguridad, con relación a la seguridad de la información del Organismo. Dichas iniciativas deben ser aprobadas luego por la máxima autoridad del Organismo.

- garantizar que la seguridad sea parte del proceso de planificación de la información; evaluar y coordinar la implementación de controles específicos de seguridad de la información para nuevos sistemas o servicios;

- promover la difusión y apoyo a la seguridad de la información dentro del Organismo y coordinar el proceso de administración de la continuidad de las actividades del Organismo.

El **Coordinador del Comité de Seguridad de la Información** será el responsable de:

- coordinar las acciones del Comité de Seguridad de la Información y de
- impulsar la implementación y cumplimiento de la presente Política.

El **Responsable de Seguridad de la Información**

- cumplirá funciones relativas a la seguridad de los sistemas de información del Organismo,
- lo cual incluye: la supervisión de todos los aspectos inherentes a los temas tratados en la presente Política.

Los **Propietarios de la Información**² y **Propietarios de activos** son responsables de:

- clasificarla de acuerdo con el grado de sensibilidad y criticidad de la misma,
- de documentar y mantener actualizada la clasificación efectuada, y
- de definir qué usuarios deben tener permisos de acceso a la información de acuerdo a sus funciones y competencia.

El **Responsable del Área de Recursos Humanos** o quien desempeñe esas funciones, cumplirá la función de:

- notificar a todo el personal que ingresa de sus obligaciones respecto del cumplimiento de la Política de Seguridad de la Información y de todas las normas, procedimientos y prácticas que de ella surjan.

- Asimismo, tendrá a su cargo la notificación de la presente Política a todo el personal, de los cambios que en ella se produzcan, la implementación de la suscripción de los Compromisos de Confidencialidad (entre otros) y las tareas de capacitación continua en materia de seguridad.

El **Responsable del Área Informática** cumplirá la función de cubrir los requerimientos de seguridad informática establecidos para la operación, administración y comunicación de los sistemas y recursos de tecnología del Organismo. Por otra parte tendrá la función de efectuar las tareas de desarrollo y mantenimiento de sistemas, siguiendo una metodología de ciclo de vida de sistemas apropiada, y que contemple la inclusión de medidas de seguridad en los sistemas en todas las fases.

El **Responsable del Área Legal o Jurídica** verificará el cumplimiento de la presente Política en la gestión de todos los contratos, acuerdos u otra documentación del Organismo con sus empleados y con terceros. Asimismo, asesorará en materia legal al Organismo, en lo que se refiere a la seguridad de la información.

Los **usuarios de la información y de los sistemas** utilizados para su procesamiento son responsables de conocer, dar a conocer, cumplir y hacer cumplir la Política de Seguridad de la Información vigente.

La **Unidad de Auditoría Interna**, o en su defecto quien sea propuesto por el Comité de Seguridad de la Información es responsable de practicar auditorías periódicas sobre los sistemas y actividades vinculadas con la tecnología de información, debiendo informar sobre el cumplimiento de las especificaciones y medidas de seguridad de la información establecidas por esta Política y por las normas, procedimientos y prácticas que de ella surjan (Ver capítulo 15 Cláusula Cumplimiento).

Política

5.1 Categoría: Política de Seguridad de la información

Objetivo

Proporcionar a la Dirección Superior la dirección y soporte para la seguridad de la información en concordancia con los requerimientos y las leyes y regulaciones relevantes. La gerencia debe establecer claramente la dirección de la política en línea con los objetivos.

5.1.1 Control: Documento de la política de seguridad de la información

El documento de la política debe ser aprobado por el Comité de Seguridad, publicado y comunicado a todos los empleados y las partes externas relevantes.

Esta Política se conforma de una serie de pautas sobre aspectos específicos de la Seguridad de la Información, que incluyen los siguientes tópicos:

Organización de la Seguridad

Orientado a administrar la seguridad de la información dentro del Organismo y establecer un marco gerencial para controlar su implementación.

Gestión de Activos

Destinado a mantener una adecuada protección de los activos del Organismo.

Recursos Humanos

Orientado a reducir los riesgos de error humano, comisión de ilícitos contra el Organismo o uso inadecuado de instalaciones.

Física y Ambiental

Destinado a impedir accesos no autorizados, daños e interferencia a las sedes e información del Organismo.

² El concepto "Propietario de la Información" define a la persona responsable de la integridad, confidencialidad y disponibilidad de una cierta información.

Gestión de las Comunicaciones y las Operaciones

Dirigido a garantizar el funcionamiento correcto y seguro de las instalaciones de procesamiento de la información y medios de comunicación.

Gestión de Accesos

Orientado a controlar el acceso lógico a la información.

Adquisición. Desarrollo y Mantenimiento de los Sistemas

Orientado a garantizar la incorporación de medidas de seguridad en los sistemas de información desde su adquisición, desarrollo y/o implementación y durante su mantenimiento.

Gestión de Incidentes de seguridad

Orientado a administrar todos los eventos que atenten contra la confidencialidad, integridad y disponibilidad de la información y los activos tecnológicos

Gestión de Continuidad

Orientado a contrarrestar las interrupciones de las actividades y proteger los procesos críticos de los efectos de fallas significativas o desastres.

Cumplimiento

Destinado a impedir infracciones y violaciones de las leyes del derecho civil y penal; de las obligaciones establecidas por leyes, estatutos, normas, reglamentos o contratos; y de los requisitos de seguridad.

A fin de asegurar la implementación de las medidas de seguridad comprendidas en esta Política, el Organismo identificará los recursos necesarios e indicará formalmente las partidas presupuestarias correspondientes, como anexo a la presente Política. Lo expresado anteriormente no implicará necesariamente la asignación de partidas presupuestarias adicionales.

La máxima autoridad del Organismo aprobará formalmente la Política y la comunicará a todos los empleados y terceras partes relevantes.

5-1-2 Control: Revisión de la política de seguridad de la información

La política de seguridad de la información debe tener un dueño, responsable de las actividades de desarrollo, evaluación y revisión de la política.

La actividad de revisión debe incluir las oportunidades de mejoras, en respuesta a los cambios, entre otros: organizacionales, normativos, legales, tercero, tecnológicos.

Las mejoras tenidas en cuenta, deben quedar registradas y tener las aprobaciones de los responsables.

El Comité de Seguridad de la Información debe revisarla a intervalos planeados y prever el tratamiento de caso de los cambios no planeados, a efectos de mantener actualizada la política.

Asimismo efectuará toda modificación que sea necesaria en función a posibles cambios que puedan afectar su definición, como ser, cambios tecnológicos, variación de los costos de los controles, impacto de los incidentes de seguridad, etc.

6. Cláusula: Organización



Generalidades

La presente Política de Seguridad establece la administración de la seguridad de la información, como parte fundamental de los objetivos y actividades del Organismo.

Por ello, se definirá formalmente un ámbito de gestión para efectuar tareas tales como la aprobación de la Política, la coordinación de su implementación y la asignación de funciones y responsabilidades.

Asimismo, se contemplará la necesidad de disponer de fuentes con conocimiento y experimentadas para el asesoramiento, cooperación y colaboración en materia de seguridad de la información.

Por otro lado debe tenerse en cuenta que ciertas actividades del Organismo pueden requerir que terceros accedan a información interna, o bien puede ser necesaria la tercerización de ciertas funciones relacionadas con el procesamiento de la información. En estos casos se considerará que la información puede ponerse en riesgo si el acceso de dichos terceros se produce en el marco de una inadecuada administración de la seguridad, por lo que se establecerán las medidas adecuadas para la protección de la información.

Objetivo

Administrar la seguridad de la información dentro del Organismo y establecer un marco gerencial para iniciar y controlar su implementación, así como para la distribución de funciones y responsabilidades.

Fomentar la consulta y cooperación con Organismos especializados para la obtención de asesoría en materia de seguridad de la información.

Garantizar la aplicación de medidas de seguridad adecuadas en los accesos de terceros a la información del Organismo.

Alcance

Esta Política se aplica a todos los recursos del Organismo y a todas sus relaciones con terceros que impliquen el acceso a sus datos, recursos y/o a la administración y control de sus sistemas de información.

Responsabilidad

El Coordinador del Comité de Seguridad de la Información será el responsable de impulsar la implementación de la presente Política.

El Comité de Seguridad de la Información tendrá a cargo el mantenimiento y la presentación para la aprobación de la presente Política, ante la máxima autoridad del organismo, el seguimiento de acuerdo a las incumbencias propias de cada área de las actividades relativas a la seguridad de la información (análisis de riesgos, monitoreo de incidentes, supervisión de la investigación, implementación de controles, administración de la continuidad, impulsión de procesos de concientización, etc.) y la proposición de asignación de funciones.

El Responsable de Seguridad de la Información asistirá al personal del Organismo en materia de seguridad de la información y coordinará la interacción con Organismos especializados. Asimismo, junto con los propietarios de la información, analizará el riesgo de los accesos de terceros a la información del Organismo y verificará la aplicación de las medidas de seguridad necesarias para la protección de la misma.

Los Responsables de las Unidades Organizativas cumplirán la función de autorizar la incorporación de nuevos recursos de procesamiento de información a las áreas de su incumbencia.

La Unidad de Auditoría Interna o en su defecto quien sea propuesto por el Comité de Seguridad de la Información será responsable de realizar revisiones independientes sobre la vigencia y el cumplimiento de la presente Política.

El Responsable del Área de Administración cumplirá la función de incluir en los contratos con proveedores de servicios de tecnología y cualquier otro proveedor de bienes o servicios cuya actividad afecte directa o indirectamente a los activos de información, la obligatoriedad del cumplimiento de la Política de Seguridad de la Información y de todas las normas, procedimientos y prácticas relacionadas.

El Responsable del Área Jurídica participará en dicha tarea.

Asimismo, notificará a los proveedores sobre las modificaciones que se efectúen a la Política de Seguridad de la Información del Organismo

Política**6.1 Categoría: Organización interna****Objetivo**

Manejar la seguridad de la información dentro del organismo.

Se debe establecer un marco referencial gerencial o política, para iniciar y controlar la implementación de la seguridad de la información dentro del organismo.

La Dirección debe aprobar la política de seguridad de la información, asignar los roles de seguridad y coordinar y revisar la implementación de la seguridad en todo el organismo.

6.1.1 Control: Compromiso de la dirección con la seguridad de la información

La dirección debe apoyar la seguridad de la información a través de una dirección clara, mostrando compromiso, asignando roles y reconociendo responsabilidades explícitas.

Debe formular, revisar y aprobar la política de seguridad de la información, como asimismo revisar los beneficios de la implementación de la misma.

La seguridad de la información es una responsabilidad del Organismo compartida por todas las Autoridades políticas y Directores Nacionales o Generales, Gerentes o equivalentes, por lo cual se crea el Comité de Seguridad de la Información, integrado por representantes de todos los Directores mencionados, destinado a garantizar el apoyo manifiesto de las autoridades a las iniciativas de seguridad de la información. El mismo contará con un Coordinador, quien cumplirá la función de impulsar la implementación de la presente Política.

Conformación del Comité de Seguridad de la Información

Area/Dirección	Representante

Este Comité tendrá entre sus funciones:

a) Revisar y proponer a la máxima autoridad del Organismo para su aprobación, la Política y las funciones generales en materia de seguridad de la información.

b) Monitorear cambios significativos en los riesgos que afectan a los recursos de información frente a las amenazas más importantes.

c) Tomar conocimiento y supervisar la investigación y monitoreo de los incidentes relativos a la seguridad.

d) Aprobar las principales iniciativas para incrementar la seguridad de la información, de acuerdo a las competencias y responsabilidades asignadas a cada área³.

e) Acordar y aprobar metodologías y procesos específicos relativos a la seguridad de la información.

f) Garantizar que la seguridad sea parte del proceso de planificación informática del Organismo.

g) Evaluar y coordinar la implementación de controles específicos de seguridad de la información para nuevos sistemas o servicios.

h) Promover la difusión y apoyo a la seguridad de la información dentro del Organismo.

i) Coordinar el proceso de administración de la continuidad de la operatoria de los sistemas de tratamiento de la información del Organismo frente a interrupciones imprevistas.

El (Subsecretario de Coordinación o equivalente en cada área ministerial o Secretaría de la Presidencia de la Nación o el funcionario designado por las máximas autoridades en cada Organismo descentralizado - Indicar cargo) coordinará las actividades del Comité de Seguridad de la Información.

³ Se refiere a dar curso a las propuestas presentadas por parte de las áreas de acuerdo a sus competencias, elevándolas a la máxima autoridad, a través del Comité de Seguridad, con relación a la seguridad de la información del Organismo. Dichas iniciativas deben ser aprobadas luego por la máxima autoridad del Organismo.

6-1-2 Control: Coordinación de la seguridad de la información

Típicamente, la coordinación de la seguridad de la información debiera involucrar la cooperación y colaboración de los Directores Nacionales o Generales, Gerentes o equivalentes, usuarios, administradores, diseñadores de aplicación, auditores y personal de seguridad, y capacidades especializadas en áreas como seguros, temas legales, recursos humanos, TI o gestión del riesgo. Esta actividad debiera:

a) asegurar que las actividades de seguridad sean ejecutadas en conformidad con la política de seguridad de la información;

b) identificar cómo manejar las no-conformidades;

c) aprobar las metodologías y procesos para la seguridad de la información; por ejemplo, la evaluación del riesgo, la clasificación de la información;

d) identificar cambios significativos en las amenazas y la exposición de la información y los medios de procesamiento de la información ante amenazas;

e) evaluar la idoneidad y coordinar la implementación de los controles de la seguridad de información;

f) promover de manera efectiva la educación, capacitación y conocimiento de la seguridad de la información a través de toda la organización;

g) evaluar la información recibida del monitoreo y revisar los incidentes de seguridad de la información, y recomendar las acciones apropiadas en respuesta a los incidentes de seguridad de información identificados.

6-1-3 Control: Asignación de responsabilidades de la seguridad de la información

La asignación de responsabilidades de la seguridad de la información debe ejecutarse en forma alineada a la política de seguridad de la información (ver cláusula 5 política de seguridad)

El (indicar la máxima autoridad del Organismo), asigna las funciones relativas a la Seguridad Informática del Organismo a (indicar cargo), en adelante el "Responsable de Seguridad de la Información", quien tendrá a cargo las funciones relativas a la seguridad de los sistemas de información del Organismo, lo cual incluye la supervisión de todos los aspectos inherentes a seguridad informática tratados en la presente Política.

El Comité de Seguridad de la Información propondrá a la autoridad que corresponda para su aprobación la definición y asignación de las responsabilidades que surjan del presente Modelo.

A continuación se detallan los procesos de seguridad, indicándose en cada caso el/los responsable/s del cumplimiento de los aspectos de esta Política aplicables a cada caso:

Proceso	Responsable
Seguridad del Personal
Seguridad Física y Ambiental
Seguridad en las Comunicaciones y las Operaciones
Control de Accesos
Seguridad en el Desarrollo y Mantenimiento de Sistemas
Planificación de la Continuidad Operativa
.....

De igual forma, seguidamente se detallan los propietarios de la información, quienes serán los Responsables de las Unidades Organizativas a cargo del manejo de la misma:

Información	Propietario	Recursos asociados	Procesos involucrados	Administrador
Contable	Sistemas de información, equipamiento, bases de datos, comunicaciones,
Presupuesto
Inventario				
.....				
.....				

Cabe aclarar que, si bien los propietarios pueden delegar la administración de sus funciones a personal idóneo a su cargo, conservarán la responsabilidad del cumplimiento de las mismas. La delegación de la administración por parte de los propietarios de la información será documentada por los mismos y proporcionada al Responsable de Seguridad de la Información.

6-1-4 Control: Autorización para Instalaciones de Procesamiento de Información

Los nuevos recursos de procesamiento de información serán autorizados por los Responsables de las Unidades Organizativas involucradas, considerando su propósito y uso, conjuntamente con el Responsable de Seguridad de la Información, a fin de garantizar que se cumplan todas las Políticas y requerimientos de seguridad pertinentes.

Las siguientes guías deben ser consideradas para el proceso de autorización:

a) Cumplir con los niveles de aprobación vigentes en la organización, incluso el responsable del ambiente de seguridad de la información, asegurando el cumplimiento de las políticas y requerimientos.

b) Cuando corresponda, se verificará el hardware y software para garantizar su compatibilidad con los componentes de otros sistemas del Organismo.

c) El uso de recursos personales de procesamiento de información en el lugar de trabajo puede ocasionar nuevas vulnerabilidades. En consecuencia, su uso será evaluado en cada caso por el Responsable de Seguridad de la Información y debe ser autorizado por el Responsable del Área Informática y por el Director Nacional (General, Gerente o equivalente en el Organismo) responsable del área al que se destinen los recursos.

6-1-5 Control: Acuerdos de confidencialidad

Se definirán, implementarán y revisarán regularmente los acuerdos de confidencialidad o de no divulgación para la protección de la información del Organismo. Dichos acuerdos deben

responder a los requerimientos de confidencialidad o no divulgación del Organismo, los cuales serán revisados periódicamente. Asimismo, deben cumplir con toda legislación o normativa que alcance al Organismo en materia de confidencialidad de la información.

Dichos acuerdos deben celebrarse tanto con el personal del organismo como con aquellos terceros que se relacionen de alguna manera con su información.

6-1-6 Control: Contacto con otros organismos

A efectos de intercambiar experiencias y obtener asesoramiento para el mejoramiento de las prácticas y controles de seguridad, se mantendrán contactos con los siguientes Organismos especializados en temas relativos a la seguridad informática:

• **Oficina Nacional de Tecnologías de Información (ONTI), y particularmente con:**

- **La Oficina Nacional de Tecnologías de Información - Coordinación de Emergencias en Redes Teleinformáticas.**

La Coordinación de Emergencias en Redes Teleinformáticas es una unidad de respuesta ante incidentes en redes, que centraliza y coordina los esfuerzos para el manejo de los incidentes de seguridad que afecten a los recursos informáticos del Sector Público.

• **Dirección Nacional de Protección de Datos Personales.**

En los intercambios de información de seguridad, no se divulgará información sensible (de acuerdo a lo definido en la normativa vigente, ej.: Ley 25.326) o confidencial perteneciente al Organismo a personas no autorizadas.

El intercambio de información confidencial para fines de asesoramiento o de transmisión de experiencias, sólo se permite cuando se haya firmado un Acuerdo de Confidencialidad previo o con aquellas Organizaciones especializadas en temas relativos a la seguridad de la Información cuyo personal está obligado a mantener la confidencialidad de los temas que trata.

6-1-7 Control: Contacto con grupos de interés especial

El Responsable de Seguridad de la Información será el encargado de coordinar los conocimientos y las experiencias disponibles en el Organismo a fin de brindar ayuda en la toma de decisiones en materia de seguridad. Este podrá obtener asesoramiento de otros Organismos. Con el objeto de optimizar su gestión, se habilitará al Responsable de Seguridad de la Información el contacto con las Unidades Organizativas de todas las Áreas del Organismo.

Debe considerar ser miembro de grupos de interés especial para:

- Adquirir nuevos conocimientos acerca de las mejores prácticas y estar actualizado
- Asegurar que la concientización acerca de la seguridad de la información esté actualizada y completa
- Recibir alertas tempranas, avisos y recomendaciones ante ataques y vulnerabilidades
- Proporcionar vínculos adecuados durante el tratamiento de los incidentes de seguridad de la información.

6-1-8 Control: Revisión independiente de la seguridad de la información

La Unidad de Auditoría Interna o en su defecto quien sea propuesto por el Comité de Seguridad de la Información realizará revisiones independientes sobre la vigencia, implementación y gestión de la Política de Seguridad de la Información, a efectos de garantizar que las prácticas del Organismo reflejan adecuadamente sus disposiciones.

Estas revisiones deben incluir las oportunidades de evaluación de mejoras y las necesidades de cambios de enfoque en la seguridad, incluyendo políticas y objetivos de control.

Se deben registrar y reportar todas estas actividades.

6.2 Categoría: Grupos o personas externas

Objetivo

Mantener la seguridad de la información y los medios de procesamiento de información del Organismo que son ingresados, procesados, comunicados a, o manejados por, grupos externos.

La seguridad de la información y los medios de procesamiento de la información del Organismo no deben ser reducidos por la introducción de productos y servicios de grupos externos.

6.2.1 Control: Identificación de los riesgos relacionados con grupos externos

Cuando exista la necesidad de otorgar acceso a terceras partes a información del Organismo, el Responsable de Seguridad de la Información y el Propietario de la Información de que se trate, llevarán a cabo y documentarán una evaluación de riesgos para identificar los requerimientos de controles específicos, teniendo en cuenta, entre otros aspectos:

- Los medios de procesamiento de información a los cuales necesita tener acceso el grupo externo
- El tipo de acceso requerido (físico/lógico y a qué recurso).
- Los motivos para los cuales se solicita el acceso.
- El valor de la información.
- Los controles empleados por la tercera parte.
- Diferentes medios y controles empleados por el grupo externo cuando almacena, procesa, comunica, comparte e intercambia información.
- La incidencia de este acceso en la seguridad de la información del Organismo.

En todos los contratos o acuerdos cuyo objeto sea la prestación de servicios a título personal bajo cualquier modalidad jurídica que deban desarrollarse dentro del Organismo, se establecerán los controles, requerimientos de seguridad y compromisos de confidencialidad aplicables al caso, restringiendo al mínimo necesario, los permisos a otorgar.

Se cita a modo de ejemplo:

- Personal de mantenimiento y soporte de hardware y software.
- Limpieza, "catering", guardia de seguridad y otros servicios de soporte tercerizados.
- Pasantías y otras designaciones de corto plazo.
- Consultores.
- Audidores

En ningún caso se otorgará acceso a terceros a la información, a las instalaciones de procesamiento u otras áreas de servicios críticos, hasta tanto se hayan implementado los controles apropiados y se haya firmado un contrato o acuerdo que defina las condiciones para la conexión o el acceso.

6-2- 2 Control: Puntos de seguridad de la información a considerar en Contratos o Acuerdos con terceros

Se revisarán los contratos o acuerdos existentes o que se efectúen con terceros, teniendo en cuenta la necesidad de aplicar los siguientes controles:

- Cumplimiento de la Política de seguridad de la información del Organismo.
- Protección de los activos del Organismo, incluyendo:
 - Procedimientos para proteger los bienes del Organismo, abarcando los activos físicos, la información y el software.
 - Procedimientos para determinar si ha ocurrido algún evento que comprometa los bienes, por ejemplo, debido a pérdida o modificación de datos.
 - Controles para garantizar la recuperación o destrucción de la información y los activos al finalizar el contrato o acuerdo, o en un momento convenido durante la vigencia del mismo.
 - Restricciones a la copia y divulgación de información.
- Descripción de los servicios disponibles.
- Nivel de servicio esperado y niveles de servicio aceptables.
- Permiso para la transferencia de personal cuando sea necesario.
- Obligaciones de las partes emanadas del acuerdo y responsabilidades legales.
- Existencia de Derechos de Propiedad Intelectual.
- Definiciones relacionadas con la protección de datos.
- Acuerdos de control de accesos que contemplen:
 - Métodos de acceso permitidos, y el control y uso de identificadores únicos como identificadores de usuario y contraseñas de usuarios.
 - Proceso de autorización de accesos y privilegios de usuarios.
 - Requerimiento para mantener actualizada una lista de individuos autorizados a utilizar los servicios que han de implementarse y sus derechos y privilegios con respecto a dicho uso.
- Definición de criterios de desempeño comprobables, de monitoreo y de presentación de informes.
- Adquisición de derecho a auditar responsabilidades contractuales o surgidas del acuerdo.
- Establecimiento de un proceso para la resolución de problemas y en caso de corresponder disposiciones con relación a situaciones de contingencia.
- Responsabilidades relativas a la instalación y al mantenimiento de hardware y software.
- Estructura de dependencia y del proceso de elaboración y presentación de informes que contemple un acuerdo con respecto a los formatos de los mismos.
- Proceso claro y detallado de administración de cambios.
- Controles de protección física requeridos y los mecanismos que aseguren la implementación de los mismos.
- Métodos y procedimientos de entrenamiento de usuarios y administradores en materia de seguridad.
- Controles que garanticen la protección contra software malicioso.
- Elaboración y presentación de informes, notificación e investigación de incidentes y violaciones relativos a la seguridad.
- Relación entre proveedores y subcontratistas.

6-2-3 Control: Puntos de Seguridad de la Información a ser considerados en acuerdos con terceros

Los contratos o acuerdos de tercerización total o parcial para la administración y control de sistemas de información, redes y/o ambientes de equipamiento de Trabajo del Organismo, contemplarán además de los puntos especificados en 6.2.2, los siguientes aspectos:

- Forma en que se cumplirán los requisitos legales aplicables.
- Medios para garantizar que todas las partes involucradas en la tercerización, incluyendo los subcontratistas, están al corriente de sus responsabilidades en materia de seguridad.
- Forma en que se mantendrá y comprobará la integridad y confidencialidad de los activos del Organismo.

d) Controles físicos y lógicos que se utilizarán para restringir y delimitar el acceso a la información sensible del Organismo.

e) Forma en que se mantendrá la disponibilidad de los servicios ante la ocurrencia de desastres.

f) Niveles de seguridad física que se asignarán al equipamiento tercerizado.

g) Derecho a la auditoría por parte del Organismo sobre los aspectos tercerizados en forma directa o a través de la contratación de servicios ad hoc.

Se debe prever la factibilidad de ampliar los requerimientos y procedimientos de seguridad con el acuerdo de las partes.

7. Cláusula: Gestión de Activos



Generalidades

El Organismo debe tener un conocimiento preciso sobre los activos que posee como parte importante de la administración de riesgos. Algunos ejemplos de activos son:

- Recursos de información: bases de datos y archivos, documentación de sistemas, manuales de usuario, material de capacitación, procedimientos operativos o de soporte, planes de continuidad y contingencia, información archivada, etc.

- Recursos de software: software de aplicaciones, sistemas operativos, herramientas de desarrollo y publicación de contenidos, utilitarios, etc.

- Activos físicos: equipamiento informático (procesadores, monitores, computadoras portátiles, módems), equipos de comunicaciones (routers, PABXs, máquinas de fax, contestadores automáticos, switches de datos, etc.), medios magnéticos (cintas, discos, dispositivos móviles de almacenamiento de datos —pen drives, discos externos, etc.—), otros equipos técnicos (relacionados con el suministro eléctrico, unidades de aire acondicionado, controles automatizados de acceso, etc.), mobiliario, lugares de emplazamiento, etc.

- Servicios: servicios informáticos y de comunicaciones, utilitarios generales (calefacción, iluminación, energía eléctrica, etc.).

Los activos de información deben ser clasificados de acuerdo a la sensibilidad y criticidad de la información que contienen o bien de acuerdo a la funcionalidad que cumplen y rotulados en función a ello, con el objeto de señalar cómo ha de ser tratada y protegida dicha información.

Generalmente, la información deja de ser sensible o crítica después de un cierto período de tiempo, por ejemplo, cuando la información se ha hecho pública. Estos aspectos deben tenerse en cuenta, puesto que la clasificación por exceso puede traducirse en gastos adicionales innecesarios para el Organismo.

Las pautas de clasificación deben prever y contemplar el hecho de que la clasificación de un ítem de información determinado no necesariamente debe mantenerse invariable por siempre, y que ésta puede cambiar de acuerdo con una Política predeterminada. Se debe considerar la cantidad de categorías a definir para la clasificación dado que los esquemas demasiado complejos pueden tornarse engorrosos y antieconómicos o resultar poco prácticos.

La información adopta muchas formas, tanto en los sistemas informáticos como fuera de ellos. Puede ser almacenada (en dichos sistemas o en medios portátiles), transmitida (a través de redes o entre sistemas) e impresa o escrita en papel. Cada una de estas formas debe contemplar todas las medidas necesarias para asegurar la confidencialidad, integridad y disponibilidad de la información.

Por último, la información puede pasar a ser obsoleta y por lo tanto, ser necesario eliminarla. La destrucción de la información es un proceso que debe asegurar la confidencialidad de la misma hasta el momento de su eliminación.

Objetivo

Garantizar que los activos de información reciban un apropiado nivel de protección.

Clasificar la información para señalar su sensibilidad y criticidad.

Definir niveles de protección y medidas de tratamiento especial acordes a su clasificación.

Alcance

Esta Política se aplica a toda la información administrada en el Organismo, cualquiera sea el soporte en que se encuentre.

Responsabilidad

Los Propietarios de los Activos son los encargados de clasificarlos de acuerdo con su grado de sensibilidad y criticidad, de documentar y mantener actualizada la clasificación efectuada, de definir las funciones que deben tener permisos de acceso a los activos y son responsables de mantener los controles adecuados para garantizar su seguridad.

El Responsable de Seguridad de la Información es el encargado de asegurar que los lineamientos para la utilización de los recursos de la tecnología de información contemplen los requerimientos de seguridad establecidos según la criticidad de la información que procesan.

Cada Propietario de la Información supervisará que el proceso de clasificación y rótulo de información de su área de competencia sea cumplimentado de acuerdo a lo establecido en la presente Política.

Política

7.1 Categoría: Responsabilidad sobre los activos

Objetivo

Todos los activos deben ser inventariados y contar con un propietario nombrado.

Los propietarios deben identificar todos los activos y se debiera asignar la responsabilidad por el mantenimiento de los controles apropiados. La implementación de controles específicos puede ser delegada por el propietario conforme sea apropiado, pero el propietario sigue siendo responsable por la protección apropiada de los activos.

7.1.1 Control: Inventario de activos

Se identificarán los activos de información del Organismo. Existen muchos tipos de activos, que incluyen:

a) información: bases de datos, archivos de datos, documentación, contratos, acuerdos;

b) activos de software: software de aplicaciones, software de sistemas, herramientas de desarrollo, y utilitarios;

c) activos físicos: equipamiento de computación, equipamiento de comunicaciones, medios removibles y otros equipamientos;

d) instalaciones: edificios, ubicaciones físicas, tendido eléctrico, red de agua y gas, etc.;

e) servicios: servicios de cómputo y de comunicaciones, servicios generales, por ejemplo: calefacción, iluminación, energía, y aire acondicionado;

f) personas, y sus calificaciones, habilidades y experiencia;

g) activos intangibles, tales como la reputación y la imagen del Organismo.

El inventario será actualizado ante cualquier modificación de la información registrada y revisado con una periodicidad de (establecer período no mayor a 6 meses).

El encargado de elaborar el inventario y mantenerlo actualizado es cada Responsable de Unidad Organizativa.

7.1.2 Control: Propiedad de los activos

Toda la información y los activos junto a sus medios de procesamiento de información deben ser propiedad de un responsable designado en el organismo.

Se designarán los Propietarios de los activos identificados, quienes deben cumplir sus funciones de propietario, esto es:

a) informar sobre cualquier cambio que afecte el inventario de activos

b) clasificar los activos en función a su valor

c) definir los requisitos de seguridad de los activos

d) velar por la implementación y el mantenimiento de los controles de seguridad requeridos en los activos

Cabe aclarar que, si bien los propietarios pueden delegar la administración de sus funciones a personal idóneo a su cargo, conservarán la responsabilidad del cumplimiento de las mismas. La delegación de la administración por parte de los propietarios de los activos será documentada por los mismos y proporcionada al Responsable de Seguridad de la Información.

7.1.3 Control: Uso aceptable de los activos

Se identificarán, documentarán e implementarán reglas para el uso aceptable de la información y los activos asociados con las instalaciones de procesamiento de la información.

Todos los empleados, contratistas y usuarios de terceras partes deben seguir las reglas para el uso aceptable de la información y los activos asociados con las instalaciones de procesamiento de la misma, incluyendo:

a) correo electrónico,

b) sistemas de gestión,

c) estaciones de trabajo,

d) dispositivos móviles,

e) herramientas y equipamiento de de publicación de contenidos

f) etc.

7.2 Categoría: Clasificación de la información

Objetivo

Asegurar que la información reciba un nivel de protección apropiado.

La información debe ser clasificada para indicar la necesidad, prioridades y grado de protección esperado cuando se maneja la información.

La información tiene diversos grados de confidencialidad e importancia. Algunos ítems pueden requerir un nivel de protección adicional o manejo especial. Se debe utilizar un esquema de clasificación de información para definir un conjunto apropiado de niveles de protección y comunicar la necesidad de medidas de uso especiales.

7.2.1 Control: Directrices de clasificación

Para clasificar un Activo de Información, se evaluarán las tres características de la información en las cuales se basa la seguridad: confidencialidad, integridad y disponibilidad.

A continuación se establece la metodología de clasificación de la información propuesta en función a cada una de las mencionadas características:

- Confidencialidad:

0- Información que puede ser conocida y utilizada sin autorización por cualquier persona, sea empleado del Organismo o no. PUBLICO

1- Información que puede ser conocida y utilizada por todos los empleados del Organismo y algunas entidades externas debidamente autorizadas, y cuya divulgación o uso no autorizados podría ocasionar riesgos o pérdidas leves para el Organismo, el Sector Público Nacional o terceros. RESERVADA - USO INTERNO

2- Información que sólo puede ser conocida y utilizada por un grupo de empleados, que la necesiten para realizar su trabajo, y cuya divulgación o uso no autorizados podría ocasionar pérdidas significativas al Organismo, al Sector Público Nacional o a terceros. RESERVADA - CONFIDENCIAL

3- Información que sólo puede ser conocida y utilizada por un grupo muy reducido de empleados, generalmente de la alta dirección del Organismo, y cuya divulgación o uso no autorizados podría ocasionar pérdidas graves al mismo, al Sector Público Nacional o a terceros. RESERVADA SECRETA

- Integridad:

0- Información cuya modificación no autorizada puede repararse fácilmente, o no afecta la operatoria del Organismo.

1- Información cuya modificación no autorizada puede repararse aunque podría ocasionar pérdidas leves para el Organismo, el Sector Público Nacional o terceros.

2- Información cuya modificación no autorizada es de difícil reparación y podría ocasionar pérdidas significativas para el Organismo, el Sector Público Nacional o terceros.

3- Información cuya modificación no autorizada no podría repararse, ocasionando pérdidas graves al Organismo, al Sector Público Nacional o a terceros.

- Disponibilidad:

0- Información cuya inaccesibilidad no afecta la operatoria del Organismo.

1- Información cuya inaccesibilidad permanente durante (definir un plazo no menor a una semana) podría ocasionar pérdidas significativas para el Organismo, el Sector Público Nacional o terceros.

2- Información cuya inaccesibilidad permanente durante (definir un plazo no menor a un día) podría ocasionar pérdidas significativas al Organismo, al Sector Público Nacional o a terceros.

3- Información cuya inaccesibilidad permanente durante (definir un plazo no menor a una hora) podría ocasionar pérdidas significativas al Organismo, al Sector Público Nacional o a terceros.

Al referirse a pérdidas, se contemplan aquellas medibles (materiales) y no medibles (imagen, valor estratégico de la información, obligaciones contractuales o públicas, disposiciones legales, etc.).

Se asignará a la información un valor por cada uno de estos criterios. Luego, se clasificará la información en una de las siguientes categorías:

- CRITICIDAD BAJA: ninguno de los valores asignados superan el 1.
- CRITICIDAD MEDIA: alguno de los valores asignados es 2
- CRITICIDAD ALTA: alguno de los valores asignados es 3

Sólo el Propietario de la Información puede asignar o cambiar su nivel de clasificación, cumpliendo con los siguientes requisitos previos:

- Asignarle una fecha de efectividad.
- Comunicárselo al depositario del recurso.
- Realizar los cambios necesarios para que los Usuarios conozcan la nueva clasificación.

Luego de clasificada la información, el propietario de la misma identificará los recursos asociados (sistemas, equipamiento, servicios, etc.) y los perfiles funcionales que deben tener acceso a la misma.

En adelante se mencionará como "información clasificada" (o "datos clasificados") a aquella que se encuadre en los niveles 1, 2 ó 3 de Confidencialidad.

7.2.2 Control: Etiquetado y manipulado de la información

Se definirán procedimientos para el rotulado y manejo de información, de acuerdo al esquema de clasificación definido. Los mismos contemplarán los recursos de información tanto en formatos físicos como electrónicos e incorporarán las siguientes actividades de procesamiento de la información:

- Copia;
- Almacenamiento;
- Transmisión por correo, fax, correo electrónico;
- Transmisión oral (telefonía fija y móvil, correo de voz, contestadores automáticos, etc.).
- Transmisión a través de mecanismos de intercambio de archivos (FTP, almacenamiento masivo remoto, etc.)

Para cada uno de los niveles de clasificación, se deben definir los procedimientos de manejo seguros, incluyendo las actividades de procesamiento, almacenaje, transmisión, de-clasificación y destrucción.

8. Cláusula: Recursos Humanos



Generalidades

La seguridad de la información se basa en la capacidad para preservar su integridad, confidencialidad y disponibilidad, por parte de los elementos involucrados en su tratamiento: equipamiento, software, procedimientos, así como de los recursos humanos que utilizan dichos componentes.

En este sentido, es fundamental educar e informar al personal desde su ingreso y en forma continua, cualquiera sea su situación de revista, acerca de las medidas de seguridad que afectan al desarrollo de sus funciones y de las expectativas depositadas en ellos en materia de seguridad y asuntos de confidencialidad. De la misma forma, es necesario definir las sanciones que se aplicarán en caso de incumplimiento.

La implementación de la Política de Seguridad de la Información tiene como meta minimizar la probabilidad de ocurrencia de incidentes. Es por ello que resulta necesario implementar un mecanismo que permita reportar las debilidades y los incidentes tan pronto como sea posible, a fin de subsanarlos y evitar eventuales repeticiones. Por lo tanto, es importante analizar las causas del incidente producido y aprender del mismo, a fin de corregir las prácticas existentes, que no pudieron prevenirlo, y evitarlo en el futuro.

Objetivo

Reducir los riesgos de error humano, comisión de ilícitos, uso inadecuado de instalaciones y recursos, y manejo no autorizado de la información.

Explicitar las responsabilidades en materia de seguridad en la etapa de reclutamiento de personal e incluirlas en los acuerdos a firmarse y verificar su cumplimiento durante el desempeño del individuo como empleado.

Garantizar que los usuarios estén al corriente de las amenazas e incumbencias en materia de seguridad de la información, y se encuentren capacitados para respaldar la Política de Seguridad del Organismo en el transcurso de sus tareas normales.

Establecer Compromisos de Confidencialidad con todo el personal y usuarios externos de las instalaciones de procesamiento de información.

Establecer las herramientas y mecanismos necesarios para promover la comunicación de debilidades existentes en materia de seguridad, así como de los incidentes ocurridos, con el objeto de minimizar sus efectos y prevenir su reincidencia.

Alcance

Esta Política se aplica a todo el personal del Organismo, cualquiera sea su situación de revista, y al personal externo que efectúe tareas dentro del ámbito del Organismo.

Responsabilidad

El Responsable del Area de Recursos Humanos incluirá las funciones relativas a la seguridad de la información en las descripciones de puestos de los empleados, informará a todo el personal que ingresa de sus obligaciones respecto del cumplimiento de la Política de Seguridad de la Información, gestionará los Compromisos de Confidencialidad con el personal y coordinará las tareas de capacitación de usuarios respecto de la presente Política.

El Responsable del Area Jurídica participará en la confección del Compromiso de Confidencialidad a firmar por los empleados y terceros que desarrollen funciones en el organismo, en el asesoramiento sobre las sanciones a ser aplicadas por incumplimiento de la presente Política y en el tratamiento de incidentes de seguridad que requieran de su intervención.

Política

8.1 Categoría: Antes del empleo

Objetivo

Asegurar que los empleados, contratistas y terceros entiendan sus responsabilidades, y sean idóneos para los roles para los cuales son considerados; y reducir el riesgo de robo, fraude y mal uso de los medios.

Las responsabilidades de seguridad deben ser tratadas antes del empleo en las definiciones de trabajo adecuadas y en los términos y condiciones del empleo

8.1.1 Control: Funciones y responsabilidades

Las funciones y responsabilidades en materia de seguridad serán incorporadas en la descripción de las responsabilidades de los puestos de trabajo.

Estas incluirán las responsabilidades generales relacionadas con la implementación y el mantenimiento de la Política de Seguridad, y las responsabilidades específicas vinculadas a la protección de cada uno de los activos, o la ejecución de procesos o actividades de seguridad determinadas.

Se definirán y comunicarán claramente los roles y responsabilidades de seguridad a los candidatos para el puesto de trabajo durante el proceso de preselección.

8.1.2 Control: Investigación de antecedentes

Se llevarán a cabo controles de verificación del personal en el momento en que se solicita el puesto. Estos controles incluirán todos los aspectos que indiquen las normas que a tal efecto, alcanzan al Organismo.

Los chequeos de verificación deben incluir:

- a) Disponibilidad de referencias de carácter satisfactorias

- b) Chequeo del currículum vitae del postulante
- c) Confirmación de títulos académicos y profesionales mencionados por el postulante
- d) Acreditación de su identidad

8.1.3 Control: Términos y condiciones de contratación

Como parte de sus términos y condiciones iniciales de empleo, los empleados, cualquiera sea su situación de revista, firmarán un Compromiso de Confidencialidad o no divulgación, en lo que respecta al tratamiento de la información del Organismo. La copia firmada del Compromiso debe ser retenida en forma segura por el Area de Recursos Humanos u otra competente.

Asimismo, mediante el Compromiso de Confidencialidad el empleado declarará conocer y aceptar la existencia de determinadas actividades que pueden ser objeto de control y monitoreo. Estas actividades deben ser detalladas a fin de no violar el derecho a la privacidad del empleado.

Se desarrollará un procedimiento para la suscripción del Compromiso de Confidencialidad donde se incluirán aspectos sobre:

- a) Suscripción inicial del Compromiso por parte de la totalidad del personal.
- b) Revisión del contenido del Compromiso cada ... (indicar período no mayor al año).
- c) Método de re-suscripción en caso de modificación del texto del Compromiso.

Los términos y condiciones de empleo establecerán la responsabilidad del empleado en materia de seguridad de la información.

Cuando corresponda, los términos y condiciones de empleo establecerán que estas responsabilidades se extienden más allá de los límites de la sede del Organismo y del horario normal de trabajo.

Los derechos y obligaciones del empleado relativos a la seguridad de la información, por ejemplo en relación con las leyes de Propiedad Intelectual o la legislación de protección de datos, se encontrarán aclarados e incluidos en los términos y condiciones de empleo.

8.2 Categoría: Durante el empleo

Objetivo

Asegurar que los usuarios empleados, contratistas y terceras personas estén al tanto de las amenazas e inquietudes de la seguridad de la información, sus responsabilidades y obligaciones, y estén equipadas para apoyar la política de seguridad organizacional en el curso de su trabajo normal, y reducir el riesgo de error humano.

Se deben definir las responsabilidades de la gerencia para asegurar que se aplique la seguridad a lo largo de todo el tiempo del empleo de la persona dentro del Organismo.

8.2.1 Control: Responsabilidad de la dirección

La dirección solicitará a los empleados, contratistas y usuarios de terceras partes que apliquen la seguridad en concordancia con las políticas y procedimientos establecidos por la organización, cumpliendo con o siguiente:

- a) estar adecuadamente informados de sus roles y responsabilidades de seguridad de la información antes de que se les otorgue el acceso a información sensible o a los sistemas de información;
- b) ser provistos de guías para establecer las expectativas de seguridad de su rol dentro del Organismo;
- c) ser motivados para cumplir con las políticas de seguridad del Organismo;
- d) alcancen un nivel de conciencia sobre la seguridad acorde con sus roles y responsabilidades dentro del Organismo;
- e) cumplir con las condiciones y términos del empleo, los cuales incluyen las políticas de seguridad de la información del Organismo y métodos adecuados de trabajo;
- f) mantenerse con las habilidades y calificaciones adecuadas.

Si los empleados, contratistas y usuarios no son conscientes de sus responsabilidades de seguridad, ellos pueden causar daños considerables al organismo. Un personal motivado tiene más probabilidades de ser más confiable y causar menos incidentes de seguridad de la información.

8.2.2 Control: Concientización, formación y capacitación en seguridad de la información

Todos los empleados del Organismo y, cuando sea pertinente, los usuarios externos y los terceros que desempeñen funciones en el organismo, recibirán una adecuada capacitación y actualización periódica en materia de la política, normas y procedimientos del Organismo. Esto comprende los requerimientos de seguridad y las responsabilidades legales, así como la capacitación referida al uso correcto de las instalaciones de procesamiento de información y el uso correcto de los recursos en general, como por ejemplo su estación de trabajo.

El Responsable del Area de Recursos Humanos será el encargado de coordinar las acciones de capacitación que surjan de la presente Política.

Cada (indicar periodicidad no mayor a un año) se revisará el material correspondiente a la capacitación, a fin de evaluar la pertinencia de su actualización, de acuerdo al estado del arte de ese momento.

Las siguientes áreas serán encargadas de generar el material de capacitación

Areas Responsables del Material de Capacitación
.....
.....

Adicionalmente, las áreas responsables de generar el material de capacitación dispondrán de información sobre seguridad de la Información para la Administración Pública Nacional en la Coordinación de Emergencias en Redes Teleinformáticas para complementar los materiales por ellas generados.

El personal que ingrese al Organismo recibirá el material, indicándosele el comportamiento esperado en lo que respecta a la seguridad de la información, antes de serle otorgados los privilegios de acceso a los sistemas que correspondan.

Por otra parte, se arbitrarán los medios técnicos necesarios para comunicar a todo el personal, eventuales modificaciones o novedades en materia de seguridad, que deban ser tratadas con un orden preferencial.

8.2.3 Control: Proceso disciplinario

Se seguirá el proceso disciplinario formal contemplado en las normas estatutarias, escalafonarias y convencionales que rigen al personal de la Administración Pública Nacional, para los empleados que violen la Política, Normas y Procedimientos de Seguridad del Organismo.

El proceso disciplinario también se puede utilizar como un elemento disuasivo para evitar que los empleados, contratistas y terceros que violen las políticas y procedimientos de la seguridad del organismo y cualquier otro incumplimiento de la seguridad.

8.3 Categoría: Cese del empleo o cambio de puesto de trabajo

Objetivo

Asegurar que los usuarios empleados, contratistas y terceras personas salgan del Organismo o cambien de empleo de una manera ordenada.

Se deben establecer las responsabilidades para asegurar que la salida del Organismo del usuario empleado, contratista o tercera persona sea manejada y se complete la devolución de todo el equipo y se eliminen todos los derechos de acceso.

8.3.1 Control: Responsabilidad del cese o cambio

Las responsabilidades para realizar la desvinculación o cambio de puesto deben ser claramente definidas y asignadas, incluyendo requerimientos de seguridad y responsabilidades legales a posteriori y, cuando sea apropiado, las responsabilidades contenidas dentro de cualquier acuerdo de confidencialidad, y los términos y condiciones de empleo con continuidad por un período definido de tiempo luego de la finalización del trabajo del empleado, contratista o usuario de tercera parte.

Puede ser necesario informar a los empleados, contratistas y terceros de los cambios en el personal y los acuerdos de operación.

8.3.2 Control: Devolución de activos

Todos los empleados, contratistas y usuarios de terceras partes deben devolver todos los activos de la organización en su poder (software, documentos corporativos, equipamiento, dispositivos de computación móviles, tarjetas de crédito, tarjetas de ingreso, etc.) tras la terminación de su empleo, contrato, o acuerdo.

En los casos donde el empleado, contratista y usuarios tengan conocimiento que es importante para las operaciones actuales, esa información debe ser documentada y transferida al organismo.

8.3.3 Control: Retiro de los derechos de acceso

Se revisarán los derechos de acceso de un individuo a los activos asociados con los sistemas y servicios de información tras la desvinculación, Esto determinará si es necesario remover los derechos de acceso.

Con el cambio de un empleo deben removerse todos los derechos de acceso que no fueron aprobados para el nuevo empleo, comprendiendo esto accesos lógicos y físicos, llaves, tarjetas de identificación, instalaciones de procesamiento de la información, suscripciones, y remoción de cualquier documentación que lo identifique como un miembro corriente del Organismo.

Si un empleado, contratista o usuario de tercera parte que se está desvinculando tiene conocimiento de contraseñas para cuentas que permanecen activas, éstas deben ser cambiadas tras la finalización o cambio de empleo, contrato o acuerdo.

Se evaluará la reducción o eliminación de los derechos de acceso a los activos de la información y a las instalaciones de procesamiento de la información antes de que el empleo termine o cambie, dependiendo de factores de riesgos, tales como:

- a) si la terminación o cambio es iniciado por el empleado, contratista o usuario de tercera parte, o por la gestión y la razón de la finalización;
- b) las responsabilidades actuales del empleado, contratista o cualquier otro usuario;
- c) el valor de los activos accesibles actualmente.

9. Cláusula: Física y Ambiental



Generalidades

La seguridad física y ambiental brinda el marco para minimizar los riesgos de daños e interferencias a la información y a las operaciones del Organismo. Asimismo, pretende evitar al máximo el riesgo de accesos físicos no autorizados, mediante el establecimiento de perímetros de seguridad.

Se distinguen tres conceptos a tener en cuenta: la protección física de accesos, la protección ambiental y el transporte, protección y mantenimiento de equipamiento y documentación.

El establecimiento de perímetros de seguridad y áreas protegidas facilita la implementación de controles tendientes a proteger las instalaciones de procesamiento de información crítica o sensible del Organismo, de accesos físicos no autorizados.

El control de los factores ambientales permite garantizar el correcto funcionamiento de los equipos de procesamiento y minimizar las interrupciones de servicio. Deben contemplarse tanto los riesgos en las instalaciones del Organismo como en instalaciones próximas a la sede del mismo que puedan interferir con las actividades.

El equipamiento donde se almacena información es susceptible de mantenimiento periódico, lo cual implica en ocasiones su traslado y permanencia fuera de las áreas protegidas del Organismo. Dichos procesos deben ser ejecutados bajo estrictas normas de seguridad y de preservación de la información almacenada en los mismos. Así también se tendrá en cuenta la aplicación de dichas normas en equipamiento perteneciente al Organismo pero situado físicamente fuera del mismo ("housing") así como en equipamiento ajeno que albergue sistemas y/o preste servicios de procesamiento de información al Organismo ("hosting").

La información almacenada en los sistemas de procesamiento y la documentación contenida en diferentes medios de almacenamiento, son susceptibles de ser recuperadas mientras no están siendo utilizados. Es por ello que el transporte y la disposición final presentan riesgos que deben ser evaluados.

Gran cantidad de información manejada en las oficinas se encuentra almacenada en papel, por lo que es necesario establecer pautas de seguridad para la conservación de dicha documentación; y para su destrucción cuando así lo amerite.

Objetivo

Prevenir e impedir accesos no autorizados, daños e interferencia a las sedes, instalaciones e información del Organismo.

Proteger el equipamiento de procesamiento de información crítica del Organismo ubicándolo en áreas protegidas y resguardadas por un perímetro de seguridad definido, con medidas de seguridad y controles de acceso apropiados. Asimismo, contemplar la protección del mismo en su traslado y permanencia fuera de las áreas protegidas, por motivos de mantenimiento u otros.

Controlar los factores ambientales que podrían perjudicar el correcto funcionamiento del equipamiento informático que alberga la información del Organismo.

Implementar medidas para proteger la información manejada por el personal en las oficinas, en el marco normal de sus labores habituales.

Proporcionar protección proporcional a los riesgos identificados.

Alcance

Esta Política se aplica a todos los recursos físicos relativos a los sistemas de información del Organismo: instalaciones, equipamiento, cableado, expedientes, medios de almacenamiento, etc.

Responsabilidad

El Responsable de Seguridad de la Información definirá junto con el Responsable del Area Informática y los Propietarios de Información, según corresponda, las medidas de seguridad física y ambiental para el resguardo de los activos críticos, en función a un análisis de riesgos, y controlará su implementación. Asimismo, verificará el cumplimiento de las disposiciones sobre seguridad física y ambiental indicadas en el presente Capítulo.

El Responsable del Area Informática asistirá al Responsable de Seguridad de la Información en la definición de las medidas de seguridad a implementar en áreas protegidas, y coordinará su implementación. Asimismo, controlará el mantenimiento del equipamiento informático de acuerdo a las indicaciones de proveedores tanto dentro como fuera de las instalaciones del Organismo.

Los Responsables de Unidades Organizativas definirán los niveles de acceso físico del personal del organismo a las áreas restringidas bajo su responsabilidad.

Los Propietarios de la Información autorizarán formalmente el trabajo fuera de las instalaciones con información de su incumbencia a los empleados del Organismo cuando lo crean conveniente.

La Unidad de Auditoría Interna o en su defecto quien sea propuesto por el Comité de Seguridad de la Información revisará los registros de acceso a las áreas protegidas.

Todo el personal del Organismo es responsable del cumplimiento de la política de pantallas y escritorios limpios, para la protección de la información relativa al trabajo diario en las oficinas.

Política

9.1 Categoría: Areas Seguras

Objetivo

Evitar el acceso físico no autorizado, daño e interferencia con la información y los locales del Organismo.

Los medios de procesamiento de información crítica o confidencial deben ubicarse en áreas seguras, protegidas por los perímetros de seguridad definidos, con las barreras de seguridad y controles de entrada apropiados. Deben estar físicamente protegidos del acceso no autorizado, daño e interferencia.

9.1.1 Control: Perímetro de seguridad física

La protección física se llevará a cabo mediante la creación de diversas barreras o medidas de control físicas alrededor de las sedes del Organismo y de las instalaciones de procesamiento de información.

El Organismo utilizará perímetros de seguridad para proteger las áreas que contienen instalaciones de procesamiento de información, de suministro de energía eléctrica, de aire acondicionado, y cualquier otra área considerada crítica para el correcto funcionamiento de los sistemas de información. Un perímetro de seguridad está delimitado por una barrera, por ejemplo una pared, una puerta de acceso controlado por dispositivo de autenticación o un escritorio u oficina de recepción atendidos por personas. El emplazamiento y la fortaleza de cada barrera estarán definidas por el Responsable del Area Informática con el asesoramiento del Responsable de Seguridad de la Información, de acuerdo a la evaluación de riesgos efectuada.

Se considerarán e implementarán los siguientes lineamientos y controles, según corresponda:

a) Definir y documentar claramente el perímetro de seguridad.

b) Ubicar las instalaciones de procesamiento de información dentro del perímetro de un edificio o área de construcción físicamente sólida (por ejemplo no deben existir aberturas en el perímetro o áreas

donde pueda producirse fácilmente una irrupción). Las paredes externas del área deben ser sólidas y todas las puertas que comunican con el exterior deben estar adecuadamente protegidas contra accesos no autorizados, por ejemplo mediante mecanismos de control, vallas, alarmas, cerraduras, etc.

c) Verificar la existencia de un área de recepción atendida por personal. Si esto no fuera posible se implementarán los siguientes medios alternativos de control de acceso físico al área o edificio:..... (indicar otros medios alternativos de control). El acceso a dichas áreas y edificios estará restringido exclusivamente al personal autorizado. Los métodos implementados registrarán cada ingreso y egreso en forma precisa.

d) Extender las barreras físicas necesarias desde el piso (real) hasta el techo (real), a fin de impedir el ingreso no autorizado y la contaminación ambiental, por ejemplo por incendio, humedad e inundación.

e) Identificar claramente todas las puertas de incendio de un perímetro de seguridad.

Un área segura puede ser una oficina con llave, o varias oficinas rodeadas por una barrera de seguridad física interna continua. Pueden ser necesarios barreras y perímetros adicionales para controlar el acceso físico entre las áreas con diferentes requerimientos de seguridad, dentro del mismo perímetro de seguridad

El Responsable de Seguridad de la Información llevará un registro actualizado de los sitios protegidos, indicando:

a) Identificación del Edificio y Area.

b) Principales elementos a proteger.

c) Medidas de protección física

9.1.2 Control: Controles físicos de entrada

Las áreas protegidas se resguardarán mediante el empleo de controles de acceso físico, los que serán determinados por el Responsable de Seguridad de la Información junto con el Responsable del Area Informática, a fin de permitir el acceso sólo al personal autorizado. Estos controles de acceso físico tendrán, por lo menos, las siguientes características:

a) Supervisar o inspeccionar a los visitantes a áreas protegidas y registrar la fecha y horario de su ingreso y egreso. Sólo se permitirá el acceso mediando propósitos específicos y autorizados e instruyéndose al visitante en el momento de ingreso sobre los requerimientos de seguridad del área y los procedimientos de emergencia.

b) Controlar y limitar el acceso a la información clasificada y a las instalaciones de procesamiento de información, exclusivamente a las personas autorizadas. Se utilizarán los siguientes controles de autenticación para autorizar y validar todos los accesos:..... (por ejemplo: personal de guardia con listado de personas habilitadas o por tarjeta magnética o inteligente y número de identificación personal (PIN), etc.). Se mantendrá un registro protegido para permitir auditar todos los accesos.

c) Implementar el uso de una identificación unívoca visible para todo el personal del área protegida e instruirlo acerca de cuestionar la presencia de desconocidos no escoltados por personal autorizado y a cualquier persona que no exhiba una identificación visible.

d) Revisar y actualizar cada (definir período no mayor a 6 meses) los derechos de acceso a las áreas protegidas, los que serán documentados y firmados por el Responsable de la Unidad Organizativa de la que dependa.

e) Revisar los registros de acceso a las áreas protegidas. Esta tarea la realizará la Unidad de Auditoría Interna o en su defecto quien sea propuesto por el Comité de Seguridad de la Información.

9.1.3 Control: Seguridad de oficinas, despachos, instalaciones

Para la selección y el diseño de un área protegida se tendrá en cuenta la posibilidad de daño producido por incendio, inundación, explosión, agitación civil, y otras formas de desastres naturales o provocados por el hombre. También se tomarán en cuenta las disposiciones y normas (estándares) en materia de sanidad y seguridad. Asimismo, se considerarán las amenazas a la seguridad que representan los edificios y zonas aledañas, por ejemplo, filtración de agua desde otras instalaciones.

Se definen los siguientes sitios como áreas protegidas del Organismo

Áreas Protegidas
.....
.....

Se establecen las siguientes medidas de protección para áreas protegidas:

a) Ubicar las instalaciones críticas en lugares a los cuales no pueda acceder personal no autorizado.

b) Establecer que los edificios o sitios donde se realicen actividades de procesamiento de información serán discretos y ofrecerán un señalamiento mínimo de su propósito, sin signos obvios, exteriores o interiores.

c) Ubicar las funciones y el equipamiento de soporte, por ejemplo: impresoras, fotocopiadoras, máquinas de fax, adecuadamente dentro del área protegida para evitar solicitudes de acceso, el cual podría comprometer la información.

d) Establecer que las puertas y ventanas permanecerán cerradas cuando no haya vigilancia. Se agregará protección externa a las ventanas, en particular las que se encuentran en planta baja o presenten riesgos especiales.

e) Implementar los siguientes mecanismos de control para la detección de intrusos: (detallar cuáles). Los mismos serán instalados según estándares profesionales y probados periódicamente. Estos mecanismos de control comprenderán todas las puertas exteriores y ventanas accesibles.

f) Separar las instalaciones de procesamiento de información administradas por el Organismo de aquellas administradas por terceros.

g) Restringir el acceso público a las guías telefónicas y listados de teléfonos internos que identifican las ubicaciones de las instalaciones de procesamiento de información sensible.

h) Almacenar los materiales peligrosos o combustibles en los siguientes lugares seguros a una distancia prudencial de las áreas protegidas del Organismo: (incluir lista de lugares seguros). Los suministros, como los útiles de escritorio, no serán trasladados al área protegida hasta que sean requeridos.

i) Almacenar los equipos redundantes y la información de resguardo (back up) en un sitio seguro y distante del lugar de procesamiento, para evitar daños ocasionados ante eventuales contingencias en el sitio principal: (detallar ubicación).

9.1.4 Control: Protección contra amenazas externas y de origen ambiental

Se debe asignar y aplicar protección física contra daño por fuego, inundación, terremoto, explosión, revuelta civil y otras formas de desastres naturales o causados por el hombre.

Se debe prestar consideración a cualquier amenaza contra la seguridad presentada por locales vecinos; por ejemplo, un fuego en un edificio vecino, escape de agua en el techo o pisos en sótano o una explosión en la calle.

Se debe considerar los siguientes lineamientos para evitar el daño por fuego, inundación, terremoto, explosión, revuelta civil y otras formas de desastres naturales o causados por el hombre:

a) los materiales peligrosos o combustibles deben ser almacenados a una distancia segura del área asegurada. Los suministros a granel como papelería no deben almacenarse en el área asegurada;

b) el equipo de reemplazo y los medios de respaldo debieran ubicarse a una distancia segura para evitar el daño de un desastre que afecte el local principal;

c) se debe proporcionar equipo contra-incendios ubicado adecuadamente.

9.1.5 Control: Trabajo en áreas seguras

Para incrementar la seguridad de las áreas protegidas, se establecen los siguientes controles y lineamientos adicionales. Esto incluye controles para el personal que trabaja en el área protegida, así como para las actividades de terceros que tengan lugar allí:

a) Dar a conocer al personal la existencia del área protegida, o de las actividades que allí se llevan a cabo, sólo si es necesario para el desarrollo de sus funciones.

b) Evitar la ejecución de trabajos por parte de terceros sin supervisión.

c) Bloquear físicamente e inspeccionar periódicamente las áreas protegidas desocupadas.

d) Limitar el acceso al personal del servicio de soporte externo a las áreas protegidas o a las instalaciones de procesamiento de información sensible. Este acceso, como el de cualquier otra persona ajena que requiera acceder al área protegida, será otorgado solamente cuando sea necesario y se encuentre autorizado y monitoreado. Se mantendrá un registro de todos los accesos de personas ajenas.

e) Pueden requerirse barreras y perímetros adicionales para controlar el acceso físico entre áreas con diferentes requerimientos de seguridad, y que están ubicadas dentro del mismo perímetro de seguridad.

f) Impedir el ingreso de equipos de computación móvil, fotográficos, de vídeo, audio o cualquier otro tipo de equipamiento que registre información, a menos que hayan sido formalmente autorizadas por el Responsable de dicho área o el Responsable del Área Informática y el Responsable de Seguridad de la Información.

g) Prohibir comer, beber y fumar dentro de las instalaciones de procesamiento de la información.

9.1.6 Control: Áreas de acceso público, de carga y descarga

Se controlarán las áreas de Recepción y Distribución, las cuales estarán aisladas de las instalaciones de procesamiento de información, a fin de impedir accesos no autorizados.

Para ello se establecerán controles físicos que considerarán los siguientes lineamientos:

a) Limitar el acceso a las áreas de depósito, desde el exterior de la sede del Organismo, sólo al personal previamente identificado y autorizado.

b) Diseñar el área de depósito de manera tal que los suministros puedan ser descargados sin que el personal que realiza la entrega acceda a otros sectores del edificio.

c) Proteger todas las puertas exteriores del depósito cuando se abre la puerta interna.

d) Inspeccionar el material entrante para descartar peligros potenciales antes de ser trasladado desde el área de depósito hasta el lugar de uso.

e) Registrar el material entrante al ingresar al sitio pertinente.

f) Cuando fuese posible, el material entrante debe estar segregado o separado en sus diferentes partes que lo constituyan.

9.2 Categoría: Seguridad de los equipos

Objetivo

Evitar pérdida, daño, robo o compromiso de los activos y la interrupción de las actividades del Organismo.

Se debe proteger el equipo de amenazas físicas y ambientales.

9.2.1 Control: emplazamiento y protección de equipos

El equipamiento será ubicado y protegido de tal manera que se reduzcan los riesgos ocasionados por amenazas y peligros ambientales, y las oportunidades de acceso no autorizado, teniendo en cuenta los siguientes puntos:

a) Ubicar el equipamiento en un sitio donde se minimice el acceso innecesario y provea un control de acceso adecuado.

b) Ubicar las instalaciones de procesamiento y almacenamiento de información que manejan datos clasificados, en un sitio que permita la supervisión durante su uso.

c) Aislar los elementos que requieren protección especial para reducir el nivel general de protección requerida.

d) Adoptar controles adecuados para minimizar el riesgo de amenazas potenciales, por:

Amenazas Potenciales	Controles
Robo o hurto	
Incendio	
Explosivos	
Humo	
Inundaciones o filtraciones de agua (o falta de suministro)	
Polvo	
Vibraciones	
Efectos químicos	
Interferencia en el suministro de energía eléctrica (cortes de suministro, variación de tensión)	
Radiación electromagnética	
Derrumbes	
.....	

e) Se deben establecer lineamientos sobre las actividades de comer, beber y fumar en la proximidad de los medios de procesamiento de la información.

f) Revisar regularmente las condiciones ambientales para verificar que las mismas no afecten de manera adversa el funcionamiento de las instalaciones de procesamiento de la información. Esta revisión se realizará cada:(indicar periodicidad, no mayor a seis meses).

g) Se deben aplicar protección contra rayos a todos los edificios y se deben adaptar filtros de protección contra rayos a todas las líneas de ingreso de energía y comunicaciones.

h) Considerar asimismo el impacto de las amenazas citadas en el punto d) que tengan lugar en zonas próximas a la sede del Organismo.

9.2.2 Control: Instalaciones de suministro

El equipamiento estará protegido con respecto a las posibles fallas en el suministro de energía u otras anomalías eléctricas. El suministro de energía estará de acuerdo con las especificaciones del fabricante o proveedor de cada equipo. Para asegurar la continuidad del suministro de energía, se contemplarán las siguientes medidas de control:

a) Disponer de múltiples enchufes o líneas de suministro para evitar un único punto de falla en el suministro de energía.

b) Contar con un suministro de energía ininterrumpible (UPS) para asegurar el apagado regulado y sistemático o la ejecución continua del equipamiento que sustenta las operaciones críticas del Organismo. La determinación de dichas operaciones críticas, será el resultado del análisis de impacto realizado por el Responsable de Seguridad de la Información conjuntamente con los Propietarios de la Información con incumbencia. Los planes de contingencia contemplarán las acciones que han de emprenderse ante una falla de la UPS. Los equipos de UPS serán inspeccionados y probados periódicamente para asegurar que funcionan correctamente y que tienen la autonomía requerida.

c) Montar un generador de respaldo para los casos en que el procesamiento deba continuar ante una falla prolongada en el suministro de energía. Debe realizarse un análisis de impacto de las posibles consecuencias ante una interrupción prolongada del procesamiento, con el objeto de definir qué componentes será necesario abastecer de energía alternativa. Dicho análisis será realizado por el Responsable de Seguridad de la Información conjuntamente con los Propietarios de la Información. Se dispondrá de un adecuado suministro de combustible para garantizar que el generador pueda funcionar por un período prolongado. Cuando el encendido de los generadores no sea automático, se asegurará que el tiempo de funcionamiento de la UPS permita el encendido manual de los mismos. Los generadores serán inspeccionados y probados periódicamente para asegurar que funcionen según lo previsto.

Asimismo, se procurará que los interruptores de emergencia se ubiquen cerca de las salidas de emergencia de las salas donde se encuentra el equipamiento, a fin de facilitar un corte rápido de la energía en caso de producirse una situación crítica. Se proveerá de iluminación de emergencia en caso de producirse una falla en el suministro principal de energía. Se implementará protección contra descargas eléctricas en todos los edificios y líneas de comunicaciones externas de acuerdo a las normativas vigentes.

Las opciones para lograr la continuidad de los suministros de energía incluyen múltiples alimentaciones para evitar que una falla en el suministro de energía.

9.2.3 Control: Seguridad del cableado

El cableado de energía eléctrica y de comunicaciones que transporta datos o brinda apoyo a los servicios de información estará protegido contra interceptación o daño, mediante las siguientes acciones:

a) Cumplir con los requisitos técnicos vigentes de la República Argentina.

b) Utilizar pisoducto o cableado embutido en la pared, siempre que sea posible, cuando corresponda a las instalaciones de procesamiento de información. En su defecto estarán sujetas a la siguiente protección alternativa:(indicar protección alternativa del cableado).

c) Proteger el cableado de red contra interceptación no autorizada o daño mediante los siguientes controles: ... (ejemplo: el uso de conductos o evitando trayectos que atraviesen áreas públicas).

d) Separar los cables de energía de los cables de comunicaciones para evitar interferencias.

e) Proteger el tendido del cableado troncal (backbone) mediante la utilización de ductos blindados.

Para los sistemas sensibles o críticos y (detallar cuáles son), se implementarán los siguientes controles adicionales:

- a) Instalar conductos blindados y recintos o cajas con cerradura en los puntos terminales y de inspección.
- b) Utilizar rutas o medios de transmisión alternativos.

9.2.4 Control: Mantenimiento de los equipos

Se realizará el mantenimiento del equipamiento para asegurar su disponibilidad e integridad permanentes. Para ello se debe considerar:

- a) Someter el equipamiento a tareas de mantenimiento preventivo, de acuerdo con los intervalos de servicio y especificaciones recomendados por el proveedor y con la autorización formal del Responsables del Area Informática. El Area de Informática mantendrá un listado actualizado del equipamiento con el detalle de la frecuencia en que se realizará el mantenimiento preventivo.
- b) Establecer que sólo el personal de mantenimiento autorizado puede brindar mantenimiento y llevar a cabo reparaciones en el equipamiento.
- c) Registrar todas las fallas supuestas o reales y todo el mantenimiento preventivo y correctivo realizado.
- d) Registrar el retiro de equipamiento de la sede del Organismo para su mantenimiento.
- e) Eliminar la información confidencial que contenga cualquier equipamiento que sea necesario retirar, realizándose previamente las respectivas copias de resguardo.

9.2.5 Control: Seguridad de los equipos fuera de las instalaciones

El uso de equipamiento destinado al procesamiento de información, fuera del ámbito del Organismo, será autorizado por el responsable patrimonial. En el caso de que en el mismo se almacene información clasificada, debe ser aprobado además por el Propietario de la misma. La seguridad provista debe ser equivalente a la suministrada dentro del ámbito del Organismo para un propósito similar, teniendo en cuenta los riesgos de trabajar fuera de la misma.

Se respetarán permanentemente las instrucciones del fabricante respecto del cuidado del equipamiento. Asimismo, se mantendrá una adecuada cobertura de seguro para proteger el equipamiento fuera del ámbito del Organismo, cuando sea conveniente.

Los riesgos de seguridad, por ejemplo: daño, robo o interceptación; puede variar considerablemente entre los edificios y se debe tomarlo en cuenta para evaluar los controles apropiados.

9.2.6 Control: Reutilización o retiro seguro de equipos

La información puede verse comprometida por una desafectación o una reutilización descuidada del equipamiento. Los medios de almacenamiento conteniendo material sensible, por ejemplo discos rígidos no removibles, serán físicamente destruidos o sobrescritos en forma segura en lugar de utilizar las funciones de borrado estándar, según corresponda.

Los dispositivos que contengan información confidencial deben requerir una evaluación de riesgo para determinar si los ítems debieran ser físicamente destruidos en lugar de enviarlos a reparar o descartar.

9.2.7 Control: Retirada de materiales propiedad de la empresa

El equipamiento, la información y el software no serán retirados de la sede del Organismo sin autorización formal.

Periódicamente, se llevarán a cabo comprobaciones puntuales para detectar el retiro no autorizado de activos del Organismo, las que serán llevadas a cabo por (indicar el Area responsable). El personal será puesto en conocimiento de la posibilidad de realización de dichas comprobaciones.

Los empleados deben saber que se llevan a cabo chequeos inesperados, y los chequeos se deben realizar con la debida autorización de los requerimientos legales y reguladores.

9.2.8 Políticas de Escritorios y Pantallas Limpias. Se adopta una política de escritorios limpios para proteger documentos en papel y dispositivos de almacenamiento removibles y una política de pantallas limpias en las instalaciones de procesamiento de información, a fin de reducir los riesgos de acceso no autorizado, pérdida y daño de la información, tanto durante el horario normal de trabajo como fuera del mismo.

Se aplicarán los siguientes lineamientos:

- a) Almacenar bajo llave, cuando corresponda, los documentos en papel y los medios informáticos, en gabinetes y/u otro tipo de mobiliario seguro cuando no están siendo utilizados, especialmente fuera del horario de trabajo.
- b) Guardar bajo llave la información sensible o crítica del Organismo (preferentemente en una caja fuerte o gabinete a prueba de incendios) cuando no está en uso, especialmente cuando no hay personal en la oficina.
- c) Desconectar de la red/sistema/servicio las computadoras personales, terminales e impresoras asignadas a funciones críticas, cuando están desatendidas. Las mismas deben ser protegidas mediante cerraduras de seguridad, contraseñas u otros controles cuando no están en uso (como por ejemplo la utilización de protectores de pantalla con contraseña). Los responsables de cada área mantendrán un registro de las contraseñas o copia de las llaves de seguridad utilizadas en el sector a su cargo. Tales elementos se encontrarán protegidos en sobre cerrado o caja de seguridad para impedir accesos no autorizados, debiendo dejarse constancia de todo acceso a las mismas, y de los motivos que llevaron a tal acción.
- d) Proteger los puntos de recepción y envío de correo postal y las máquinas de fax no atendidas.
- e) Bloquear las fotocopadoras (o protegerlas de alguna manera del uso no autorizado) fuera del horario normal de trabajo.
- f) Retirar inmediatamente la información sensible o confidencial, una vez impresa.

10. Cláusula: Gestión de Comunicaciones y Operaciones



Generalidades

La proliferación de software malicioso, como virus, troyanos, etc., hace necesario que se adopten medidas de prevención, a efectos de evitar la ocurrencia de tales amenazas.

Es conveniente separar los ambientes de desarrollo, prueba y operaciones de los sistemas del Organismo, estableciendo procedimientos que aseguren la calidad de los procesos que se implementen en el ámbito operativo, a fin de minimizar los riesgos de incidentes producidos por la manipulación de información operativa.

Los sistemas de información están comunicados entre sí, tanto dentro del Organismo como con terceros fuera de él. Por lo tanto es necesario establecer criterios de seguridad en las comunicaciones que se establezcan.

Las comunicaciones establecidas permiten el intercambio de información, que debe estar regulado para garantizar las condiciones de confidencialidad, integridad y disponibilidad de la información que se emite o recibe por los distintos canales.

Objetivo

Garantizar el funcionamiento correcto y seguro de las instalaciones de procesamiento de la información y comunicaciones.

Establecer responsabilidades y procedimientos para su gestión y operación, incluyendo instrucciones operativas, procedimientos para la respuesta a incidentes y separación de funciones.

Alcance

Todas las instalaciones de procesamiento y transmisión de información del Organismo.

Responsabilidad

El Responsable de Seguridad de la información tendrá a su cargo, entre otros:

- Definir procedimientos para el control de cambios a los procesos operativos documentados, los sistemas e instalaciones de procesamiento de información, y verificar su cumplimiento, de manera que no afecten la seguridad de la información.
- Establecer criterios de aprobación para nuevos sistemas de información, actualizaciones y nuevas versiones, contemplando la realización de las pruebas necesarias antes de su aprobación definitiva. Verificar que dichos procedimientos de aprobación de software incluyan aspectos de seguridad para todas las aplicaciones.
- Definir procedimientos para el manejo de incidentes de seguridad y para la administración de los medios de almacenamiento.
- Definir y documentar una norma clara con respecto al uso del correo electrónico.
- Controlar los mecanismos de distribución y difusión de información dentro del Organismo.
- Definir y documentar controles para la detección y prevención del acceso no autorizado, la protección contra software malicioso y para garantizar la seguridad de los datos y los servicios conectados en las redes del Organismo.
- Desarrollar procedimientos adecuados de concientización de usuarios en materia de seguridad, controles de acceso al sistema y administración de cambios.
- Verificar el cumplimiento de las normas, procedimientos y controles establecidos.

El Responsable del Area Informática tendrá a su cargo lo siguiente:

- Controlar la existencia de documentación actualizada relacionada con los procedimientos de comunicaciones y operaciones.
- Evaluar el posible impacto operativo de los cambios previstos a sistemas y equipamiento y verificar su correcta implementación, asignando responsabilidades.
- Administrar los medios técnicos necesarios para permitir la segregación de los ambientes de procesamiento.
- Monitorear las necesidades de capacidad de los sistemas en operación y proyectar las futuras demandas de capacidad, a fin de evitar potenciales amenazas a la seguridad del sistema o a los servicios del usuario.
- Controlar la realización de las copias de resguardo de información, así como la prueba periódica de su restauración.
- Asegurar el registro de las actividades realizadas por el personal operativo, para su posterior revisión.
- Desarrollar y verificar el cumplimiento de procedimientos para comunicar las fallas en el procesamiento de la información o los sistemas de comunicaciones, que permita tomar medidas correctivas.
- Implementar los controles de seguridad definidos (software malicioso y accesos no autorizados).
- Definir e implementar procedimientos para la administración de medios informáticos de almacenamiento, como cintas, discos, casetes e informes impresos y para la eliminación segura de los mismos.
- Participar en el tratamiento de los incidentes de seguridad, de acuerdo a los procedimientos establecidos.

El Responsable de Seguridad de la información junto con el Responsable del Area Informática y el Responsable del Area Jurídica del Organismo evaluarán los contratos y acuerdos con terceros para garantizar la incorporación de consideraciones relativas a la seguridad de la información involucrada en la gestión de los productos o servicios prestados.

Cada Propietario de la Información, junto con el Responsable de Seguridad de la Información y el Responsable del Area Informática, determinará los requerimientos para resguardar la información por la cual es responsable. Asimismo, aprobará los servicios de mensajería autorizados para transportar la información cuando sea requerido, de acuerdo a su nivel de criticidad.

La Unidad de Auditoría Interna o en su defecto quien sea propuesto por el Comité de Seguridad de la Información, revisará las actividades que no hayan sido posibles segregar. Asimismo, revisará los registros de actividades del personal operativo.

Política

10.1 Categoría: Procedimientos y Responsabilidades Operativas

Objetivo

Asegurar la operación correcta y segura de los medios de procesamiento de la información.

Se deben establecer las responsabilidades y procedimientos para la gestión y operación de todos los medios de procesamiento de la información. Esto incluye el desarrollo de los procedimientos de operación apropiados.

10.1.1 Control: Documentación de los Procedimientos Operativos

Se documentarán y mantendrán actualizados los procedimientos operativos identificados en esta Política y sus cambios serán autorizados por el Responsable de Seguridad de la Información.

Los procedimientos especificarán instrucciones para la ejecución detallada de cada tarea, incluyendo:

- a) Procesamiento y manejo de la información.
- b) Requerimientos de programación de procesos, interdependencias con otros sistemas, tiempos de inicio de las primeras tareas y tiempos de terminación de las últimas tareas.
- c) Instrucciones para el manejo de errores u otras condiciones excepcionales que puedan surgir durante la ejecución de tareas.
- d) Restricciones en el uso de utilitarios del sistema.
- e) Personas de soporte a contactar en caso de dificultades operativas o técnicas imprevistas.
- f) Instrucciones especiales para el manejo de "salidas", como el uso de papelería especial o la administración de salidas confidenciales, incluyendo procedimientos para la eliminación segura de salidas fallidas de tareas.
- g) Reinicio del sistema y procedimientos de recuperación en caso de producirse fallas en el sistema.

Se preparará adicionalmente documentación sobre procedimientos referidos a las siguientes actividades:

- a) Instalación y mantenimiento de equipamiento para el procesamiento de información y comunicaciones.
- b) Instalación y mantenimiento de las plataformas de procesamiento.
- c) Monitoreo del procesamiento y las comunicaciones.
- d) Inicio y finalización de la ejecución de los sistemas.
- e) Programación y ejecución de procesos.
- f) Gestión de servicios.
- g) Resguardo de información.
- h) Gestión de incidentes de seguridad en el ambiente de procesamiento y comunicaciones.
- i) Reemplazo o cambio de componentes del ambiente de procesamiento y comunicaciones.
- j) Uso del correo electrónico.

10.1.2 Control: Cambios en las Operaciones

Se definirán procedimientos para el control de los cambios en el ambiente operativo y de comunicaciones. Todo cambio debe ser evaluado previamente en aspectos técnicos y de seguridad.

El Responsable de Seguridad de la Información controlará que los cambios en los componentes operativos y de comunicaciones no afecten la seguridad de los mismos ni de la información que soportan. El Responsable del Area Informática evaluará el posible impacto operativo de los cambios previstos y verificará su correcta implementación.

Se retendrá un registro de auditoría que contenga toda la información relevante de cada cambio implementado.

Los procedimientos de control de cambios contemplarán los siguientes puntos:

- a) Identificación y registro de cambios significativos.
- b) Evaluación del posible impacto de dichos cambios.
- c) Aprobación formal de los cambios propuestos.
- d) Planificación del proceso de cambio.
- e) Prueba del nuevo escenario.
- f) Comunicación de detalles de cambios a todas las personas pertinentes.

g) Identificación de las responsabilidades por la cancelación de los cambios fallidos y la recuperación respecto de los mismos.

10.1.3 Control: Separación de Funciones

Se separará la gestión o ejecución de ciertas tareas o áreas de responsabilidad, a fin de reducir el riesgo de modificaciones no autorizadas o mal uso de la información o los servicios por falta de independencia en la ejecución de funciones críticas.

Si este método de control no se pudiera cumplir en algún caso, se implementarán controles como:

- a) Monitoreo de las actividades.
- b) Registros de auditoría y control periódico de los mismos.
- c) Supervisión por parte de la Unidad de Auditoría Interna o en su defecto quien sea propuesto a tal efecto, siendo independiente al área que genera las actividades auditadas.

Asimismo, se documentará la justificación formal por la cual no fue posible efectuar la segregación de funciones.

Se asegurará la independencia de las funciones de auditoría de seguridad, tomando recaudos para que ninguna persona pueda realizar actividades en áreas de responsabilidad única sin ser monitoreada, y la independencia entre el inicio de un evento y su autorización, considerando los siguientes puntos:

- a) Separar actividades que requieren connivencia para defraudar, por ejemplo efectuar una orden de compra y verificar que la mercadería fue recibida.
- b) Diseñar controles, si existe peligro de connivencia de manera tal que dos o más personas estén involucradas, reduciendo la posibilidad de conspiración.

10.1.4 Control: Separación entre Instalaciones de Desarrollo e Instalaciones Operativas

Los ambientes de desarrollo, prueba y operaciones, siempre que sea posible, estarán separados preferentemente en forma física, y se definirán y documentarán las reglas para la transferencia de software desde el estado de desarrollo hacia el estado productivo.

Para ello, se tendrán en cuenta los siguientes controles:

- a) Ejecutar el software de desarrollo y de producción, en diferentes ambientes de operaciones, equipos, o directorios.
- b) Separar las actividades de desarrollo y prueba, en entornos diferentes.
- c) Impedir el acceso a los compiladores, editores y otros utilitarios del sistema en el ambiente de producción, cuando no sean indispensables para el funcionamiento del mismo.
- d) Utilizar sistemas de autenticación y autorización independientes para los diferentes ambientes, así como perfiles de acceso a los sistemas. Prohibir a los usuarios compartir contraseñas en estos sistemas. Las interfaces de los sistemas identificarán claramente a qué instancia se está realizando la conexión.
- e) Definir propietarios de la información para cada uno de los ambientes de procesamiento existentes.
- f) El personal de desarrollo no tendrá acceso al ambiente productivo. De ser extrema dicha necesidad, se establecerá un procedimiento de emergencia para la autorización, documentación y registro de dichos accesos.

Para el caso que no puedan mantener separados los distintos ambientes en forma física, deben implementarse los controles indicados en el punto "10.1.3 Control: Separación de Funciones".

En el Anexo al capítulo 12 se presenta un esquema modelo de segregación de ambientes de procesamiento.

10.2 Categoría: Gestión de Provisión de Servicios

Objetivo

Implementar y mantener el nivel apropiado de seguridad de la información y la entrega del servicio en línea con los acuerdos de entrega de servicios de terceros.

La organización debe chequear la implementación de los acuerdos, monitorear su cumplimiento con los estándares y manejar los cambios para asegurar que los servicios sean entregados para satisfacer todos los requerimientos acordados por la tercera persona.

10.2.1 Control: Provisión de servicio

Se verificará que los servicios brindados por una tercera parte incluyan los acuerdos de seguridad arreglados, definiciones de servicio, y aspectos de la gestión del servicio. En el caso de acuerdos de tercerización, el Organismo debe planificar las transiciones necesarias (de la información, de las instalaciones de procesamiento de información, y cualquier otro componente que necesite ser trasladado), y que asegure que la seguridad es mantenida a lo largo del período de transición.

En el caso de tercerizar la administración de las instalaciones de procesamiento, se acordarán controles con el proveedor del servicio y se incluirán en el contrato, contemplando las siguientes cuestiones específicas (Ver 6-2-2 Control: Puntos de seguridad de la información a considerar en Contratos o Acuerdos con terceros):

- a) Identificar las aplicaciones sensibles o críticas que convenga retener en el Organismo.
- b) Obtener la aprobación de los propietarios de aplicaciones específicas.
- c) Identificar las implicancias para la continuidad de los planes de las actividades del Organismo.
- d) Especificar las normas de seguridad y el proceso de medición del cumplimiento.
- e) Asignar funciones específicas y procedimientos para monitorear todas las actividades de seguridad.

f) Definir las funciones y procedimientos de comunicación y manejo de incidentes relativos a la seguridad.

Dichas consideraciones deben ser acordadas entre el Responsable de Seguridad de la Información, el Responsable del Área de Informática y el Responsable del Área Jurídica del Organismo.

10.2.2 Control: Seguimiento y revisión de los servicios de las terceras partes

Se llevará a cabo el seguimiento, control y revisión de los servicios de las terceras partes asegurando que se encuentran adheridos a los términos de seguridad de la información y las condiciones definidas en los acuerdos, y que los incidentes de seguridad de la información y los problemas son manejados en forma apropiada.

El Organismo mantendrá control suficiente y visión general de todos los aspectos de seguridad para la información sensible o crítica, o de las instalaciones de procesamiento de información accedidas, procesadas o gestionadas por una tercera parte. Se recomienda que la organización asegure que se mantenga la visibilidad de las actividades de seguridad como gestión de cambios, identificación de vulnerabilidades y reporte/respuesta de incidentes de seguridad de información a través de un proceso de reportes claro y definido, con formato y estructura.

10.2.3 Control: Gestión del cambio de los servicios de terceras partes

Se gestionarán los cambios en la provisión de los servicios, incluyendo el mantenimiento y las mejoras de las políticas, procedimientos y controles de seguridad de la información existentes, teniendo en cuenta la criticidad de los sistemas y procesos del negocio involucrados y la reevaluación de los riesgos.

El proceso de gestión del cambio de un servicio de tercera parte necesita tener cuenta:

- Los cambios realizados por la organización para implementar:
 - mejoras a los servicios corrientes ofrecidos;
 - desarrollo de cualquier aplicaciones y sistemas nuevos;
 - modificaciones o actualizaciones de las políticas y procedimientos del Organismo;
 - nuevos controles para resolver los incidentes de la seguridad de la información y para mejorar la seguridad;

- cambios en los servicios de las terceras partes para implementar:

- cambios y mejoras de las redes;
- uso de nuevas tecnologías;
- adopción de nuevos productos o nuevas versiones/publicaciones;
- nuevas herramientas de desarrollo y ambientes;
- cambios de las ubicaciones físicas de las instalaciones de servicio;
- cambio de los vendedores.

10.3 Categoría: Planificación y Aprobación de Sistemas

Objetivo

Minimizar el riesgo de fallas en los sistemas. Se requiere planificación y preparación anticipadas para asegurar la disponibilidad de la capacidad y los recursos adecuados para entregar el desempeño del sistema requerido.

Se deben realizar proyecciones de los requerimientos de la capacidad futura para reducir el riesgo de sobrecarga en el sistema.

Se deben establecer, documentar y probar los requerimientos operacionales de los sistemas nuevos antes de su aceptación y uso.

10.3.1 Control: Planificación de la Capacidad

El Responsable del Área Informática, o el personal que éste designe, efectuará el monitoreo de las necesidades de capacidad de los sistemas en operación y proyectar las futuras demandas, a fin de garantizar un procesamiento y almacenamiento adecuados. Para ello tomará en cuenta además los nuevos requerimientos de los sistemas así como las tendencias actuales y proyectadas en el procesamiento de la información del Organismo para el período estipulado de vida útil de cada componente. Asimismo, informará las necesidades detectadas a las autoridades competentes para que puedan identificar y evitar potenciales cuellos de botella, que podrían plantear una amenaza a la seguridad o a la continuidad del procesamiento, y puedan planificar una adecuada acción correctiva.

10.3.2 Control: Aprobación del Sistema

El Responsable del Área Informática y el Responsable de Seguridad de la Información sugerirán criterios de aprobación para nuevos sistemas de información, actualizaciones y nuevas versiones, solicitando la realización de las pruebas necesarias antes de su aprobación definitiva. Se deben considerar los siguientes puntos:

- a) Verificar el impacto en el desempeño y los requerimientos de capacidad de las computadoras.
- b) Garantizar la recuperación ante errores.
- c) Preparar y poner a prueba los procedimientos operativos de rutina según normas definidas.
- d) Garantizar la implementación de un conjunto acordado de controles de seguridad.
- e) Confeccionar disposiciones relativas a la continuidad de las actividades del Organismo.
- f) Asegurar que la instalación del nuevo sistema no afectará negativamente los sistemas existentes, especialmente en los períodos pico de procesamiento.
- g) Considerar el efecto que tiene el nuevo sistema en la seguridad global del Organismo.

h) Disponer la realización de entrenamiento en la operación y/o uso de nuevos sistemas.

10.4 Categoría: Protección Contra Código Malicioso

Objetivo

Proteger la integridad del software y la integración. Se requiere tomar precauciones para evitar y detectar la introducción de códigos maliciosos y códigos móviles no-autorizados. El software y los medios de procesamiento de la información son vulnerables a la introducción de códigos maliciosos; como ser, entre otros, virus Troyanos, bombas lógicas, etc. Los usuarios deben estar al tanto de los peligros de los códigos maliciosos. Cuando sea apropiado, los gerentes deben introducir controles para evitar, detectar y eliminar los códigos maliciosos y controlar los códigos móviles.

10.4.1 Control: Código Malicioso

El Responsable de Seguridad de la Información definirá controles de detección y prevención para la protección contra software malicioso. El Responsable del Área Informática, o el personal designado por éste, implementarán dichos controles.

El Responsable de Seguridad de la Información desarrollará procedimientos adecuados de concientización de usuarios en materia de seguridad, controles de acceso al sistema y administración de cambios.

Estos controles deben considerar establecer políticas y procedimientos formales que contemplen las siguientes acciones:

a) Prohibir la instalación y uso de software no autorizado por el Organismo (Ver 0 Derecho de Propiedad Intelectual del Software).

b) Redactar procedimientos para evitar los riesgos relacionados con la obtención de archivos y software desde o a través de redes externas, o por cualquier otro medio (ej.: dispositivos portátiles), señalando las medidas de protección a tomar.

c) Instalar y actualizar periódicamente software de detección y reparación de virus, examinado computadoras y medios informáticos, como medida precautoria y rutinaria.

d) Mantener los sistemas al día con las últimas actualizaciones de seguridad disponibles (probar dichas actualizaciones en un entorno de prueba previamente si es que constituyen cambios críticos a los sistemas).

e) Revisar periódicamente el contenido de software y datos de los equipos de procesamiento que sustentan procesos críticos del Organismo, investigando formalmente la presencia de archivos no aprobados o modificaciones no autorizadas, en especial, realizar revisión y análisis de logs.

f) Verificar antes de su uso, la presencia de virus en archivos de medios electrónicos de origen incierto, o en archivos recibidos a través de redes no confiables.

g) Redactar procedimientos para verificar toda la información relativa a software malicioso, garantizando que los boletines de alerta sean exactos e informativos.

h) Concientizar al personal acerca del problema de los falsos antivirus (rogues) y las cadenas falsas (hoax) y de cómo proceder frente a los mismos.

i) Redactar normas de protección y habilitación de puertos de conexión de dispositivos móviles y sus derechos de acceso.

10.4.2 Control: Código Móvil

En caso que el código móvil sea autorizado, se debe garantizar que la configuración asegure que el código móvil autorizado opere de acuerdo a una configuración de seguridad claramente definida, previniendo que el código móvil no autorizado sea ejecutado.

Asimismo, se implementarán acciones para la protección contra acciones maliciosas resultantes de la ejecución no autorizada de código móvil, como ser:

- a) ejecución del código móvil en un ambiente lógicamente aislado;
- b) bloqueo del uso de código móvil;
- c) bloqueo de la recepción de código móvil;
- d) activación de medidas técnicas como sea disponible en un sistema específico para asegurar que el código móvil es gestionado;
- e) control de los recursos disponibles para el acceso del código móvil;
- f) implementación de controles criptográficos para autenticar de forma unívoca el código móvil.

10.5 Categoría: Respaldo o Back-up

Objetivo

Mantener la integridad y disponibilidad de la información y los medios de procesamiento de información.

Se deben establecer los procedimientos de rutina para implementar la política de respaldo acordada y la estrategia (ver también Capítulo 14.1 Gestión de Continuidad del Organismo) para tomar copias de respaldo de los datos y practicar su restauración oportuna.

10.5.1 Control: Resguardo de la Información

El Responsable del Área Informática y el de Seguridad de la Información junto al Responsable del Área Informática y los Propietarios de Información determinarán los requerimientos para resguardar cada software o dato en función de su criticidad. En base a ello, se definirá y documentará un esquema de resguardo de la información.

El Responsable del Área Informática dispondrá y controlará la realización de dichas copias, así como la prueba periódica de su restauración e integridad. Para esto se debe contar con instalaciones de resguardo que garanticen la disponibilidad de toda la información y del software crítico del Organismo. Los sistemas de resguardo deben probarse periódicamente, asegurándose que cumplen con los requerimientos de los planes de continuidad de las actividades del organismo, según el punto (ver también Capítulo 14.1 Gestión de Continuidad del Organismo).

Se definirán procedimientos para el resguardo de la información, que deben considerar los siguientes puntos:

a) Definir un esquema de rótulo de las copias de resguardo, que permita contar con toda la información necesaria para identificar cada una de ellas y administrarlas debidamente.

b) Establecer un esquema de remplazo de los medios de almacenamiento de las copias de resguardo, una vez concluida la posibilidad de ser reutilizados, de acuerdo a lo indicado por el proveedor, y asegurando la destrucción de los medios desechados.

c) Almacenar en una ubicación remota copias recientes de información de resguardo junto con registros exactos y completos de las mismas y los procedimientos documentados de restauración, a una distancia suficiente como para evitar daños provenientes de un desastre en el sitio principal. Se deben retener al menos tres generaciones o ciclos de información de resguardo para la información y el software esenciales para el Organismo. Para la definición de información mínima a ser resguardada en el sitio remoto, se debe tener en cuenta el nivel de clasificación otorgado a la misma, en términos de disponibilidad y requisitos legales a los que se encuentre sujeta.

d) Asignar a la información de resguardo un nivel de protección física y ambiental según las normas aplicadas en el sitio principal. Extender los mismos controles aplicados a los dispositivos en el sitio principal al sitio de resguardo.

e) Probar periódicamente los medios de resguardo.

f) Verificar y probar periódicamente los procedimientos de restauración garantizando su eficacia y cumplimiento dentro del tiempo asignado a la recuperación en los procedimientos operativos.

Los procedimientos de realización de copias de resguardo y su almacenamiento deben respetar las disposiciones capítulo 7 Gestión de Activos y 15.1.3 Control: Protección de los Registros del Organismo la presente Política.

10.5.2 Control: Registro de Actividades del Personal Operativo

El Responsable del Area Informática asegurará el registro de las actividades realizadas en los sistemas, incluyendo según corresponda:

a) Tiempos de inicio y cierre del sistema.

b) Errores del sistema y medidas correctivas tomadas.

c) Intentos de acceso a sistemas, recursos o información crítica o acciones restringidas

d) Ejecución de operaciones críticas

e) Cambios a información crítica

La Unidad de Auditoría Interna o en su defecto quien sea propuesto por el Comité de Seguridad de la Información contrastará los registros de actividades del personal operativo con relación a los procedimientos operativos.

10.5.3 Control: Registro de Fallas

El Responsable del Area Informática desarrollará y verificará el cumplimiento de procedimientos para comunicar las fallas en el procesamiento de la información o los sistemas de comunicaciones, que permita tomar medidas correctivas.

Se registrarán las fallas comunicadas, debiendo existir reglas claras para el manejo de las mismas, con inclusión de:

a) Revisión de registros de fallas para garantizar que las mismas fueron resueltas satisfactoriamente.

b) Revisión de medidas correctivas para garantizar que los controles no fueron comprometidos, y que las medidas tomadas fueron autorizadas.

c) Documentación de la falla con el objeto de prevenir su repetición o facilitar su resolución en caso de reincidencia.

d) Integrar la comunicación y gestión de la falla acorde a lo definido en el Capítulo 13 – Gestión de Incidentes.

10.6 Categoría: Gestión de la Red

Objetivo

Asegurar la protección de la información en redes y la protección de la infraestructura de soporte.

La gestión segura de las redes, la cual puede abarcar los límites organizacionales, requiere de la cuidadosa consideración del flujo de datos, implicancias legales, monitoreo y protección.

También se pueden requerir controles adicionales para proteger la información confidencial que pasa a través de redes públicas.

10.6.1 Control: Redes

El Responsable de Seguridad de la Información definirá controles para garantizar la seguridad de los datos y los servicios conectados en las redes del Organismo, contra el acceso no autorizado, considerando la ejecución de las siguientes acciones:

a) Establecer los procedimientos para la administración del equipamiento remoto, incluyendo los equipos en las áreas usuarias, la que será llevada a cabo por el responsable establecido en el punto "6-1-3 control: Asignación de responsabilidad de la seguridad de la información".

b) Establecer controles especiales para salvaguardar la confidencialidad e integridad del procesamiento de los datos que pasan a través de redes públicas, y para proteger los sistemas conectados. Implementar controles especiales para mantener la disponibilidad de los servicios de red y computadoras conectadas.

c) Garantizar mediante actividades de supervisión, que los controles se aplican uniformemente en toda la infraestructura de procesamiento de información.

El Responsable del Area Informática implementará dichos controles.

10.7 Categoría: Administración y Seguridad de los medios de almacenamiento

Objetivo

Evitar la divulgación no-autorizada; modificación, eliminación o destrucción de activos; y la interrupción de las actividades comerciales. Los medios se debieran controlar y proteger físicamente.

Se deben establecer los procedimientos de operación apropiados para proteger los documentos, medios de cómputo (por ejemplo, cintas y discos), entrada/salida de datos (input/output) y documentación del sistema de una divulgación no-autorizada, modificación, eliminación y destrucción.

10.7.1 Control: Administración de Medios Informáticos Removibles

El Responsable del Area Informática, con la asistencia del Responsable de Seguridad de la Información, implementará procedimientos para la administración de medios informáticos removibles, como cintas, discos, pendrives e informes impresos. El cumplimiento de los procedimientos se hará de acuerdo al capítulo "11.1 Categoría: Requerimientos para el Control de Acceso".

Se deben considerar las siguientes acciones para la implementación de los procedimientos:

a) Eliminar de forma segura los contenidos, si ya no son requeridos, de cualquier medio reutilizable que ha de ser retirado o reutilizado por el Organismo.

b) Requerir autorización para retirar cualquier medio del Organismo y realizar un control de todos los retiros a fin de mantener un registro de auditoría.

c) Almacenar todos los medios en un ambiente seguro y protegido, de acuerdo con las especificaciones de los fabricantes o proveedores y la criticidad de la información almacenada.

Se documentarán todos los procedimientos y niveles de autorización, en concordancia con el capítulo 7.1.1 Control: Inventario de activos.

10.7.2 Control: Eliminación de Medios de Información

El Responsable del Area Informática, junto con el Responsable de Seguridad de la Información, definirá procedimientos para la eliminación segura de los medios de soporte de información respetando la normativa vigente.

Los procedimientos deben considerar que los siguientes elementos requerirán almacenamiento y eliminación segura:

a) Documentos en papel.

b) Voces u otras grabaciones.

c) Papel carbónico.

d) Informes de salida.

e) Cintas de impresora de un solo uso.

f) Cintas magnéticas.

g) Discos u otros dispositivos removibles.

h) Medios de almacenamiento óptico (todos los formatos incluyendo todos los medios de distribución de software del fabricante o proveedor).

i) Listados de programas.

j) Datos de prueba.

k) Documentación del sistema.

La evaluación del mecanismo de eliminación debe contemplar el tipo de dispositivo y la criticidad de la información contenida.

10.7.3 Control: Procedimientos de Manejo de la Información

Se definirán procedimientos para el manejo y almacenamiento de la información de acuerdo a la clasificación establecida en el capítulo 7.1.1 Control: Inventario de activos.

En los procedimientos se contemplarán las siguientes acciones:

a) Incluir en la protección a documentos, sistemas informáticos, redes, computación móvil, comunicaciones móviles, correo, correo de voz, comunicaciones de voz en general, multimedia, servicios e instalaciones postales, uso de máquinas de fax y cualquier otro ítem potencialmente sensible.

b) Restringir el acceso sólo al personal debidamente autorizado.

c) Mantener un registro formal de los receptores autorizados de datos.

d) Garantizar que los datos de entrada son completos, que el procesamiento se lleva a cabo correctamente y que se valida las salidas.

e) Proteger los datos en espera ("colas") y memorias temporales (ej.: cache).

f) Conservar los medios de almacenamiento en un ambiente que concuerde con las especificaciones de los fabricantes o proveedores.

10.7.4 Control: Seguridad de la Documentación del Sistema

La documentación del sistema puede contener información sensible o confidencial, por lo que se considerarán los siguientes recaudos para su protección:

a) Almacenar la documentación del sistema en forma segura.

b) Restringir el acceso a la documentación del sistema al personal estrictamente necesario. Dicho acceso será autorizado por el Propietario de la Información relativa al sistema.

10.8 Categoría: Intercambios de Información y Software

Objetivo

Mantener la seguridad en el intercambio de información y software dentro del Organismo y con cualquier otra entidad externa.

Los intercambios de información y software dentro de las organizaciones se deben basar en una política formal de intercambio, seguida en línea con los acuerdos de intercambio, y debiera cumplir con cualquier legislación relevante (ver capítulo 15 Cumplimiento).

Se deben establecer los procedimientos y estándares para proteger la información y los medios físicos que contiene la información en-tránsito.

10.8.1 Control: Procedimientos y controles de intercambio de la información

Se establecerán procedimientos y controles formales para proteger el intercambio de información a través del uso de todos los tipos de instalaciones de comunicación, considerando lo siguiente:

- a) Protección de la información intercambiada de la interceptación, copiado, modificación, de que sea mal dirigida, y de su destrucción
- b) detección de y la protección contra el código malicioso que puede ser transmitido a través del uso de comunicaciones electrónicas
- c) definición del uso aceptable de las instalaciones de comunicación electrónicas
- d) uso seguro de comunicaciones inalámbricas
- e) responsabilidades del empleado, contratista y cualquier otro usuario de no comprometer a la organización, por ejemplo, a través de la difamación, hostigamiento, personificación, reenvío de cadenas de comunicación epistolar, compras no autorizadas y cualquier otro medio (ej.: redes sociales)
- f) uso de técnicas criptográficas para proteger la confidencialidad, integridad y la autenticidad de la información
- g) directrices de retención y eliminación para toda la correspondencia en concordancia con las leyes y regulaciones relevantes, locales y nacionales
- h) instrucción del personal sobre las precauciones que deben tomar a la hora de transmitir información del Organismo.

10.8.2 Control: Acuerdos de Intercambio de Información y Software

Cuando se realicen acuerdos entre organizaciones para el intercambio de información y software, se especificarán el grado de sensibilidad de la información del Organismo involucrada y las consideraciones de seguridad sobre la misma. Se tendrán en cuenta los siguientes aspectos:

- a) Responsabilidades gerenciales por el control y la notificación de transmisiones, envíos y recepciones.
- b) Procedimientos de notificación de emisión, transmisión, envío y recepción.
- c) Normas técnicas para el empaquetado y la transmisión.
- d) Pautas para la identificación del prestador del servicio de correo.
- e) Responsabilidades y obligaciones en caso de pérdida, exposición o divulgación no autorizada de datos.
- f) Uso de un sistema convenido para el rotulado de información clasificada, garantizando que el significado de los rótulos sea inmediatamente comprendido y que la información sea adecuadamente protegida.
- g) Términos y condiciones de la licencia bajo la cual se suministra el software.
- h) Información sobre la propiedad de la información suministrada y las condiciones de su uso.
- i) Normas técnicas para la grabación y lectura de la información y del software.
- j) Controles especiales que puedan requerirse para proteger ítems sensibles, (claves criptográficas, etc.).

10.8.3 Control: Seguridad de los Medios en Tránsito

Los procedimientos de transporte de medios informáticos entre diferentes puntos (envíos postales y mensajería) deben contemplar:

- a) La utilización de medios de transporte o servicios de mensajería confiables. El Propietario de la Información a transportar determinará qué servicio de mensajería se utilizará conforme la criticidad de la información a transmitir.
- b) Suficiente embalaje para envío de medios a través de servicios postales o de mensajería, siguiendo las especificaciones de los fabricantes o proveedores.
- c) La adopción de controles especiales, cuando resulte necesario, a fin de proteger la información sensible contra divulgación o modificación no autorizadas. Entre los ejemplos se incluyen:
 1. Uso de recipientes cerrados.
 2. Entrega en mano.
 3. Embalaje a prueba de apertura no autorizada (que revele cualquier intento de acceso).
 4. En casos excepcionales, división de la mercadería a enviar en más de una entrega y envío por diferentes rutas.

10.8.4 Control: Seguridad de los la Mensajería

La mensajería electrónica como el correo electrónico, el intercambio de datos electrónicos (EDI por sus siglas en inglés), la mensajería instantánea y las redes sociales juegan un muy impor-

tante en las comunicaciones organizacionales. La mensajería electrónica tiene diferentes riesgos que las comunicaciones basadas en papel.

Se considerarán las siguientes medidas de seguridad en los mensajes electrónicos:

- protección de mensajes por el acceso no autorizado, modificaciones o denegación de servicio;
- correcta asignación de la dirección y el transporte del mensaje;
- confiabilidad y disponibilidad general del servicio;
- consideraciones legales, por ejemplo, requerimientos para firmas electrónicas;
- obtención de aprobación previa al uso de los servicios públicos externos tales como mensajería instantánea o el compartir archivos;
- niveles altos de controles de autenticación para los accesos desde las redes públicamente accesibles.

10.8.5 Control: Seguridad del Gobierno Electrónico

El Responsable de Seguridad de la Información verificará que los procedimientos de aprobación de Software del punto "10.3.2 Control: Aprobación del Sistema" incluyan los siguientes aspectos para las aplicaciones de Gobierno Electrónico:

- a) **Autenticación:** Nivel de confianza recíproca suficiente sobre la identidad del usuario y el Organismo.
- b) **Autorización:** Niveles de Autorización adecuados para establecer disposiciones, emitir o firmar documentos clave, etc. Forma de comunicarlo al otro participante de la transacción electrónica.
- c) **Procesos de oferta y contratación pública:** Requerimientos de confidencialidad, integridad y prueba de envío y recepción de documentos clave y de no repudio de contratos.
- d) **Trámites en línea:** Confidencialidad, integridad y no repudio de los datos suministrados con respecto a trámites y presentaciones ante el Estado y confirmación de recepción.
- e) **Verificación:** Grado de verificación apropiado para constatar la información suministrada por los usuarios.
- f) **Cierre de la transacción:** Forma de interacción más adecuada para evitar fraudes.
- g) **Protección a la duplicación:** Asegurar que una transacción sólo se realiza una vez, a menos que se especifique lo contrario.
- h) **No repudio:** Manera de evitar que una entidad que haya enviado o recibido información alegue que no la envió o recibió.
- i) **Responsabilidad:** Asignación de responsabilidades ante el riesgo de eventuales presentaciones, tramitaciones o transacciones fraudulentas.
- j) **Seguridad:** contemplas los requisitos de Integridad, Confidencialidad y Disponibilidad de las Aplicaciones, por ejemplo asegurando que las aplicaciones disponibles a través de redes de acceso público (ej.: Internet) no puedan ser alteradas en su contenido, infectadas con código ni susceptibles a vulnerabilidades derivadas de malas prácticas de desarrollo.

Las consideraciones mencionadas se implementarán mediante la aplicación de las técnicas criptográficas enumeradas en el punto "12.3.1 Control: Política de Utilización de Controles Criptográficos" y tomando en cuenta el cumplimiento de los requisitos legales emanados de toda la normativa vigente.

Se darán a conocer a los usuarios, los términos y condiciones aplicables, asegurándose que los mismos fueron leídos y comprendidos por los mismos.

Todas las medidas vinculadas al plan de gobierno electrónico del organismo deben dictarse conforme lo dispuesto por el Decreto N° 378/2005.

10.9 Categoría: Seguridad del Correo Electrónico

Objetivo

Garantizar la seguridad de los servicios de correo electrónico y su uso seguro.

Se debieran considerar las implicancias de seguridad asociadas con el uso de servicios de correo electrónico.

10.9.1 Control: Riesgos de Seguridad

Se implementarán controles para reducir los riesgos de incidentes de seguridad en el correo electrónico, contemplando:

- a) La vulnerabilidad de los mensajes al acceso o modificación no autorizados o a la denegación de servicio.
- b) La posible interceptación y el consecuente acceso a los mensajes en los medios de transferencia que intervienen en la distribución de los mismos.
- c) Las posibles vulnerabilidades a errores, por ejemplo, consignación incorrecta de la dirección o dirección errónea, y la confiabilidad y disponibilidad general del servicio.
- d) La posible recepción de código malicioso en un mensaje de correo, el cual afecte la seguridad de la terminal receptora o de la red a la que se encuentra conectada.
- e) El impacto de un cambio en el medio de comunicación en los procesos del Organismo.
- f) Las consideraciones legales, como la necesidad potencial de contar con prueba de origen, envío, entrega y aceptación.
- g) Las implicancias de la publicación externa de información sensible o confidencial, accesibles al público.
- h) El acceso de usuarios remotos a las cuentas de correo electrónico.

i) El uso inadecuado por parte del personal.

10.9.2 Control: Política de Correo Electrónico

El Responsable de Seguridad de la Información junto con el Responsable del Área Informática definirán y documentarán normas y procedimientos claros con respecto al uso del correo electrónico, que incluya al menos los siguientes aspectos:

a) Protección contra ataques al correo electrónico, por ejemplo virus, interceptación, etc.

b) Protección de archivos adjuntos de correo electrónico.

c) Uso de técnicas criptográficas para proteger la confidencialidad e integridad de los mensajes electrónicos (Ver 12.3 Categoría: Controles Criptográficos).

d) Retención de mensajes que, si se almacenaran, pudieran ser usados en **caso de litigio**.

e) Controles adicionales para examinar mensajes electrónicos que no pueden ser autenticados.

f) Aspectos operativos para garantizar el correcto funcionamiento del servicio (ej.: tamaño máximo de información transmitida y recibida, cantidad de destinatarios, tamaño máximo del buzón del usuario, etc.).

g) Definición de los alcances del uso del correo electrónico por parte del personal del Organismo.

h) Potestad del Organismo para auditar los mensajes recibidos o emitidos por los servidores del Organismo, lo cual se incluirá en el "Compromiso de Confidencialidad".

Estos dos últimos puntos deben ser leídos a la luz de las normas vigentes que no sólo prohíben a los empleados a hacer uso indebido o con fines particulares del patrimonio estatal sino que también imponen la obligación de usar los bienes y recursos del Estado con los fines autorizados y de manera racional, evitando su abuso, derroche o desaprovechamiento.

Entender al correo electrónico como una herramienta más de trabajo provista al empleado a fin de ser utilizada conforme el uso al cual está destinada, faculta al empleador a implementar sistemas de controles destinados a velar por la protección y el buen uso de sus recursos.

Esta facultad, sin embargo, debe ejercerse salvaguardando la dignidad del trabajador y su derecho a la intimidad. Por tal motivo, el Organismo debe informar claramente a sus empleados:

a) cuál es el uso que el organismo espera que los empleados hagan del correo electrónico provisto por el organismo; y

b) bajo qué condiciones los mensajes pueden ser objeto de control y monitoreo.

10.9.3 Control: Seguridad de los Sistemas Electrónicos de Oficina

Se controlarán los mecanismos de distribución y difusión tales como documentos, computadoras, dispositivos de computación móvil, comunicaciones móviles, correo, correo de voz, comunicaciones de voz en general (analógica o digital), multimedia, servicios o instalaciones postales, equipos de fax, etc.

Al interconectar dichos medios, se considerarán las implicancias en lo que respecta a la seguridad y a las actividades propias del Organismo, incluyendo:

a) Vulnerabilidades de la información en los sistemas de oficina, por ejemplo la grabación de llamadas telefónicas o teleconferencias, la confidencialidad de las llamadas, el almacenamiento de faxes, la apertura o distribución del correo.

b) Procedimientos y controles apropiados para administrar la distribución de información, por ejemplo el uso de boletines electrónicos institucionales.

c) Exclusión de categorías de información sensible del Organismo, si el sistema no brinda un adecuado nivel de protección.

d) Limitación del acceso a la información de las actividades que desarrollan determinadas personas, por ejemplo aquellas que trabaja en proyectos sensibles.

e) La aptitud del sistema para dar soporte a las aplicaciones del Organismo, como la comunicación de órdenes o autorizaciones.

f) Categorías de personal y contratistas o terceros a los que se permite el uso del sistema y las ubicaciones desde las cuales se puede acceder al mismo.

g) Restricción de acceso a determinadas instalaciones a específicas categorías de usuarios.

h) Identificación de la posición o categoría de los usuarios, por ejemplo empleados del Organismo o contratistas, en directorios accesibles por otros usuarios.

i) Retención y resguardo de la información almacenada en el sistema.

j) Requerimientos y disposiciones relativos a sistemas de soporte de reposición de información previa.

10.9.4 Control: Sistemas de Acceso Público

Se tomarán recaudos para la protección de la integridad de la información publicada electrónicamente, a fin de prevenir la modificación no autorizada que podría dañar la reputación del Organismo que emite la publicación. Es posible que la información de un sistema de acceso público, por ejemplo la información en un servidor Web accesible por Internet, deba cumplir con ciertas normas de la jurisdicción en la cual se localiza el sistema o en la cual tiene lugar la transacción electrónica.

Se implementará un proceso de autorización formal antes de que la información se ponga a disposición del público, estableciéndose en todos los casos los encargados de dicha aprobación.

Todos los sistemas de acceso público deben prever que:

a) La información se obtenga, procese y proporcione de acuerdo a la normativa vigente, en especial la Ley de Protección de Datos Personales.

b) La información que se ingresa al sistema de publicación, o aquella que procesa el mismo, sea procesada en forma completa, exacta y oportuna.

c) La información sensible o confidencial sea protegida durante el proceso de recolección y su almacenamiento.

d) El acceso al sistema de publicación no permita el acceso accidental a las redes a las cuales se conecta el mismo.

e) El responsable de la publicación de información en sistemas de acceso público sea claramente identificado.

f) La información se publique teniendo en cuenta las normas establecidas al respecto.

g) Se garantice la validez y vigencia de la información publicada.

10.9.5 Control: Otras Formas de Intercambio de Información

Se implementarán normas, procedimientos y controles para proteger el intercambio de información a través de medios de comunicaciones de voz, fax y vídeo, contemplando las siguientes acciones:

a) Concientizar al personal sobre la toma de debidas precauciones, por ejemplo no revelar información sensible como para evitar ser escuchado o interceptado, al hacer una llamada telefónica, por:

1. Personas cercanas, en especial al utilizar teléfonos móviles o smartphones.

2. Terceros que tengan acceso a la comunicación mediante la Intervención de la línea telefónica, y otras formas de escucha subrepticias, a través del acceso físico al aparato o a la línea telefónica, o mediante equipos de barrido de frecuencias al utilizar teléfonos móviles análogos.

3. Terceros en el lado receptor.

b) Recordar al personal que no sostengan conversaciones confidenciales en lugares públicos u oficinas abiertas y lugares de reunión con paredes delgadas.

c) No dejar mensajes en contestadores automáticos puesto que éstos pueden ser escuchados por personas no autorizadas, almacenados en sistemas públicos o almacenados incorrectamente como resultado de un error de discado.

d) Recordar al personal los problemas ocasionados por el uso de máquinas de fax, en particular:

1. El acceso no autorizado a sistemas incorporados de almacenamiento de mensajes con el objeto de recuperarlos.

2. La programación deliberada o accidental de equipos para enviar mensajes a determinados números.

El envío de documentos y mensajes a un número equivocado por errores de discado o por utilizar el número almacenado equivocado.

10.10 Categoría: Seguimiento y control

Objetivo

Detectar las actividades de procesamiento de información no autorizadas.

Se deben monitorear los sistemas y se deben reportar los eventos de seguridad de la información. Se deben utilizar bitácoras de operador y se deben registrar las fallas para asegurar que se identifiquen los problemas en los sistemas de información. Una organización debe cumplir con todos los requerimientos legales relevantes aplicables a sus actividades de monitoreo y registro.

Se debe utilizar el monitoreo del sistema para chequear la efectividad de los controles adoptados y para verificar la conformidad con un modelo de política de acceso.

10.10.1 Control: Registro de auditoría

Se producirán y mantendrán registros de auditoría en los cuales se registren las actividades, excepciones, y eventos de seguridad de la información de los usuarios, por un período acordado para permitir la detección e investigación de incidentes.

Se debe evaluar la registración en los mencionados registros de la siguiente información:

a) identificación de los usuarios;

b) fechas, tiempos, y detalles de los eventos principales, por ejemplo, inicio y cierre de sesión;

c) identidad del equipo o la ubicación si es posible;

d) registros de intentos de acceso al sistema exitosos y fallidos;

e) registros de intentos de acceso a los datos u otro recurso, exitosos y rechazados;

f) cambios a la configuración del sistema;

g) uso de privilegios;

h) uso de utilitarios y aplicaciones de sistemas;

i) archivos accedidos y el tipo de acceso;

j) direcciones de redes y protocolos;

k) alarmas que son ejecutadas por el sistema de control de accesos;

l) activación y desactivación de los sistemas de protección, tales como sistemas antivirus y sistemas de detección de intrusos.

10.10.2 Control: Protección de los registros

Se implementarán controles para la protección de los registros de auditoría contra cambios no autorizados y problemas operacionales, incluyendo:

- a) alteraciones de los tipos de mensajes que son grabados;
- b) edición o eliminación de archivos de registro;

Exceso de la capacidad de almacenamiento de los archivos de registro, resultando en la falla para registrar los eventos o sobrescribiendo eventos registrados en el pasado.

10.10.3 Control: Registro de actividad de administrador y operador

Se registrarán y revisarán periódicamente en particular las actividades de los administradores y operadores de sistema incluyendo:

- a) cuenta de administración u operación involucrada;
- b) momento en el cual ocurre un evento (éxito o falla);
- c) información acerca del evento (por ejemplo, los archivos manipulados) o las fallas (por ejemplo, los errores ocurridos y las acciones correctivas tomadas);
- d) procesos involucrados.

10.10.4 Control: Sincronización de Relojes

A fin de garantizar la exactitud de los registros de auditoría, al menos los equipos que realicen estos registros, deben tener una correcta configuración de sus relojes.

Para ello, se dispondrá de un procedimiento de ajuste de relojes, el cual indicará también la verificación de los relojes contra una fuente externa del dato y la modalidad de corrección ante cualquier variación significativa.

11. Cláusula: Gestión de Accesos



Generalidades

El acceso por medio de un sistema de restricciones y excepciones a la información es la base de todo sistema de seguridad informática. Para impedir el acceso no autorizado a los sistemas de información se deben implementar procedimientos formales para controlar la asignación de derechos de acceso a los sistemas de información, bases de datos y servicios de información, y éstos deben estar claramente documentados, comunicados y controlados en cuanto a su cumplimiento.

Los procedimientos comprenden todas las etapas del ciclo de vida de los accesos de los usuarios de todos los niveles, desde el registro inicial de nuevos usuarios hasta la privación final de derechos de los usuarios que ya no requieren el acceso.

La cooperación de los usuarios es esencial para la eficacia de la seguridad, por lo tanto es necesario concientizar a los mismos acerca de sus responsabilidades por el mantenimiento de controles de acceso eficaces, en particular aquellos relacionados con el uso de contraseñas y la seguridad del equipamiento.

Objetivo

Impedir el acceso no autorizado a los sistemas de información, bases de datos y servicios de información. Implementar seguridad en los accesos de usuarios por medio de técnicas de autenticación y autorización.

Controlar la seguridad en la conexión entre la red del Organismo y otras redes públicas o privadas. Registrar y revisar eventos y actividades críticas llevadas a cabo por los usuarios en los sistemas.

Concientizar a los usuarios respecto de su responsabilidad frente a la utilización de contraseñas y equipos.

Garantizar la seguridad de la información cuando se utiliza computación móvil e instalaciones de trabajo remoto.

Alcance

La Política definida en este documento se aplica a todas las formas de acceso de aquellos a quienes se les haya otorgado permisos sobre los sistemas de información, bases de datos o servicios de información del Organismo, cualquiera sea la función que desempeñe.

Asimismo se aplica al personal técnico que define, instala, administra y mantiene los permisos de acceso y las conexiones de red, y a los que administran su seguridad.

Responsabilidad

El Responsable de Seguridad de la Información estará a cargo de:

Definir normas y procedimientos para: la gestión de accesos a todos los sistemas, bases de datos y servicios de información multiusuario; el monitoreo del uso de las instalaciones de procesamiento de la información; la solicitud y aprobación de accesos a Internet; el uso de computación móvil, trabajo remoto y reportes de incidentes relacionados; la respuesta a la activación de alarmas silenciosas; la revisión de registros de actividades (logs); y el ajuste de relojes de acuerdo a un estándar preestablecido.

- Definir pautas de utilización de Internet para todos los usuarios.

- Participar en la definición de normas y procedimientos de seguridad a implementar en el ambiente informático (ej.: sistemas operativos, servicios de red, enrutadores o gateways, etc.) y validarlos periódicamente.

- Controlar periódicamente la asignación de privilegios a usuarios.

- Analizar y sugerir medidas a ser implementadas para efectivizar el control de acceso a Internet de los usuarios.

- Verificar el cumplimiento de las pautas establecidas, relacionadas con control de accesos, registración de usuarios, administración de privilegios, administración de contraseñas, utilización de servicios de red, autenticación de usuarios y nodos, uso controlado de utilitarios del sistema, alarmas silenciosas, desconexión de terminales por tiempo muerto, limitación del horario de conexión, registro de eventos, protección de puertos (físicos y lógicos), subdivisión de redes, control de conexiones a la red, control de ruteo de red, etc.

- Concientizar a los usuarios sobre el uso apropiado de contraseñas y de equipos de trabajo.

- Verificar periódicamente el cumplimiento de los procedimientos de revisión de registros de auditoría.

- Asistir a los usuarios que corresponda en el análisis de riesgos a los que se expone la información y los componentes del ambiente informático que sirven de soporte a la misma.

Los Propietarios de la Información estarán encargados de:

- Evaluar los riesgos a los cuales se expone la información con el objeto de:

• determinar los controles de accesos, autenticación y utilización a ser implementados en cada caso.

• definir los eventos y actividades de usuarios a ser registrados en los sistemas de procesamiento de su incumbencia y la periodicidad de revisión de los mismos.

- Aprobar y solicitar la asignación de privilegios a usuarios.

- Llevar a cabo un proceso formal y periódico de revisión de los derechos de acceso a la información.

- Definir un cronograma de depuración de registros de auditoría en línea.

Los Propietarios de la Información junto con la Unidad de Auditoría Interna o en su defecto quien sea propuesto por el Comité de Seguridad de la Información, definirán un cronograma de depuración de logs y registros de auditoría en línea en función a normas vigentes y a sus propias necesidades.

Los Responsable de las Unidades Organizativas, junto con el Responsable de Seguridad de la Información, autorizarán el trabajo remoto del personal a su cargo, en los casos en que se verifique que son adoptadas todas las medidas que correspondan en materia de seguridad de la información, de modo de cumplir con las normas vigentes. Asimismo autorizarán el acceso de los usuarios a su cargo a los servicios y recursos de red y a Internet.

El Responsable del Area Informática cumplirá las siguientes funciones:

- Implementar procedimientos para la activación y desactivación de derechos de acceso a las redes.

- Analizar e implementar los métodos de autenticación y control de acceso definidos en los sistemas, bases de datos y servicios.

- Evaluar el costo y el impacto de la implementación de "enrutadores", "gateways" y/o firewalls adecuados para subdividir la red y recomendar el esquema apropiado.

- Implementar el control de puertos, de conexión a la red y de ruteo de red.

- Implementar el registro de eventos o actividades (logs) de usuarios de acuerdo a lo definido por los propietarios de la información, así como la depuración de los mismos.

- Definir e implementar los registros de eventos y actividades correspondientes a sistemas operativos y otras plataformas de procesamiento.

- Evaluar los riesgos sobre la utilización de las instalaciones de procesamiento de información, con el objeto de definir medios de monitoreo y tecnologías de identificación y autenticación de usuarios (Ej.: biometría, verificación de firma, uso de autenticadores de hardware).

- Definir e implementar la configuración que debe efectuarse para cada servicio de red, de manera de garantizar la seguridad en su operatoria.

- Analizar las medidas a ser implementadas para efectivizar el control de acceso a Internet de los usuarios.

- Otorgar acceso a los servicios y recursos de red, únicamente de acuerdo al pedido formal correspondiente.

- Efectuar un control de los registros de auditoría generados por los sistemas operativos y de comunicaciones.

La Unidad de Auditoría Interna o en su defecto quien sea propuesto por el Comité de Seguridad de la Información, tendrá acceso a los registros de eventos a fin de colaborar en el control y efectuar recomendaciones sobre modificaciones a los aspectos de seguridad.

El Comité de Seguridad de la Información aprobará el análisis de riesgos de la información efectuado. Asimismo, aprobará el período definido para el mantenimiento de los registros de auditoría generados.

Política

11.1 Categoría: Requerimientos para el Control de Acceso

Objetivo

Controlar el acceso a la información. Se debe controlar el acceso a la información, medios de procesamiento de la información y procesos de negocio sobre la base de los requerimientos de negocio y de seguridad.

Las reglas de control del acceso deben tomar en cuenta las políticas para la divulgación y autorización de la información.

11.1.1 Control: Política de Control de Accesos

En la aplicación de controles de acceso, se contemplarán los siguientes aspectos:

- a) Identificar los requerimientos de seguridad de cada una de las aplicaciones.
- b) Identificar toda la información relacionada con las aplicaciones.
- c) Establecer criterios coherentes entre esta Política de Control de Acceso y la Política de Clasificación de Información de los diferentes sistemas y redes (Ver capítulo 7 Gestión de Activos).
- d) Identificar la legislación aplicable y las obligaciones contractuales con respecto a la protección del acceso a datos y servicios.
- e) Definir los perfiles de acceso de usuarios estándar, comunes a cada categoría de puestos de trabajo.
- f) Administrar los derechos de acceso en un ambiente distribuido y de red, que reconozcan todos los tipos de conexiones y dispositivos disponibles.

11.1.2 Control: Reglas de Control de Acceso

Las reglas de control de acceso especificadas, deben:

- a) Indicar expresamente si las reglas son obligatorias u optativas.
- b) Establecer reglas sobre la premisa "Todo debe estar prohibido a menos que se permita expresamente" y no sobre la premisa inversa de "Todo está permitido a menos que se prohíba expresamente".
- c) Controlar los cambios en los rótulos de información que son iniciados automáticamente por herramientas de procesamiento de información, de aquellos que son iniciados a discreción del usuario (Ver capítulo 7 Gestión de Activos).
- d) Controlar los cambios en los permisos de usuario que son iniciados automáticamente por el sistema de información y aquellos que son iniciados por el administrador.

e) Controlar las reglas que requieren la aprobación del administrador o del Propietario de la Información de que se trate, antes de entrar en vigencia, y aquellas que no requieren aprobación.

11.2 Categoría: Administración de Accesos de Usuarios

Objetivo

Con el objetivo de impedir el acceso no autorizado a la información se implementarán procedimientos formales para controlar la asignación de derechos de acceso a los sistemas, datos y servicios de información.

Los procedimientos debieran abarcar todas las etapas en el ciclo de vida del acceso del usuario, desde el registro inicial de usuarios nuevos hasta la baja final de los usuarios que ya no requieren acceso a los sistemas y servicios de información.

11.2.1 Control: Registración de Usuarios

El Responsable de Seguridad de la Información definirá un procedimiento formal de registro de usuarios para otorgar y revocar el acceso a todos los sistemas, bases de datos y servicios de información multiusuario, el cual debe comprender:

- a) Utilizar identificadores de usuario únicos, de manera que se pueda identificar a los usuarios por sus acciones evitando la existencia de múltiples perfiles de acceso para un mismo empleado. El uso de identificadores grupales sólo debe ser permitido cuando sean convenientes para el trabajo a desarrollar debido a razones operativas.
- b) Verificar que el usuario tiene autorización del Propietario de la Información para el uso del sistema, base de datos o servicio de información.
- c) Verificar que el nivel de acceso otorgado es adecuado para el propósito de la función del usuario y es coherente con la Política de Seguridad del Organismo, por ejemplo que no compromete la segregación de funciones.
- d) Entregar a los usuarios un detalle escrito de sus derechos de acceso.
- e) Requerir que los usuarios firmen declaraciones señalando que comprenden y aceptan las condiciones para el acceso.
- f) Garantizar que los proveedores de servicios no otorguen acceso hasta que se hayan completado los procedimientos de autorización.
- g) Mantener un registro formal de todas las personas registradas para utilizar el servicio.
- h) Cancelar inmediatamente los derechos de acceso de los usuarios que cambiaron sus tareas, o de aquellos a los que se les revocó la autorización, se desvincularon del Organismo o sufrieron la pérdida/robo de sus credenciales de acceso.

i) Efectuar revisiones periódicas con el objeto de:

- cancelar identificadores y cuentas de usuario redundantes
- inhabilitar cuentas inactivas por más de (indicar período no mayor a 60 días)
- eliminar cuentas inactivas por más de..... (indicar período no mayor a 120 días)

En el caso de existir excepciones, deben ser debidamente justificadas y aprobadas.

j) Garantizar que los identificadores de usuario redundantes no se asignen a otros usuarios.

k) Incluir cláusulas en los contratos de personal y de servicios que especifiquen sanciones si el personal o los agentes que prestan un servicio intentan accesos no autorizados.

11.2.2 Control: Gestión de Privilegios

Se limitará y controlará la asignación y uso de privilegios, debido a que el uso inadecuado de los privilegios del sistema resulta frecuentemente en el factor más importante que contribuye a la falla de los sistemas a los que se ha accedido ilegalmente.

Los sistemas multiusuario que requieren protección contra accesos no autorizados, deben prever una asignación de privilegios controlada mediante un proceso de autorización formal. Se deben tener en cuenta los siguientes pasos:

- a) Identificar los privilegios asociados a cada producto del sistema, por ejemplo sistema operativo, sistema de administración de bases de datos y aplicaciones, y las categorías de personal a las cuales deben asignarse los productos.
- b) Asignar los privilegios a individuos sobre la base de la necesidad de uso y evento por evento, por ejemplo el requerimiento mínimo para su rol funcional.
- c) Mantener un proceso de autorización y un registro de todos los privilegios asignados. Los privilegios no deben ser otorgados hasta que se haya completado el proceso formal de autorización.
- d) Establecer un período de vigencia para el mantenimiento de los privilegios (en base a la utilización que se le dará a los mismos) luego del cual los mismos serán revocados.
- e) Promover el desarrollo y uso de rutinas del sistema para evitar la necesidad de otorgar privilegios a los usuarios.

Los Propietarios de Información serán los encargados de aprobar la asignación de privilegios a usuarios y solicitar su implementación, lo cual será supervisado por el Responsable de Seguridad de la Información.

11.2.3 Control: Gestión de Contraseñas de Usuario

La asignación de contraseñas se controlará a través de un proceso de administración formal, mediante el cual deben respetarse los siguientes pasos:

- a) Requerir que los usuarios firmen una declaración por la cual se comprometen a mantener sus contraseñas personales en secreto y las contraseñas de los grupos de trabajo exclusivamente entre los miembros del grupo. Esta declaración bien puede estar incluida en el Compromiso de Confidencialidad.
- b) Garantizar que los usuarios cambien las contraseñas iniciales que les han sido asignadas la primera vez que ingresan al sistema. Las contraseñas provisionales, que se asignan cuando los usuarios olvidan su contraseña, sólo debe suministrarse una vez acreditada la identidad del usuario.
- c) Generar contraseñas provisionales seguras para otorgar a los usuarios. Se debe evitar la participación de terceros o el uso de mensajes de correo electrónico sin protección (texto claro) en el mecanismo de entrega de la contraseña y los usuarios deben dar acuse de recibo formal cuando la reciban.
- d) Almacenar las contraseñas sólo en sistemas informáticos protegidos.
- e) Utilizar otras tecnologías de autenticación y autorización de usuarios, como ser la biométrica (por ejemplo verificación de huellas dactilares), verificación de firma, uso de autenticadores de hardware (como las tarjetas de circuito integrado), etc. El uso de esas herramientas se dispondrá cuando la evaluación de riesgos realizada por el Responsable de Seguridad de la Información conjuntamente con el Responsable del Área de Informática y el Propietario de la Información lo determine necesario (o lo justifique).
- f) Configurar los sistemas de tal manera que:
 - las contraseñas sean del tipo "password fuerte" y tengan ... (especificar cantidad no menor a 8 caracteres) caracteres,
 - suspendan o bloqueen permanentemente al usuario luego de ... (especificar cantidad no mayor a 3) intentos de entrar con una contraseña incorrecta (debe pedir la rehabilitación ante quien corresponda),
 - solicitar el cambio de la contraseña cada ... (especificar lapso no mayor a 45 días),
 - impedir que las últimas (especificar cantidad no menor a 12) contraseñas sean reutilizadas,
 - establecer un tiempo de vida mínimo de ... (especificar cantidad no mayor a 3) días para las contraseñas.

11.2.4 Control: Administración de Contraseñas Críticas

En los diferentes ambientes de procesamiento existen cuentas de usuarios con las cuales es posible efectuar actividades críticas como ser instalación de plataformas o sistemas, habilitación de servicios, actualización de software, configuración de componentes informáticos, etc. Dichas cuentas no serán de uso habitual (diario), sino que sólo serán utilizadas ante una necesidad específica de realizar alguna tarea que lo requiera y se encontrarán protegidas por contraseñas con un mayor nivel de complejidad que el habitual. El Responsable de Seguridad de la Información definirá procedimientos para la administración de dichas contraseñas críticas que contemplen lo siguiente:

- a) Se definirán las causas que justificarán el uso de contraseñas críticas así como el nivel de autorización requerido.
- b) Las contraseñas seleccionadas serán seguras, y su definición será efectuada como mínimo por dos personas, de manera que ninguna de ellas conozca la contraseña completa.
- c) Las contraseñas y los nombres de las cuentas críticas a las que pertenecen serán resguardadas debidamente.
- d) La utilización de las contraseñas críticas será registrada, documentando las causas que determinaron su uso, así como el responsable de las actividades que se efectúen con la misma.
- e) Cada contraseña crítica se renovará una vez utilizada y se definirá un período luego del cual la misma será renovada en caso de que no se la haya utilizado.
- f) Se registrarán todas las actividades que se efectúen con las cuentas críticas para luego ser revisadas. Dicho registro será revisado posteriormente por el Responsable de Seguridad de la Información.

11.2.5 Revisión de Derechos de Acceso de Usuarios

A fin de mantener un control eficaz del acceso a los datos y servicios de información, el Propietario de la Información de que se trate llevará a cabo un proceso formal, a intervalos regulares

de (indicar periodicidad no mayor a 6 meses), a fin de revisar los derechos de acceso de los usuarios. Se deben contemplar los siguientes controles:

- a) Revisar los derechos de acceso de los usuarios a intervalos de (especificar tiempo no mayor a 6 meses).
- b) Revisar las autorizaciones de privilegios especiales de derechos de acceso a intervalos de (especificar tiempo no mayor a 3 meses).
- c) Revisar las asignaciones de privilegios a intervalos de (especificar tiempo no mayor a 6 meses), a fin de garantizar que no se obtengan privilegios no autorizados.

11.3 Categoría: Responsabilidades del Usuario

Objetivo

Evitar el acceso de usuarios no-autorizados, evitar poner en peligro la información y evitar el robo de información y los medios de procesamiento de la información.

La cooperación de los usuarios autorizados es esencial para una seguridad efectiva.

Los usuarios deben estar al tanto de sus responsabilidades para mantener controles de acceso efectivos, particularmente con relación al uso de claves secretas y la seguridad del equipo del usuario.

Se debe implementar una política de escritorio y pantalla limpias para reducir el riesgo de acceso no autorizado o daño a los papeles, medios y medios de procesamiento de la información.

11.3.1 Control: Uso de Contraseñas

Los usuarios deben seguir buenas prácticas de seguridad en la selección y uso de contraseñas.

Las contraseñas constituyen un medio de validación y autenticación de la identidad de un usuario, y consecuentemente un medio para establecer derechos de acceso a las instalaciones o servicios de procesamiento de información.

Los usuarios deben cumplir las siguientes directivas:

- a) Mantener las contraseñas en secreto.
- b) Pedir el cambio de la contraseña siempre que exista un posible indicio de compromiso del sistema o de las contraseñas.
- c) Seleccionar contraseñas de calidad, de acuerdo a las prescripciones informadas por el Responsable del Activo de Información de que se trate, que:
 1. Sean fáciles de recordar.
 2. No estén basadas en algún dato que otra persona pueda adivinar u obtener fácilmente mediante información relacionada con la persona, por ejemplo nombres, números de teléfono, fecha de nacimiento, etc.
 3. No tengan caracteres idénticos consecutivos o grupos totalmente numéricos o totalmente alfabéticos.
- d) Cambiar las contraseñas cada vez que el sistema se lo solicite y evitar reutilizar o reciclar viejas contraseñas.
- e) Cambiar las contraseñas provisionales en el primer inicio de sesión ("log on").
- f) Evitar incluir contraseñas en los procesos automatizados de inicio de sesión, por ejemplo, aquellas almacenadas en una tecla de función o macro.
- g) Notificar de acuerdo a lo establecido en capítulo 13 (Gestión de Incidentes de Seguridad), cualquier incidente de seguridad relacionado con sus contraseñas: pérdida, robo o indicio de pérdida de confidencialidad.

Si los usuarios necesitan acceder a múltiples servicios o plataformas y se requiere que mantengan múltiples contraseñas, se notificará a los mismos que pueden utilizar una única contraseña para todos los servicios que brinden un nivel adecuado de protección de las contraseñas almacenadas y en tránsito.

11.3.2 Control: Equipos Desatendidos en Areas de Usuarios

Los usuarios deben garantizar que los equipos desatendidos sean protegidos adecuadamente.

Los equipos instalados en áreas de usuarios, por ejemplo estaciones de trabajo o servidores de archivos, requieren una protección específica contra accesos no autorizados cuando se encuentran desatendidos.

El Responsable de Seguridad de la Información debe coordinar con el Area de Recursos Humanos las tareas de concientización a todos los usuarios y contratistas, acerca de los requerimientos y procedimientos de seguridad, para la protección de equipos desatendidos, así como de sus funciones en relación a la implementación de dicha protección.

Los usuarios cumplirán con las siguientes pautas:

- a) Concluir las sesiones activas al finalizar las tareas, a menos que puedan protegerse mediante un mecanismo de bloqueo adecuado, por ejemplo, un protector de pantalla protegido por contraseña.
- b) Proteger las PC's o terminales contra usos no autorizados mediante un bloqueo de seguridad o control equivalente, por ejemplo, contraseña de acceso cuando no se utilizan.

11.4 Categoría: Control de Acceso a la Red

Objetivo

Evitar el acceso no autorizado a los servicios de la red.

Se debe controlar el acceso a los servicios de redes internas y externas.

El acceso del usuario a las redes y servicios de las redes no deben comprometer la seguridad de los servicios de la red asegurando:

- a) que existan las interfaces apropiadas entre la red del Organismo y las redes de otras organizaciones, y redes públicas;
- b) se apliquen los mecanismos de autenticación apropiados para los usuarios y el equipo;
- c) el control del acceso del usuario a la información sea obligatorio.

11.4.1 Control: Política de Utilización de los Servicios de Red

Las conexiones no seguras a los servicios de red pueden afectar a todo el Organismo, por lo tanto, se controlará el acceso a los servicios de red tanto internos como externos. Esto es necesario para garantizar que los usuarios que tengan acceso a las redes y a sus servicios, no comprometan la seguridad de los mismos.

El Responsable del Area Informática tendrá a cargo el otorgamiento del acceso a los servicios y recursos de red, únicamente de acuerdo al pedido formal del titular de una Unidad Organizativa que lo solicite para personal de su incumbencia.

Este control es particularmente importante para las conexiones de red a aplicaciones que procesen información clasificada o aplicaciones críticas, o a usuarios que utilicen el acceso desde sitios de alto riesgo, por ejemplo áreas públicas o externas que están fuera de la administración y del control de seguridad del Organismo.

Para ello, se desarrollarán procedimientos para la activación y desactivación de derechos de acceso a las redes, los cuales comprenderán:

- a) Identificar las redes y servicios de red a los cuales se permite el acceso.
- b) Realizar normas y procedimientos de autorización para determinar las personas y las redes y servicios de red a los cuales se les otorgará el acceso.
- c) Establecer controles y procedimientos de gestión para proteger el acceso a las conexiones y servicios de red.

Esta Política será coherente con la Política de Control de Accesos del Organismo .

11.4.2 Control: Camino Forzado

Las redes están diseñadas para permitir el máximo alcance de distribución de recursos y flexibilidad en la elección de la ruta a utilizar. Estas características también pueden ofrecer oportunidades para el acceso no autorizado a las aplicaciones del Organismo, o para el uso no autorizado de servicios de información. Por esto, el camino de las comunicaciones será controlado.

Se limitarán las opciones de elección de la ruta entre la terminal de usuario y los servicios a los cuales el mismo se encuentra autorizado a acceder, mediante la implementación de controles en diferentes puntos de la misma.

A continuación se enumeran algunos ejemplos a considerar en caso de implementar estos controles a los sistemas existentes:

- a) Asignar números telefónicos o líneas, en forma dedicada.
- b) Establecer la conexión automática de puertos a gateways de seguridad o a sistemas de aplicación específicos.
- c) Limitar las opciones de menú y submenú de cada uno de los usuarios.
- d) Evitar la navegación ilimitada por la red.
- e) Imponer el uso de sistemas de aplicación y/o gateways de seguridad específicos para usuarios externos de la red.
- f) Controlar activamente las comunicaciones con origen y destino autorizados a través de un gateway, por ejemplo utilizando firewalls y generando alertas ante eventos no previstos.
- g) Restringir el acceso a redes, estableciendo dominios lógicos separados, por ejemplo, redes privadas virtuales para grupos de usuarios dentro o fuera del Organismo.

Los requerimientos relativos a caminos forzados se basarán en la Política de Control de Accesos del Organismo. El Responsable de Seguridad de la Información, conjuntamente con el Propietario de la Información de que se trate, realizará una evaluación de riesgos a fin de determinar los mecanismos de control que corresponda en cada caso.

11.4.3 Control: Autenticación de Usuarios para Conexiones Externas

Las conexiones externas son de gran potencial para accesos no autorizados a la información del Organismo. Por consiguiente, el acceso de usuarios remotos estará sujeto al cumplimiento de procedimientos de autenticación. Existen diferentes métodos de autenticación, algunos de los cuales brindan un mayor nivel de protección que otros. El Responsable de Seguridad de la Información, conjuntamente con el Propietario de la Información de que se trate, realizará una evaluación de riesgos a fin de determinar el mecanismo de autenticación que corresponda en cada caso.

La autenticación de usuarios remotos puede llevarse a cabo utilizando:

- a) Un método de autenticación físico (por ejemplo tokens de hardware), para lo que debe implementarse un procedimiento que incluya:
 - Asignación de la herramienta de autenticación.
 - Registro de los poseedores de autenticadores.
 - Mecanismo de rescate al momento de la desvinculación del personal al que se le otorgó.
 - Método de revocación de acceso del autenticador, en caso de compromiso de seguridad.
- b) Un protocolo de autenticación (por ejemplo desafío/respuesta), para lo que debe implementarse un procedimiento que incluya:
 - Establecimiento de las reglas con el usuario.

- Establecimiento de un ciclo de vida de las reglas para su renovación.

c) También pueden utilizarse líneas dedicadas privadas o una herramienta de verificación de la dirección del usuario de red, a fin de constatar el origen de la conexión.

Los procedimientos y controles de rellamada, o dial-back, pueden brindar protección contra conexiones no autorizadas a las instalaciones de procesamiento de información del Organismo. Al aplicar este tipo de control, el Organismo no debe utilizar servicios de red que incluyan desvío de llamadas. Si por alguna causa es preciso mantener el desvío de llamadas, no será posible aplicar el control de rellamada. Asimismo, es importante que el proceso de re-llamada garantice que se produzca a su término, una desconexión real del lado del Organismo.

En caso de utilizarse sistemas de Voz sobre IP, deben ajustarse los controles a fin de que no sean utilizados para efectuar comunicaciones no autorizadas (ej: bloqueo de puertos).

11.4.4 Control: Autenticación de Nodos

Una herramienta de conexión automática a una computadora remota podría brindar un medio para obtener acceso no autorizado a una aplicación del Organismo. Por consiguiente, las conexiones a sistemas informáticos remotos serán autenticadas. Esto es particularmente importante si la conexión utiliza una red que está fuera de control de la gestión de seguridad del Organismo. En el punto anterior se mencionan algunos ejemplos de autenticación y de cómo puede lograrse. La autenticación de nodos puede servir como un medio alternativo de autenticación de grupos de usuarios remotos, cuando éstos están conectados a un servicio informático seguro y compartido.

11.4.5 Control: Protección de los Puertos (Ports) de Diagnóstico Remoto

Muchas computadoras y sistemas de comunicación son instalados y administrados con una herramienta de diagnóstico remoto. Si no están protegidos, estos puertos de diagnóstico proporcionan un medio de acceso no autorizado. Por consiguiente, serán protegidos por un mecanismo de seguridad apropiado, con las mismas características del punto "11.4.3 Control: Autenticación de Usuarios para Conexiones Externas". También para este caso debe tenerse en cuenta el punto "11.4.2 Control: Camino Forzado".

11.4.6 Control: Subdivisión de Redes

Para controlar la seguridad en redes extensas, se podrán dividir en dominios lógicos separados. Para esto se definirán y documentarán los perímetros de seguridad que sean convenientes. Estos perímetros se implementarán mediante la instalación de "gateways" con funcionalidades de "firewall" o redes privadas virtuales, para filtrar el tráfico entre los dominios y para bloquear el acceso no autorizado de acuerdo a la Política de Control de Accesos.

La subdivisión en dominios de la red tomará en cuenta criterios como los requerimientos de seguridad comunes de grupos de integrantes de la red, la mayor exposición de un grupo a peligros externos, separación física, u otros criterios de aglutinamiento o segregación preexistentes.

Basándose en la Política de Control de Accesos y los requerimientos de acceso (11.1 Categoría: Requerimientos para el Control de Acceso), el Responsable del Área Informática evaluará el costo relativo y el impacto en el desempeño que ocasione la implementación de enrutadores o gateways adecuados para subdividir la red. Luego decidirá, junto con el Responsable de Seguridad de la Información, el esquema más apropiado a implementar.

11.4.7 Control: Acceso a Internet

El acceso a Internet será utilizado con propósitos autorizados o con el destino por el cual fue provisto.

El Responsable de Seguridad de la Información definirá procedimientos para solicitar y aprobar accesos a Internet. Los accesos serán autorizados formalmente por el Responsable de la Unidad Organizativa a cargo del personal que lo solicite. Asimismo, se definirán las pautas de utilización de Internet para todos los usuarios.

Se evaluará la conveniencia de generar un registro de los accesos de los usuarios a Internet, con el objeto de realizar revisiones de los accesos efectuados o analizar casos particulares. Dicho control será comunicado a los usuarios de acuerdo a lo establecido en el punto 6-1-5 Control Acuerdos de confidencialidad. Para ello, el Responsable de Seguridad de la Información junto con el Responsable del Área de Informática analizarán las medidas a ser implementadas para efectivizar dicho control, como ser la instalación de "firewalls", "proxies", etc.

11.4.8 Control: Conexión a la Red

Sobre la base de lo definido en el punto "11.1 Categoría: Requerimientos", se implementarán controles para limitar la capacidad de conexión de los usuarios. Dichos controles se podrán implementar en los "gateways" que separen los diferentes dominios de la red.

Algunos ejemplos de los entornos a las que deben implementarse restricciones son:

- Correo electrónico.
- Transferencia de archivos.
- Acceso interactivo.
- Acceso a la red fuera del horario laboral.

11.4.9 Control: Ruteo de Red

En las redes compartidas, especialmente aquellas que se extienden fuera de los límites del Organismo, se incorporarán controles de ruteo, para asegurar que las conexiones informáticas y los flujos de información no violen la Política de Control de Accesos. Estos controles contemplarán mínimamente la verificación positiva de direcciones de origen y destino. Adicionalmente, para este objetivo pueden utilizarse diversos métodos incluyendo entre otros autenticación de protocolos de ruteo, ruteo estático, traducción de direcciones y listas de control de acceso.

11.4.10 Control: Seguridad de los Servicios de Red

El Responsable de Seguridad de la Información junto con el Responsable del Área Informática definirán las pautas para garantizar la seguridad de los servicios de red del Organismo, tanto públicos como privados.

Para ello se tendrán en cuenta las siguientes directivas:

- Mantener instalados y habilitados sólo aquellos servicios que sean utilizados.

- Controlar el acceso lógico a los servicios, tanto a su uso como a su administración.

- Configurar cada servicio de manera segura, evitando las vulnerabilidades que pudieran presentar.

- Instalar periódicamente las actualizaciones de seguridad.

Dicha configuración será revisada periódicamente por el Responsable de Seguridad de la Información.

11.5 Categoría: Control de Acceso al Sistema Operativo

Objetivo

Evitar el acceso no autorizado a los sistemas operativos.

Se deben utilizar medios de seguridad para restringir el acceso a los sistemas operativos a los usuarios autorizados. Los medios deben tener la capacidad para:

- autenticar a los usuarios autorizados, en concordancia con una política de control de acceso definida;
- registrar los intentos exitosos y fallidos de autenticación del sistema;
- registrar el uso de los privilegios especiales del sistema;
- emitir alarmas cuando se violan las políticas de seguridad del sistema;
- proporcionar los medios de autenticación apropiados;
- cuando sea apropiado, restringir el tiempo de conexión de los usuarios

11.5.1 Control: Identificación Automática de Terminales

El Responsable de Seguridad de la Información junto con el Responsable del Área Informática realizarán una evaluación de riesgos a fin de determinar el método de protección adecuado para el acceso al Sistema Operativo.

Si del análisis realizado surgiera la necesidad de proveer un método de identificación de terminales, se redactará un procedimiento que indique:

- El método de identificación automática de terminales utilizado.
- El detalle de transacciones permitidas por terminal o dispositivo.

11.5.2 Control: Procedimientos de Conexión de Terminales

El acceso a los servicios de información sólo será posible a través de un proceso de conexión seguro. El procedimiento de conexión en un sistema informático será diseñado para minimizar la oportunidad de acceso no autorizado.

Este procedimiento, por lo tanto, debe divulgar la mínima información posible acerca del sistema, a fin de evitar proveer de asistencia innecesaria a un usuario no autorizado.

El procedimiento de identificación debe:

- Mantener en secreto los identificadores de sistemas o aplicaciones hasta tanto se halla llevado a cabo exitosamente el proceso de conexión.
- Desplegar un aviso general advirtiendo que sólo los usuarios autorizados pueden acceder a la computadora.
- Evitar dar mensajes de ayuda que pudieran asistir a un usuario no autorizado durante el procedimiento de conexión.
- Validar la información de la conexión sólo al completarse la totalidad de los datos de entrada. Si surge una condición de error, el sistema no debe indicar que parte de los datos es correcta o incorrecta.

e) Limitar el número de intentos de conexión no exitosos permitidos y:

- Registrar los intentos no exitosos.
- Impedir otros intentos de identificación, una vez superado el límite permitido.
- Desconectar conexiones de comunicaciones de datos.
- f) Limitar el tiempo máximo permitido para el procedimiento de conexión. Si éste es excedido, el sistema debe finalizar la conexión.

g) Desplegar la siguiente información, al completarse una conexión exitosa:

- Fecha y hora de la conexión exitosa anterior.
- Detalles de los intentos de conexión no exitosos desde la última conexión exitosa.

11.5.3 Control: Identificación y Autenticación de los Usuarios

Todos los usuarios (incluido el personal de soporte técnico, como los operadores, administradores de red, programadores de sistemas y administradores de bases de datos) tendrán un identificador único (ID de usuario) solamente para su uso personal exclusivo, de manera que las actividades puedan rastrearse con posterioridad hasta llegar al individuo responsable, a fin de garantizar la trazabilidad de las transacciones. Los identificadores de usuario no darán ningún indicio del nivel de privilegio otorgado.

En circunstancias excepcionales, cuando existe un claro beneficio para el Organismo, podrá utilizarse un identificador compartido para un grupo de usuarios o una tarea específica. Para casos de esta índole, se documentará la justificación y aprobación del Propietario de la Información de que se trate.

Si se utilizará un método de autenticación físico (por ejemplo autenticadores de hardware), debe implementarse un procedimiento que incluya:

- Asignar la herramienta de autenticación.

- b) Registrar los poseedores de autenticadores.
- c) Rescatar el autenticador al momento de la desvinculación del personal al que se le otorgó.
- d) Revocar el acceso del autenticador, en caso de compromiso de seguridad.

11.5.4 Control: Sistema de Administración de Contraseñas

Las contraseñas constituyen uno de los principales medios de validación de la autoridad de un usuario para acceder a un servicio informático. Los sistemas de administración de contraseñas deben constituir una herramienta eficaz e interactiva que garantice contraseñas de calidad.

El sistema de administración de contraseñas debe:

- f) Imponer el uso de contraseñas individuales para determinar responsabilidades.
- g) Permitir que los usuarios seleccionen y cambien sus propias contraseñas (luego de cumplido el plazo mínimo de mantenimiento de las mismas) e incluir un procedimiento de confirmación para contemplar los errores de ingreso.
- h) Imponer una selección de contraseñas de calidad según lo señalado en el punto "11.3.1 Control: Uso de Contraseñas".
- i) Imponer cambios en las contraseñas en aquellos casos en que los usuarios mantengan sus propias contraseñas, según lo señalado en el punto "11.3.1 Control: Uso de Contraseñas".
- j) Obligar a los usuarios a cambiar las contraseñas provisorias en su primer procedimiento de identificación, en los casos en que ellos seleccionen sus contraseñas.
- k) Mantener un registro de las últimas 13 contraseñas utilizadas por el usuario, y evitar la reutilización de las mismas.
- l) Evitar mostrar las contraseñas en pantalla, cuando son ingresadas.
- m) Almacenar en forma separada los archivos de contraseñas y los datos de sistemas de aplicación.
- n) Almacenar las contraseñas en forma cifrada utilizando un algoritmo de cifrado unidireccional.
- o) Modificar todas las contraseñas predeterminadas por el vendedor, una vez instalado el software y el hardware (por ejemplo claves de impresoras, hubs, routers, etc.).
- p) Garantizar que el medio utilizado para acceder/utilizar el sistema de contraseñas, asegure que no se tenga acceso a información temporal o en tránsito de forma no protegida.

11.5.5 Control: Uso de Utilitarios de Sistema

La mayoría de las instalaciones informáticas tienen uno o más programas utilitarios que podrían tener la capacidad de pasar por alto los controles de sistemas y aplicaciones. Es esencial que su uso sea limitado y minuciosamente controlado. Se deben considerar los siguientes controles:

- a) Utilizar procedimientos de autenticación para utilitarios del sistema.
- b) Separar entre utilitarios del sistema y software de aplicaciones.
- c) Limitar el uso de utilitarios del sistema a la cantidad mínima viable de usuarios fiables y autorizados.
- d) Evitar que personas ajenas al Organismo tomen conocimiento de la existencia y modo de uso de los utilitarios instalados en las instalaciones informáticas.
- e) Establecer autorizaciones para uso ad hoc de utilitarios de sistema.
- f) Limitar la disponibilidad de utilitarios de sistema, por ejemplo durante el transcurso de un cambio autorizado.
- g) Registrar todo uso de utilitarios del sistema.
- h) Definir y documentar los niveles de autorización para utilitarios del sistema.
- i) Remover todo el software basado en utilitarios y software de sistema innecesarios.

11.5.6 Control: Alarmas Silenciosas para la Protección de los Usuarios

Se considerará la provisión de alarmas silenciosas para los usuarios que podrían ser objetos de coerción. La decisión de suministrar una alarma de esta índole se basará en una evaluación de riesgos que realizará el Responsable de Seguridad de la Información junto con el Responsable del Área Informática. En este caso, se definirán y asignarán funciones y procedimientos para responder a la utilización de una alarma silenciosa.

11.5.7 Control: Desconexión de Terminales por Tiempo Muerto

El Responsable de Seguridad de la Información, junto con los Propietarios de la Información de que se trate definirán cuáles se consideran terminales de alto riesgo, por ejemplo áreas públicas o externas fuera del alcance de la gestión de seguridad del Organismo, o que sirven a sistemas de alto riesgo. Las mismas se apagarán después de un período definido de inactividad, tiempo muerto, para evitar el acceso de personas no autorizadas. Esta herramienta de desconexión por tiempo muerto debe limpiar la pantalla de la terminal y debe cerrar tanto la sesión de la aplicación como la de red. El lapso por tiempo muerto responderá a los riesgos de seguridad del área y de la información que maneje la terminal.

Para las estaciones de trabajo, se implementará la desconexión por tiempo muerto, que limpie la pantalla y evite el acceso no autorizado, pero que no cierra las sesiones de aplicación o de red.

Por otro lado, si un agente debe abandonar su puesto de trabajo momentáneamente, activará protectores de pantalla con contraseñas, a los efectos de evitar que terceros puedan ver su trabajo o continuar con la sesión de usuario habilitada.

11.5.8 Control: Limitación del Horario de Conexión

Las restricciones al horario de conexión deben suministrar seguridad adicional a las aplicaciones de alto riesgo. La limitación del período durante el cual se permiten las conexiones de

terminales a los servicios informáticos reduce el espectro de oportunidades para el acceso no autorizado. Se implementará un control de esta índole para aplicaciones informáticas sensibles, especialmente aquellas terminales instaladas en ubicaciones de alto riesgo, por ejemplo áreas públicas o externas que estén fuera del alcance de la gestión de seguridad del Organismo.

Entre los controles que se deben aplicar, se enuncian:

- a) Utilizar lapsos predeterminados, por ejemplo para transmisiones de archivos en lote, o sesiones interactivas periódicas de corta duración.
- b) Limitar los tiempos de conexión al horario normal de oficina, de no existir un requerimiento operativo de horas extras o extensión horaria.
- c) Documentar debidamente los agentes que no tienen restricciones horarias y las razones de su autorización. También cuando el Propietario de la Información autorice excepciones para una extensión horaria ocasional.

11.6 Categoría: Control de Acceso a las Aplicaciones

Objetivo

Evitar el acceso no autorizado a la información mantenida en los sistemas de aplicación.

Se deben utilizar medios de seguridad para restringir el acceso a y dentro de los sistemas de aplicación.

El acceso lógico al software de la aplicación y la información se debe limitar a los usuarios autorizados. Los sistemas de aplicación debieran:

- a) controlar el acceso del usuario a la información y las funciones del sistema de aplicación, en concordancia con una política de control de acceso definida;
- b) proporcionar protección contra un acceso no autorizado de cualquier utilidad, software del sistema de operación y software malicioso que sea capaz de superar o pasar los controles del sistema o la aplicación;
- c) no comprometer a otros sistemas con los cuales se comparten recursos de información.

11.6.1 Control: Restricción del Acceso a la Información

Los usuarios de sistemas de aplicación, con inclusión del personal de soporte, tendrán acceso a la información y a las funciones de los sistemas de aplicación de conformidad con la Política de Control de Acceso definida, sobre la base de los requerimientos de cada aplicación, y conforme a la Política del Organismo para el acceso a la información.

Se aplicarán los siguientes controles, para brindar apoyo a los requerimientos de limitación de accesos:

- a) Proveer una interfaz para controlar el acceso a las funciones de los sistemas de aplicación. El Propietario de la Información involucrada será responsable de la adjudicación de accesos a las funciones. En el caso de que las actividades involucradas en el otorgamiento de acceso revistan un carácter técnico elevado, las mismas serán llevadas a cabo por personal del área de sistemas, conforme a una autorización formal emitida por el Propietario de la Información.
- b) Restringir el conocimiento de los usuarios acerca de la información o de las funciones de los sistemas de aplicación a las cuales no sean autorizados a acceder, con la adecuada edición de la documentación de usuario.
- c) Controlar los derechos de acceso de los usuarios, por ejemplo, lectura, escritura, supresión y ejecución.
- d) Garantizar que las salidas de los sistemas de aplicación que administran información sensible, contengan sólo la información que resulte pertinente para el uso de la salida, y que la misma se envíe solamente a las terminales y ubicaciones autorizadas.
- e) Revisar periódicamente dichas salidas a fin de garantizar la remoción de la información redundante.
- f) Restringir el acceso a la información por fuera del sistema encargado de su procesamiento, es decir, la modificación directa del dato almacenado.

11.6.2 Control: Aislamiento de los Sistemas Sensibles

Los sistemas críticos podrían requerir de un ambiente informático dedicado (aislado). Algunos sistemas de aplicación son suficientemente sensibles a pérdidas potenciales y requieren un tratamiento especial. La sensibilidad puede señalar que el sistema de aplicación debe ejecutarse en una computadora dedicada, que sólo debe compartir recursos con los sistemas de aplicación confiables, o no tener limitaciones. Son aplicables las siguientes consideraciones:

- a) Identificar y documentar claramente la sensibilidad de un sistema de aplicación. Esta tarea será llevada a cabo por el administrador de la aplicación.
- b) Identificar y acordar con el administrador de la aplicación sensible cuando la aplicación ha de ejecutarse en un ambiente compartido, los sistemas de aplicación con los cuales ésta compartirá los recursos.
- c) Coordinar con el Responsable del Área informática, qué servicios estarán disponibles en el entorno donde se ejecutará la aplicación, de acuerdo a los requerimientos de operación y seguridad especificados por el administrador de la aplicación.
- d) Considerar la seguridad en la administración de las copias de respaldo de la información que procesan las aplicaciones.
- e) Considerar las mismas precauciones de seguridad y privacidad, en la elaboración del plan de continuidad y/o contingencia de la ejecución de la aplicación. Ejemplo: el equipamiento alternativo o las instalaciones de emergencia donde restablecer la aplicación.

11.7 Categoría: Monitoreo del Acceso y Uso de los Sistemas

Objetivo

Asegurar que se registren y se evalúen todos los eventos significativos para la seguridad de accesos.

Verificar la existencia de procedimientos para monitorear el uso de las instalaciones de procesamiento de la información.

11.7.1 Control: Registro de Eventos

Se generarán registros de auditoría que contengan excepciones y otros eventos relativos a la seguridad.

Los registros de auditoría deben incluir:

- a) Identificación del usuario.
- b) Fecha y hora de inicio y terminación.
- c) Identidad o ubicación de la terminal, si se hubiera dispuesto identificación automática para la misma.
- d) Registros de intentos exitosos y fallidos de acceso al sistema.
- e) Registros de intentos exitosos y fallidos de acceso a datos y otros recursos.

En todos los casos, los registros de auditoría serán archivados preferentemente en un equipo diferente al que los genere y conforme los requerimientos de la Política de Retención de Registros.

Los Propietarios de la Información junto con la Unidad de Auditoría Interna o en su defecto quien sea propuesto por el Comité de Seguridad de la Información, definirán un cronograma de depuración de registros en línea en función a normas vigentes y a sus propias necesidades.

11.7.2 Control: Procedimientos y Areas de Riesgo

Se desarrollarán procedimientos para monitorear el uso de las instalaciones de procesamiento de la información, a fin de garantizar que los usuarios sólo estén desempeñando actividades que hayan sido autorizadas explícitamente.

Todos los empleados deben conocer el alcance preciso del uso adecuado de los recursos informáticos, y se les advertirá que determinadas actividades pueden ser objeto de control y monitoreo.

El alcance de estos procedimientos debe corresponderse a la evaluación de riesgos que realice el Responsable del Area Informática y el Responsable de Seguridad de la Información.

Entre las áreas que deben tenerse en cuenta se enumeran las siguientes:

- a) Acceso no autorizado, incluyendo detalles como:
 1. Identificación del usuario.
 2. Fecha y hora de eventos clave.
 3. Tipos de eventos.
 4. Archivos a los que se accede.
 5. Utilitarios y programas utilizados.
 - b) Todas las operaciones con privilegio, como:
 1. Utilización de cuenta de supervisor.
 2. Inicio y cierre del sistema.
 3. Conexión y desconexión de dispositivos de Ingreso y Salida de información o que permitan copiar datos.
 4. Cambio de fecha/hora.
 5. Cambios en la configuración de la seguridad.
 6. Alta de servicios.
 - c) Intentos de acceso no autorizado, como:
 1. Intentos fallidos.
 2. Violaciones de la Política de Accesos y notificaciones para "gateways" de red y "firewalls".
 3. Alertas de sistemas de detección de intrusiones.
 - d) Alertas o fallas de sistema como:
 1. Alertas o mensajes de consola.
 2. Excepciones del sistema de registro.
 3. Alarmas del sistema de administración de redes.
 4. Accesos remotos a los sistemas.
- Entre los factores de riesgo que se deben considerar se encuentran:
- a) La criticidad de los procesos de aplicaciones.
 - b) El valor, la sensibilidad o criticidad de la información involucrada.
 - c) La experiencia acumulada en materia de infiltración y uso inadecuado del sistema.
 - d) El alcance de la interconexión del sistema (en particular las redes públicas).

Los Propietarios de la Información manifestarán la necesidad de registrar aquellos eventos que consideren críticos para la operatoria que se encuentra bajo su responsabilidad.

11.7.3 Registro y Revisión de Eventos

Se implementará un procedimiento de registro y revisión de los registros de auditoría, orientado a producir un informe de las amenazas detectadas contra los sistemas y los métodos utilizados.

La periodicidad de dichas revisiones será definida por los Propietarios de la Información y el Responsable de Seguridad de la Información, de acuerdo a la evaluación de riesgos efectuada.

Si el volumen de la información contenida en alguno de los registros fuera muy grande, el procedimiento indicará cuáles de los registros más significativos se copiarán automáticamente en registros auxiliares.

Por otra parte, el Responsable del Area Informática, podrá disponer la utilización de herramientas de auditoría o utilitarios adecuados para llevar a cabo el control unificado de los registros.

En la asignación de funciones en materia de seguridad de la información (Ver 6-1-3 Control: Asignación de responsabilidades de la seguridad de la información), se debe separar las funciones entre quienes realizan la revisión y aquellos cuyas actividades están siendo monitoreadas.

Las herramientas de registro deben contar con los controles de acceso necesarios, a fin de garantizar que no ocurra:

- a) La desactivación de la herramienta de registro.
- b) La alteración de mensajes registrados.
- c) La edición o supresión de archivos de registro.
- d) La saturación de un medio de soporte de archivos de registro.
- e) La falla en los registros de los eventos.
- f) La sobrescritura de los registros.

La Unidad de Auditoría Interna o en su defecto quien sea propuesto por el Comité de Seguridad de la Información, tendrá acceso a los registros de eventos a fin de colaborar en el control y efectuar recomendaciones sobre modificaciones a los aspectos de seguridad. Adicionalmente podrían evaluar las herramientas de registro, pero no tendrán libre acceso a ellas.

11.8 Categoría: Dispositivos Móviles y Trabajo Remoto

Objetivo

Asegurar la seguridad de la información cuando se utiliza medios de computación y tele-trabajo móviles.

La protección requerida se debe conmensurar con los riesgos que causan estas maneras de trabajo específicas. Cuando se utiliza computación móvil, se deben considerar los riesgos de trabajar en un ambiente desprotegido y se debiera aplicar la protección apropiada. En el caso del tele-trabajo, la organización debe aplicar protección al lugar del tele-trabajo y asegurar que se establezcan los arreglos adecuados para esta manera de trabajar.

11.8.1 Control: Computación Móvil

Cuando se utilizan dispositivos informáticos móviles se debe tener especial cuidado en garantizar que no se comprometa la información ni la infraestructura del Organismo.

Se debe tener en cuenta en este sentido, cualquier dispositivo móvil y/o removible, incluyendo: Notebooks, Laptop o PDA (Asistente Personal Digital), Teléfonos Celulares y sus tarjetas de memoria, Dispositivos de Almacenamiento removibles, tales como CDs, DVDs, Disquetes, Tapes, y cualquier dispositivo de almacenamiento de conexión USB, Tarjetas de identificación personal (control de acceso), dispositivos criptográficos, cámaras digitales, etc.

Esta lista no es taxativa, ya que deben incluirse todos los dispositivos que pudieran contener información confidencial del Organismo y por lo tanto, ser pasibles de sufrir un incidente en el que se comprometa la seguridad del mismo.

Se desarrollarán procedimientos adecuados para estos dispositivos, que abarquen los siguientes conceptos:

- e) La protección física necesaria
- f) El acceso seguro a los dispositivos
- g) La utilización segura de los dispositivos en lugares públicos.
- h) El acceso a los sistemas de información y servicios del Organismo a través de dichos dispositivos.
- i) Las técnicas criptográficas a utilizar para la transmisión de información clasificada.
- j) Los mecanismos de resguardo de la información contenida en los dispositivos.
- k) La protección contra software malicioso.

La utilización de dispositivos móviles incrementa la probabilidad de ocurrencia de incidentes del tipo de pérdida, robo o hurto. En consecuencia debe entrenarse especialmente al personal que los utilice. Se desarrollarán normas y procedimientos sobre los cuidados especiales a observar ante la posesión de dispositivos móviles, que contemplarán las siguientes recomendaciones:

- a) Permanecer siempre cerca del dispositivo.
- b) No dejar desatendidos los equipos.
- c) No llamar la atención acerca de portar un equipo valioso.
- d) No poner identificaciones del Organismo en el dispositivo, salvo los estrictamente necesarios.
- e) No poner datos de contacto técnico en el dispositivo.
- f) Mantener cifrada la información clasificada.

Por otra parte, se confeccionarán procedimientos que permitan al propietario del dispositivo reportar rápidamente cualquier incidente sufrido y mitigar los riesgos a los que eventualmente estuvieran expuestos los sistemas de información del Organismo, los que incluirán:

- a) Revocación de las credenciales afectadas

b) Notificación a grupos de Trabajo donde potencialmente se pudieran haber comprometido recursos.

11.8.2 Control: Trabajo Remoto

El trabajo remoto utiliza tecnología de comunicaciones para permitir que el personal trabaje en forma remota desde un lugar externo al Organismo.

El trabajo remoto sólo será autorizado por el Responsable de la Unidad Organizativa, o superior jerárquico correspondiente, a la cual pertenezca el usuario solicitante, conjuntamente con el Responsable de Seguridad de la Información, cuando se verifique que son adoptadas todas las medidas que correspondan en materia de seguridad de la información, de modo de cumplir con la política, normas y procedimientos existentes.

Estos casos serán de excepción y serán contemplados en situaciones que justifiquen la imposibilidad de otra forma de acceso y la urgencia, tales como horarios del Organismo, solicitud de las autoridades, etc.

Para ello, se establecerán normas y procedimientos para el trabajo remoto, que consideren los siguientes aspectos:

a) La seguridad física existente en el sitio de trabajo remoto, tomando en cuenta la seguridad física del edificio y del ambiente local.

b) El ambiente de trabajo remoto propuesto.

c) Los requerimientos de seguridad de comunicaciones, tomando en cuenta la necesidad de acceso remoto a los sistemas internos del Organismo, la sensibilidad de la información a la que se accederá y que pasará a través del vínculo de comunicación y la sensibilidad del sistema interno.

d) La amenaza de acceso no autorizado a información o recursos por parte de otras personas que utilizan el lugar, por ejemplo, familia y amigos.

e) Evitar la instalación/desinstalación de software no autorizada por el Organismo.

Los controles y disposiciones comprenden:

a) Proveer de mobiliario para almacenamiento y equipamiento adecuado para las actividades de trabajo remoto.

b) Definir el trabajo permitido, el horario de trabajo, la clasificación de la información que se puede almacenar en el equipo remoto desde el cual se accede a la red del Organismo y los sistemas internos y servicio a los cuales el trabajador remoto está autorizado a acceder.

c) Proveer de un adecuado equipo de comunicación, con inclusión de métodos para asegurar el acceso remoto.

d) Incluir seguridad física.

e) Definir reglas y orientación respecto del acceso de terceros al equipamiento e información.

f) Proveer el hardware y el soporte y mantenimiento del software.

g) Definir los procedimientos de backup y de continuidad de las operaciones.

h) Efectuar auditoría y monitoreo de la seguridad.

i) Realizar la anulación de las autorizaciones, derechos de acceso y devolución del equipo cuando finalicen las actividades remotas.

j) Asegurar el reintegro del equipamiento en las mismas condiciones en que fue entregado, en el caso en que cese la necesidad de trabajar en forma remota.

Se implementarán procesos de auditoría específicos para los casos de accesos remotos, que serán revisados regularmente. Se llevará un registro de incidentes a fin de corregir eventuales fallas en la seguridad de este tipo de accesos.

12. Cláusula: Adquisición, desarrollo y mantenimiento de sistemas



Generalidades

El desarrollo y mantenimiento de las aplicaciones es un punto crítico de la seguridad.

Durante el análisis y diseño de los procesos que soportan estas aplicaciones se deben identificar, documentar y aprobar los requerimientos de seguridad a incorporar durante las etapas de desarrollo e implementación. Adicionalmente, se deben diseñar controles de validación de datos de entrada, procesamiento interno y salida de datos.

Dado que los analistas y programadores tienen el conocimiento total de la lógica de los procesos en los sistemas, se deben implementar controles que eviten maniobras dolosas por parte de estas personas u otras que puedan operar sobre los sistemas, bases de datos y plataformas de software de base (por ejemplo, operadores que puedan manipular los datos y/o atacantes que puedan comprometer/alterar la integridad de las bases de datos) y en el caso de que se lleven a cabo, identificar rápidamente al responsable.

Asimismo, es necesaria una adecuada administración de la infraestructura de base, Sistemas Operativos y Software de Base, en las distintas plataformas, para asegurar una correcta implementación de la seguridad, ya que en general los aplicativos se asientan sobre este tipo de software.

Objetivo

Asegurar la inclusión de controles de seguridad y validación de datos en la adquisición y el desarrollo de los sistemas de información.

Definir y documentar las normas y procedimientos que se aplicarán durante el ciclo de vida de los aplicativos y en la infraestructura de base en la cual se apoyan.

Definir los métodos de protección de la información crítica o sensible.

Alcance

Esta Política se aplica a todos los sistemas informáticos, tanto desarrollos propios o de terceros, y a todos los Sistemas Operativos y/o Software de Base que integren cualquiera de los ambientes administrados por el Organismo en donde residan los desarrollos mencionados.

Responsabilidad

El Responsable de Seguridad de la Información junto con el Propietario de la Información y la Unidad de Auditoría Interna, definirán los controles a ser implementados en los sistemas desarrollados internamente o por terceros, en función de una evaluación previa de riesgos.

El Responsable de Seguridad de la Información, junto con el Propietario de la Información, definirán en función a la criticidad de la información, los requerimientos de protección mediante métodos criptográficos. Luego, el Responsable de Seguridad de la Información definirá junto con el Responsable del Área de Sistemas, los métodos de encriptación a ser utilizados.

Asimismo, el Responsable de Seguridad de la Información cumplirá las siguientes funciones:

- Definir los procedimientos de administración de claves.

- Verificar el cumplimiento de los controles establecidos para el desarrollo y mantenimiento de sistemas.

- Garantizar el cumplimiento de los requerimientos de seguridad para el software.

- Definir procedimientos para: el control de cambios a los sistemas; la verificación de la seguridad de las plataformas y bases de datos que soportan e interactúan con los sistemas; el control de código malicioso; y la definición de las funciones del personal involucrado en el proceso de entrada de datos.

El Responsable del Área Informática, propondrá para su aprobación por parte del superior jerárquico que corresponda, la asignación de funciones de "implementador" y "administrador de programas fuentes" al personal de su área que considere adecuado, cuyas responsabilidades se detallan en el presente capítulo. Asimismo, verificará el cumplimiento de las definiciones establecidas sobre los controles y las medidas de seguridad a ser incorporadas a los sistemas.

El Área de Sistemas propondrá quiénes realizarán la administración de las técnicas criptográficas y claves.

El Responsable del Área de Administración incorporará aspectos relacionados con el licenciamiento, la calidad del software y la seguridad de la información en los contratos con terceros por el desarrollo de software. El Responsable del Área Jurídica participará en dicha tarea.

Política

12.1 Categoría: Requerimientos de Seguridad de los Sistemas

Objetivo

Garantizar que la seguridad sea una parte integral de los sistemas de información.

Los sistemas de información incluyen sistemas de operación, infraestructura, aplicaciones operativas, productos de venta masiva, servicios y aplicaciones desarrolladas por el usuario. El diseño e implementación del sistema de información que soporta el proceso operativo puede ser crucial para la seguridad. Se deben identificar y acordar los requerimientos de seguridad antes del desarrollo y/o implementación de los sistemas de información.

12.1.1 Control: Análisis y Especificaciones de los Requerimientos de seguridad

Esta Política se implementa para incorporar seguridad a los sistemas de información (propios o de terceros) y a las mejoras o actualizaciones que se les incorporen.

Los requerimientos para nuevos sistemas o mejoras a los existentes especificarán la necesidad de controles. Estas especificaciones deben considerar los controles automáticos a incorporar al sistema, como así también controles manuales de apoyo.

Se deben tener en cuenta las siguientes consideraciones:

a) Definir un procedimiento para que durante las etapas de análisis y diseño del sistema, se incorporen a los requerimientos, los correspondientes controles de seguridad. Este procedimiento debe incluir una etapa de evaluación de riesgos previa al diseño, para definir los requerimientos de seguridad e identificar los controles apropiados. En esta tarea deben participar las áreas usuarias, de sistemas, de seguridad informática y auditoría, especificando y aprobando los controles automáticos a incorporar al sistema y las necesidades de controles manuales complementarios. Las áreas involucradas podrán solicitar certificaciones y evaluaciones independientes para los productos a utilizar.

b) Evaluar los requerimientos de seguridad y los controles requeridos, teniendo en cuenta que éstos deben ser proporcionales en costo y esfuerzo al valor del bien que se quiere proteger y al daño potencial que pudiera ocasionar a las actividades realizadas.

c) Considerar que los controles introducidos en la etapa de diseño, son significativamente menos costosos de implementar y mantener que aquellos incluidos durante o después de la implementación.

12.2 Categoría: Seguridad en los Sistemas de Aplicación

Objetivo

Para evitar la pérdida, modificación o uso inadecuado de los datos pertenecientes a los sistemas de información, se establecerán controles y registros de auditoría, verificando:

a) La validación efectiva de datos de entrada.

b) El procesamiento interno.

c) La autenticación de mensajes (interfaces entre sistemas)

d) La validación de datos de salida.

12.2.1 Validación de Datos de Entrada

Se definirá un procedimiento que durante la etapa de diseño, especifique controles que aseguren la validez de los datos ingresados, tan cerca del punto de origen como sea posible, controlando también datos permanentes y tablas de parámetros.

Este procedimiento considerará los siguientes controles:

- Control de secuencia.
- Control de monto límite por operación y tipo de usuario.
- Control del rango de valores posibles y de su validez, de acuerdo a criterios predeterminados.
- Control de paridad.
- Control contra valores cargados en las tablas de datos.
- Controles por oposición, de forma tal que quien ingrese un dato no pueda autorizarlo y viceversa.

Por otra parte, se llevarán a cabo las siguientes acciones:

- Se definirá un procedimiento para realizar revisiones periódicas de contenidos de campos claves o archivos de datos, definiendo quién lo realizará, en qué forma, con qué método, quiénes deben ser informados del resultado, etc.
- Se definirá un procedimiento que explicita las alternativas a seguir para responder a errores de validación en un aplicativo.
- Se definirá un procedimiento que permita determinar las responsabilidades de todo el personal involucrado en el proceso de entrada de datos.

12.2.2 Control: Controles de Procesamiento Interno

Se definirá un procedimiento para que durante la etapa de diseño, se incorporen controles de validación a fin de eliminar o minimizar los riesgos de fallas de procesamiento y/o vicios por procesos de errores.

Para ello se implementarán:

- Procedimientos que permitan identificar el uso y localización en los aplicativos, de funciones de incorporación y eliminación que realizan cambios en los datos.
- Procedimientos que establezcan los controles y verificaciones necesarios para prevenir la ejecución de programas fuera de secuencia o cuando falle el procesamiento previo.
- Procedimientos que establezcan la revisión periódica de los registros de auditoría o alertas de forma de detectar cualquier anomalía en la ejecución de las transacciones.
- Procedimientos que realicen la validación de los datos generados por el sistema.
- Procedimientos que verifiquen la integridad de los datos y del software cargado o descargado entre computadoras.
- Procedimientos que controlen la integridad de registros y archivos.
- Procedimientos que verifiquen la ejecución de los aplicativos en el momento adecuado.
- Procedimientos que aseguren el orden correcto de ejecución de los aplicativos, la finalización programada en caso de falla, y la detención de las actividades de procesamiento hasta que el problema sea resuelto.

12.2.3 Control: Autenticación de Mensajes

Cuando una aplicación tenga previsto el envío de mensajes que contengan información clasificada, se implementarán los controles criptográficos determinados en el punto "12.3 Categoría: Controles Criptográficos".

12.2.4 Control: Validación de Datos de Salidas

Se establecerán procedimientos para validar la salida de los datos de las aplicaciones, incluyendo:

- Comprobaciones de la razonabilidad para probar si los datos de salida son plausibles.
- Control de conciliación de cuentas para asegurar el procesamiento de todos los datos.
- Provisión de información suficiente, para que el lector o sistema de procesamiento subsiguiente determine la exactitud, totalidad, precisión y clasificación de la información.
- Procedimientos para responder a las pruebas de validación de salidas.
- Definición de las responsabilidades de todo el personal involucrado en el proceso de salida de datos.

12.3 Categoría: Controles Criptográficos

Objetivo

Se utilizarán sistemas y técnicas criptográficas para la protección de la información en base a un análisis de riesgo efectuado, con el fin de asegurar una adecuada protección de su confidencialidad e integridad.

Se debe desarrollar una política sobre el uso de controles criptográficos. Se debe establecer una gestión clave para sostener el uso de técnicas criptográficas.

12.3.1 Control: Política de Utilización de Controles Criptográficos

El Organismo establece la presente Política de uso de controles criptográficos, a fin de determinar su correcto uso. Para ello se indica que:

a) Se utilizarán controles criptográficos en los siguientes casos:

- Para la protección de claves de acceso a sistemas, datos y servicios.
- Para la transmisión de información clasificada, fuera del ámbito del Organismo.
- Para el resguardo de información, cuando así surja de la evaluación de riesgos realizada por el Propietario de la Información y el Responsable de Seguridad de la Información.

b) Se desarrollarán procedimientos respecto de la administración de claves, de la recuperación de información cifrada en caso de pérdida, compromiso o daño de las claves y en cuanto al reemplazo de las claves de cifrado.

c) El Responsable del Area Informática propondrá la siguiente asignación de funciones:

Función	Cargo
Implementación de la Política de Controles Criptográficos	
Administración de Claves	

d) Se utilizarán los siguientes algoritmos de cifrado y tamaños de clave:

1. Cifrado Simétrico

Algoritmo	Longitud de Clave
AES	128/192/256
3DES	168 bits
IDEA	128 bits
RC4	128 bits
RC2	128 bits

2. Cifrado Asimétrico

Casos de Utilización	Algoritmo	Longitud de Clave
Para certificados utilizados en servicios relacionados a la firma digital (sellado de tiempo, almacenamiento seguro de documentos electrónicos, etc.)	RSA	2048 bits
	DSA	2048 bits
	ECDSA	210 bits
Para certificados de sitio seguro	RSA	1024 bits
Para certificados de Certificador o de información de estado de certificados	RSA	2048 bits
	DSA	2048 bits
	ECDSA	210 bits
Para certificados de usuario (personas físicas o jurídicas)	RSA	1024 bits
	DSA	1024 bits
	ECDSA	160 bits
Para digesto seguro	SHA-1	256 bits

Los algoritmos y longitudes de clave mencionados son los que a la fecha se consideran seguros. Se recomienda verificar esta condición periódicamente con el objeto de efectuar las actualizaciones correspondientes.

12.3.2 Control: Cifrado

Mediante la evaluación de riesgos que llevará a cabo el Propietario de la Información y el Responsable de Seguridad de la Información, se identificará el nivel requerido de protección, tomando en cuenta el tipo y la calidad del algoritmo de cifrado utilizado y la longitud de las claves criptográficas a utilizar.

Al implementar la Política del Organismo en materia criptográfica, se considerarán los controles aplicables a la exportación e importación de tecnología criptográfica.

12.3.4 Control: Firma Digital

Las firmas digitales proporcionan un medio de protección de la autenticidad e integridad de los documentos electrónicos. Pueden aplicarse a cualquier tipo de documento que se procese electrónicamente. Se implementan mediante el uso de una técnica criptográfica sobre la base de dos claves relacionadas de manera única, donde una clave, denominada privada, se utiliza para crear una firma y la otra, denominada pública, para verificarla.

Se tomarán recaudos para proteger la confidencialidad de las claves privadas.

Asimismo, es importante proteger la integridad de la clave pública. Esta protección se provee mediante el uso de un certificado de clave pública.

Los algoritmos de firma utilizados, como así también la longitud de clave a emplear, son las enumeradas en el punto 0. 12.3.1 Control: Política de Utilización de Controles Criptográficos, en el cuadro de cifrado asimétrico.

Se recomienda que las claves criptográficas utilizadas para firmar digitalmente no sean empleadas en procedimientos de cifrado de información. Dichas claves deben ser resguardadas bajo el control exclusivo de su titular.

Al utilizar firmas y certificados digitales, se considerará la legislación vigente (Ley N° 25.506, el Decreto N° 2628/02 y el conjunto de normas complementarias que fijan o modifican competencias y establecen procedimientos) que describa las condiciones bajo las cuales una firma digital es legalmente válida.

En algunos casos podría ser necesario establecer acuerdos especiales para respaldar el uso de las firmas digitales. A tal fin se debe obtener asesoramiento legal con respecto al marco normativo aplicable y la modalidad del acuerdo a implementar. (Ver Capítulo 12-3-1 Control: Política de utilización de controles criptográficos, en el cuadro de cifrado asimétrico).

12.3.5 Control: Servicios de No Repudio

Estos servicios se utilizarán cuando sea necesario resolver disputas acerca de la ocurrencia de un evento o acción. Su objetivo es proporcionar herramientas para evitar que aquel que haya originado una transacción electrónica niegue haberla efectuado.

12.3.6 Control: Protección de claves criptográficas

Se implementará un sistema de administración de claves criptográficas para respaldar la utilización por parte del Organismo de los dos tipos de técnicas criptográficas, a saber:

a) Técnicas de clave secreta (criptografía simétrica), cuando dos o más actores comparten la misma clave y ésta se utiliza tanto para cifrar información como para descifrarla.

b) Técnicas de clave pública (criptografía asimétrica), cuando cada usuario tiene un par de claves: una clave pública (que puede ser revelada a cualquier persona) utilizada para cifrar y una clave privada (que debe mantenerse en secreto) utilizada para descifrar. Las claves asimétricas utilizadas para cifrado no deben ser las mismas que se utilizan para firmar digitalmente.

Todas las claves serán protegidas contra modificación y destrucción, y las claves secretas y privadas serán protegidas contra copia o divulgación no autorizada.

Se aplicarán con éste propósito los algoritmos criptográficos enumerados en el punto 0. 12.3.1 Control: Política de Utilización de Controles Criptográficos.

Se proporcionará una protección adecuada al equipamiento utilizado para generar, almacenar y archivar claves, considerándolo crítico o de alto riesgo.

12.3.7 Control: Protección de Claves criptográficas: Normas y procedimientos

Se redactarán las normas y procedimientos necesarios para:

a) Generar claves para diferentes sistemas criptográficos y diferentes aplicaciones.

b) Generar y obtener certificados de clave pública de manera segura.

c) Distribuir claves de forma segura a los usuarios que corresponda, incluyendo información sobre cómo deben activarse cuando se reciban.

d) Almacenar claves, incluyendo la forma de acceso a las mismas por parte de los usuarios autorizados.

e) Cambiar o actualizar claves, incluyendo reglas sobre cuándo y cómo deben cambiarse las claves.

f) Revocar claves, incluyendo cómo deben retirarse o desactivarse las mismas, por ejemplo cuando las claves están comprometidas o cuando un usuario se desvincula del Organismo (en cuyo caso las claves también deben archivar).se).

g) Recuperar claves perdidas o alteradas como parte de la administración de la continuidad de las actividades del Organismo, por ejemplo para la recuperación de la información cifrada.

h) Archivar claves, por ejemplo, para la información archivada o resguardada.

i) Destruir claves.

j) Registrar y auditar las actividades relativas a la administración de claves.

A fin de reducir la probabilidad de compromiso, las claves tendrán fechas de inicio y caducidad de vigencia, definidas de manera que sólo puedan ser utilizadas por el lapso de (indicar lapso no mayor a 12 meses).

Además de la administración segura de las claves secretas y privadas, debe tenerse en cuenta la protección de las claves públicas. Este problema es abordado mediante el uso de un certificado de clave pública. Este certificado se generará de forma que vincule de manera única la información relativa al propietario del par de claves pública/privada con la clave pública.

En consecuencia es importante que el proceso de administración de los certificados de clave pública sea absolutamente confiable. Este proceso es llevado a cabo por una entidad denominada Autoridad de Certificación (AC) o Certificador.

12.4 Categoría: Seguridad de los Archivos del Sistema

Objetivo

Se garantizará que los desarrollos y actividades de soporte a los sistemas se lleven a cabo de manera segura, controlando el acceso a los archivos del mismo.

12.4.1 Control: Software Operativo

Se definen los siguientes controles a realizar durante la implementación del software en producción, a fin de minimizar el riesgo de alteración de los sistemas.

• Toda aplicación, desarrollada por el Organismo o por un tercero tendrá un único Responsable designado formalmente por el Responsable del Area Informática.

• Ningún programador o analista de desarrollo y mantenimiento de aplicaciones podrá acceder a los ambientes de producción.

• El Responsable del Area Informática, propondrá para su aprobación por parte del superior jerárquico que corresponda, la asignación de la función de "implementador" al personal de su área que considere adecuado, quien tendrá como funciones principales:

a) Coordinar la implementación de modificaciones o nuevos programas en el ambiente de Producción.

b) Asegurar que los sistemas aplicativos en uso, en el ambiente de Producción, sean los autorizados y aprobados de acuerdo a las normas y procedimientos vigentes.

c) Instalar las modificaciones, controlando previamente la recepción de la prueba aprobada por parte del Analista Responsable, del sector encargado del testeo y del usuario final.

d) Rechazar la implementación en caso de encontrar defectos y/o si faltara la documentación estándar establecida.

Otros controles a realizar son:

a) Guardar sólo los ejecutables en el ambiente de producción.

b) Llevar un registro de auditoría de las actualizaciones realizadas.

c) Retener las versiones previas del sistema, como medida de contingencia.

d) Definir un procedimiento que establezca los pasos a seguir para implementar las autorizaciones y conformes pertinentes, las pruebas previas a realizarse, etc.

e) Denegar permisos de modificación al implementador sobre los programas fuentes bajo su custodia.

f) Evitar, que la función de implementador sea ejercida por personal que pertenezca al sector de desarrollo o mantenimiento.

12.4.2 Control: Protección de los Datos de Prueba del Sistema

Las pruebas de los sistemas se efectuarán sobre datos extraídos del ambiente operativo. Para proteger los datos de prueba se establecerán normas y procedimientos que contemplen lo siguiente:

g) Prohibir el uso de bases de datos operativas. En caso contrario se deben despersonalizar los datos antes de su uso. Aplicar idénticos procedimientos de control de acceso que en la base de producción.

h) Solicitar autorización formal para realizar una copia de la base operativa como base de prueba, llevando registro de tal autorización.

i) Eliminar inmediatamente, una vez completadas las pruebas, la información operativa utilizada.

12.4.3 Control: Cambios a Datos Operativos

La modificación, actualización o eliminación de los datos operativos serán realizados a través de los sistemas que procesan dichos datos y de acuerdo al esquema de control de accesos implementado en los mismos. Una modificación por fuera de los sistemas a un dato, almacenado ya sea en un archivo o base de datos, podría poner en riesgo la integridad de la información.

Los casos en los que no fuera posible la aplicación de la precedente política, se considerarán como excepciones. El Responsable de Seguridad de la Información definirá procedimientos para la gestión de dichas excepciones que contemplarán lo siguiente:

a) Se generará una solicitud formal para la realización de la modificación, actualización o eliminación del dato.

b) El Propietario de la Información afectada y del Responsable de Seguridad de la Información aprobarán la ejecución del cambio evaluando las razones por las cuales se solicita.

c) Se generarán cuentas de usuario de emergencia para ser utilizadas en la ejecución de excepciones. Las mismas serán protegidas mediante contraseñas, sujetas al procedimiento de administración de contraseñas críticas y habilitadas sólo ante un requerimiento de emergencia y por el lapso que ésta dure.

d) Se designará un encargado de implementar los cambios, el cual no será personal del área de Desarrollo. En el caso de que esta función no pueda ser segregada, se aplicarán controles adicionales de acuerdo a lo establecido en 0. 10.1.3 Control: Separación de Funciones.

e) Se registrarán todas las actividades realizadas con las cuentas de emergencia. Dicho registro será revisado posteriormente por el Responsable de Seguridad de la Información.

12.4.4 Control: Acceso a las Bibliotecas de Programas fuentes

Para reducir la probabilidad de alteración de programas fuentes, se aplicarán los siguientes controles:

a) El Responsable del Area Informática, propondrá para su aprobación por parte del superior jerárquico que corresponda la función de "administrador de programas fuentes" al personal de su área que considere adecuado, quien tendrá en custodia los programas fuentes y debe:

• Proveer al Area de Desarrollo los programas fuentes solicitados para su modificación, manteniendo en todo momento la correlación programa fuente/ejecutable.

• Llevar un registro actualizado de todos los programas fuentes en uso, indicando nombre del programa, programador, Analista Responsable que autorizó, versión, fecha de última modificación y fecha/hora de compilación y estado (en modificación, en producción).

• Verificar que el Analista Responsable que autoriza la solicitud de un programa fuente sea el designado para la aplicación, rechazando el pedido en caso contrario. Registrar cada solicitud aprobada.

• Administrar las distintas versiones de una aplicación.

• Asegurar que un mismo programa fuente no sea modificado simultáneamente por más de un desarrollador.

b) Denegar al "administrador de programas fuentes" permisos de modificación sobre los programas fuentes bajo su custodia.

c) Establecer que todo programa objeto o ejecutable en producción tenga un único programa fuente asociado que garantice su origen.

d) Establecer que el implementador de producción efectuará la generación del programa objeto o ejecutable que estará en producción (compilación), a fin de garantizar tal correspondencia.

e) Desarrollar un procedimiento que garantice que toda vez que se migre a producción el módulo fuente, se cree el código ejecutable correspondiente en forma automática.

f) Evitar que la función de "administrador de programas fuentes" sea ejercida por personal que pertenezca al sector de desarrollo y/o mantenimiento.

g) Prohibir la guarda de programas fuentes históricos (que no sean los correspondientes a los programas operativos) en el ambiente de producción.

h) Prohibir el acceso a todo operador y/o usuario de aplicaciones a los ambientes y a las herramientas que permitan la generación y/o manipulación de los programas fuentes.

i) Realizar las copias de respaldo de los programas fuentes cumpliendo los requisitos de seguridad establecidos por el Organismo en los procedimientos que surgen de la presente política.

12.5 Categoría: Seguridad de los Procesos de Desarrollo y Soporte

Objetivo

Esta Política provee seguridad al software y a la información del sistema de aplicación, por lo tanto se controlarán los entornos y el soporte dado a los mismos.

12.5.1 Control Procedimiento de Control de Cambios

A fin de minimizar los riesgos de alteración de los sistemas de información, se implementarán controles estrictos durante la implementación de cambios imponiendo el cumplimiento de procedimientos formales. Estos garantizarán que se cumplan los procedimientos de seguridad y control, respetando la división de funciones.

Para ello se establecerá un procedimiento que incluya las siguientes consideraciones:

a) Verificar que los cambios sean propuestos por usuarios autorizados y respete los términos y condiciones que surjan de la licencia de uso.

b) Mantener un registro de los niveles de autorización acordados.

c) Solicitar la autorización del Propietario de la Información, en caso de tratarse de cambios a sistemas de procesamiento de la misma.

d) Efectuar un análisis de riesgos del cambio.

e) Determinar los requisitos de seguridad para el cambio.

f) Analizar el impacto de los cambios sobre los controles de seguridad existentes.

g) Obtener aprobación formal por parte del Responsable del Area Informática para las tareas detalladas, antes que comiencen las tareas.

h) Solicitar la revisión del Responsable de Seguridad de la Información para garantizar que no se violen los requerimientos de seguridad que debe cumplir el software.

i) Efectuar las actividades relativas al cambio en el ambiente de desarrollo.

j) Obtener la aprobación por parte del usuario autorizado y del área de pruebas mediante pruebas en el ambiente correspondiente.

k) Actualizar la documentación para cada cambio implementado, tanto de los manuales de usuario como de la documentación operativa.

l) Mantener un control de versiones para todas las actualizaciones de software.

m) Garantizar que la implementación se lleve a cabo minimizando la discontinuidad de las actividades y sin alterar los procesos involucrados.

n) Informar a las áreas usuarias antes de la implementación de un cambio que pueda afectar su operatoria.

o) Garantizar que sea el implementador quien efectúe el pasaje de los objetos modificados al ambiente operativo, de acuerdo a lo establecido en "12.4.1 Control: Software Operativo".

En el Anexo al presente capítulo se presenta un esquema modelo de segregación de ambientes de procesamiento.

12.5.2 Control: Revisión Técnica de los Cambios en el sistema Operativo

Toda vez que sea necesario realizar un cambio en el Sistema Operativo, los sistemas serán revisados para asegurar que no se produzca un impacto en su funcionamiento o seguridad.

Para ello, se definirá un procedimiento que incluya:

a) Revisar los procedimientos de integridad y control de aplicaciones para garantizar que no hayan sido comprometidas por el cambio.

b) Garantizar que los cambios en el sistema operativo sean informados con anterioridad a la implementación.

c) Asegurar la actualización del Plan de Continuidad de las Actividades del Organismo.

12.5.3 Control: Restricción del Cambio de Paquetes de Software

En caso de considerarlo necesario la modificación de paquetes de software suministrados por proveedores, y previa autorización del Responsable del Area Informática, se debe:

a) Analizar los términos y condiciones de la licencia a fin de determinar si las modificaciones se encuentran autorizadas.

b) Determinar la conveniencia de que la modificación sea efectuada por el Organismo, por el proveedor o por un tercero.

c) Evaluar el impacto que se produce si el Organismo se hace cargo del mantenimiento.

d) Retener el software original realizando los cambios sobre una copia perfectamente identificada, documentando exhaustivamente por si fuera necesario aplicarlo a nuevas versiones.

12.5.4 Control: Canales Ocultos y Código Malicioso

Un canal oculto puede exponer información utilizando algunos medios indirectos y desconocidos. El código malicioso está diseñado para afectar a un sistema en forma no autorizada y no requerida por el usuario.

En este sentido, se redactarán normas y procedimientos que incluyan:

a) Adquirir programas a proveedores acreditados o productos ya evaluados.

b) Examinar los códigos fuentes (cuando sea posible) antes de utilizar los programas.

c) Controlar el acceso y las modificaciones al código instalado.

d) Utilizar herramientas para la protección contra la infección del software con código malicioso.

e) Ejecutar controles y tests de evaluación de seguridad periódicamente y, en especial, previo a su puesta en producción.

12.5.6 Control: Desarrollo Externo de Software

Para el caso que se considere la tercerización del desarrollo de software, se establecerán normas y procedimientos que contemplen los siguientes puntos:

a) Acuerdos de licencias, propiedad de código y derechos conferidos (Ver 15-1-2 Derechos de Propiedad Intelectual).

b) Requerimientos contractuales con respecto a la calidad y seguridad del código y la existencia de garantías.

c) Procedimientos de certificación de la calidad y precisión del trabajo llevado a cabo por el proveedor, que incluyan auditorías, revisión de código para detectar código malicioso, verificación del cumplimiento de los requerimientos de seguridad del software establecidos, etc.

d) Verificación del cumplimiento de las condiciones de seguridad.

e) Acuerdos de custodia de los fuentes del software (y cualquier otra información requerida) en caso de quiebra de la tercera parte.

12.6 Categoría: Gestión de vulnerabilidades técnicas

Objetivo

Se implementará la gestión de las vulnerabilidades técnicas de forma efectiva, sistemática y repetible, con mediciones que confirmen su efectividad. Dichas consideraciones incluirán los sistemas operativos, y cualquier otra aplicación en uso.

12.6.1 Control: Vulnerabilidades técnicas

Se obtendrá información oportuna acerca de las vulnerabilidades técnicas de los sistemas de información utilizados, la exposición del Organismo a tales vulnerabilidades evaluadas, y se tomarán las medidas necesarias para tratar los riesgos asociados.

Para ello se contará con un inventario de software donde se detalle información de versiones del mismo así como datos del proveedor y responsable interno.

El proceso de gestión de las vulnerabilidades técnicas debe comprender:

a) Definición de roles y responsabilidades asociados con la gestión de vulnerabilidades técnicas;

b) Procedimientos de identificación de vulnerabilidades técnicas potenciales;

c) Definición de una línea de tiempo para reaccionar ante las notificaciones de las vulnerabilidades técnicas potencialmente relevantes;

d) Definición de prioridades para la atención de necesidades relacionadas con actualizaciones de seguridad;

e) Identificación de los riesgos asociados y las acciones a llevar a cabo ante vulnerabilidades identificadas;

f) Identificación de los riesgos asociados a la instalación de parches;

g) Aprobación y evaluación de los parches antes de que sean instalados para garantizar que son efectivos y que no resultan en efectos secundarios que no puedan ser tolerados;

h) Consideración de controles alternativos en caso de inexistencia de parches;

i) Generación y mantenimiento de un registro de auditoría para todos los procedimientos emprendidos;

j) Seguimiento y evaluación regular del proceso de gestión de las vulnerabilidades técnicas para garantizar su efectividad y eficiencia.

Anexo

Para cumplir con esta Política, en lo referente a los puntos "Seguridad de los Archivos del Sistema" y "Seguridad de los Procesos de Desarrollo y Soporte", se sugiere implementar un modelo de separación de funciones entre los distintos ambientes involucrados.

Toda aplicación generada en el sector de desarrollo o adquirida a un proveedor es, en algún momento, implementada en un ambiente de producción. Los controles de esta transferencia deben ser rigurosos a fin de asegurar que no se instalen programas fraudulentos. Es conveniente implementar algún software para la administración de versiones y para la transmisión de programas entre los ambientes definidos, con un registro asociado para su control.

A continuación se presenta un modelo ideal formado por tres ambientes que debe ser adaptado a las características propias de cada Organismo, teniendo en cuenta las capacidades instaladas, los recursos y el equipamiento existente.

• Ambiente de Desarrollo

Es donde se desarrollan los programas fuentes y donde se almacena toda la información relacionada con el análisis y diseño de los sistemas. El analista o programador (desarrollador) tiene total dominio sobre el ambiente. Puede recibir algún fuente para modificar, quedando registrado en el sistema de control de versiones que administra el "administrador de programas fuentes".

El desarrollador realiza las pruebas con los datos de la base de desarrollo. Cuando considera que el programa está terminado, lo pasa al ambiente de pruebas junto con la documentación requerida que le entregará al implementador de ese ambiente.

• Ambiente de Pruebas

El implementador de este ambiente recibe el programa y la documentación respectiva y realiza una prueba general con un lote de datos para tal efecto, junto con el usuario de ser posible.

El testeador realiza las pruebas con los datos de la base de pruebas. Si no detectan errores de ejecución, los resultados de las rutinas de seguridad son correctas de acuerdo a las especificaciones y considera que la documentación presentada es completa, entonces remite el programa fuente al implementador de producción por medio del sistema de control de versiones y le entrega las instrucciones. Caso contrario, vuelve atrás el ciclo devolviendo el programa al desarrollador, junto con un detalle de las observaciones.

- Ambiente de Producción

Es donde se ejecutan los sistemas y se encuentran los datos productivos. Los programas fuentes certificados se guardan en un repositorio de fuentes de producción, almacenándolos mediante un sistema de control de versiones que maneja el "administrador de programas fuentes" y donde se dejan los datos del programador que hizo la modificación, fecha, hora y tamaño de los programas fuentes y objetos o ejecutables.

El "implementador" compila el programa fuente dentro del ambiente de producción en el momento de realizar el pasaje para asegurar de esta forma que hay una correspondencia biunívoca con el ejecutable en producción y luego se elimina, dejándolo en el repositorio productivo de programas fuentes.

Deben aplicarse procedimientos de la misma naturaleza y alcance para las modificaciones de cualquier otro elemento que forme parte del sistema, por ejemplo: modelo de datos de la base de datos o cambios en los parámetros, etc. Las modificaciones realizadas al software de base (Sistemas Operativos, Motores de bases de datos, Productos middleware) deben cumplir idénticos pasos, sólo que las implementaciones las realizarán los propios administradores.

Cabe aclarar que tanto el personal de desarrollo, como el proveedor de los aplicativos, no deben tener acceso al ambiente de producción, así como tampoco a los datos reales para la realización de las pruebas en el Ambiente de Prueba. Para casos excepcionales, se debe documentar adecuadamente la autorización, los trabajos realizados y monitorearlos en todo momento.

13. Cláusula: Gestión de Incidentes de Seguridad



Generalidades

Existen numerosas amenazas que atentan contra la seguridad de la información, representando riesgos latentes que de materializarse pueden ocasionar incidentes de seguridad.

Los Organismos cuentan con innumerables activos de información, cada uno de los cuales puede encontrarse expuesto a sufrir incidentes de seguridad. Es por ello que resulta sumamente necesario contar con una capacidad de gestión de dichos incidentes que permita comenzar por su detección, llevar a cabo su tratamiento y colaborar en la prevención de futuros incidentes similares.

Objetivo

Garantizar que los eventos de seguridad de la información y las debilidades asociados a los sistemas de información sean comunicados de forma tal que se apliquen las acciones correctivas en el tiempo oportuno.

Alcance

La Política definida en este documento se aplica a todo incidente que pueda afectar la seguridad de la información del Organismo.

Responsabilidad

El Comité de Seguridad de la Información será responsable de implementar los medios y canales necesarios para que el Responsable de Seguridad de la Información maneje los reportes de incidentes y anomalías de los sistemas. Asimismo, dicho Comité, tomará conocimiento, efectuará el seguimiento de la investigación, controlará la evolución e impulsará la resolución de los incidentes relativos a la seguridad.

El Responsable de Seguridad de la Información tiene a cargo el seguimiento, documentación y análisis de los incidentes de seguridad reportados así como su comunicación al Comité de Seguridad de la Información, a los propietarios de la información y al Programa Nacional de Infraestructuras Críticas de Información y Ciberseguridad (ICIC).⁴

Asimismo, el Responsable de Seguridad de la Información y el área de Gestión de Recursos Humanos son responsables de comunicar fehacientemente los procedimientos de Gestión de Incidentes a los empleados y contratados al inicio de la relación laboral.

El Responsable del Área Jurídica participará en el tratamiento de incidentes de seguridad que requieran de su intervención.

Todo el personal del Organismo es responsable de reportar debilidades e incidentes de seguridad que oportunamente se detecten.

Política

13.1 Categoría Informe de los eventos y debilidades de la seguridad de la información

Objetivo

Asegurar que los eventos y debilidades de la seguridad de la información asociados con los sistemas de información sean comunicados de una manera que permita que se realice una acción correctiva oportuna.

13.1.1 Reporte de los eventos de la seguridad de información

Los incidentes relativos a la seguridad serán comunicados a través de las autoridades o canales apropiados tan pronto como sea posible.

⁴ El Programa Nacional tiene entre sus objetivos brindar respuesta ante incidentes en redes, centralizar y coordinar los esfuerzos para el manejo de los incidentes de seguridad que afecten a los recursos informáticos del Sector Público Nacional.

Se establecerá un procedimiento formal de comunicación y de respuesta a incidentes, indicando la acción que ha de emprenderse al recibir un informe sobre incidentes.

Dicho procedimiento debe contemplar que ante la detección de un supuesto incidente o violación de la seguridad, el Responsable de Seguridad de la Información sea informado tan pronto como se haya tomado conocimiento. Este indicará los recursos necesarios para la investigación y resolución del incidente, y se encargará de su monitoreo. Asimismo, mantendrá al Comité de Seguridad al tanto de la ocurrencia de incidentes de seguridad.

Sin perjuicio de informar a otros Organismos de competencia, el Responsable de Seguridad de la Información, comunicará al Programa Nacional de Infraestructuras Críticas de Información y Ciberseguridad (ICIC) todo incidente o violación de la seguridad, que involucre recursos informáticos.

Todos los empleados y contratistas deben conocer fehacientemente el procedimiento de comunicación de incidentes de seguridad, y deben informar formalmente los mismos tan pronto hayan tomado conocimiento de su ocurrencia.

13.1.2 Reporte de las debilidades de la seguridad

Los usuarios de servicios de información, al momento de tomar conocimiento directa o indirectamente acerca de una debilidad de seguridad, son responsables de registrar y comunicar formalmente las mismas al Responsable de Seguridad de la Información.

Se prohíbe expresamente a los usuarios la realización de pruebas para detectar y/o utilizar una supuesta debilidad o falla de seguridad.

13.1.3 Comunicación de Anomalías del Software

Se establecerán procedimientos para la comunicación de anomalías de software, los cuales deben contemplar:

- Registrar los síntomas del problema y los mensajes que aparecen en pantalla.
- Establecer las medidas de aplicación inmediata ante la presencia de una anomalía.
- Alertar inmediatamente de modo formal al Responsable de Seguridad de la Información o del Activo de que se trate.

Se prohíbe a los usuarios quitar el software que supuestamente tiene una anomalía, a menos que estén autorizados formalmente para hacerlo. La recuperación será realizada por personal experimentado, adecuadamente habilitado.

13.2 Categoría Gestión de los Incidentes y mejoras de la seguridad de la información

Objetivo

Asegurar que se aplique un enfoque consistente y efectivo a la gestión de los incidentes en la seguridad de la información.

Se deben establecer las responsabilidades y procedimientos para manejar de manera efectiva los eventos y debilidades en la seguridad de la información una vez que han sido reportados. Se debe aplicar un proceso de mejora continua para la respuesta, monitoreo, evaluación y gestión general de los incidentes en la seguridad de la información.

13.2.1 Control: Responsabilidades y procedimientos

Se establecerán funciones y procedimientos de manejo de incidentes garantizando una respuesta rápida, eficaz y sistemática a los incidentes relativos a seguridad. Se deben considerar los siguientes ítems:

- Contemplar y definir todos los tipos probables de incidentes relativos a seguridad, incluyendo como mínimo:

- Fallas operativas
- Código malicioso
- Intrusiones
- Fraude informático
- Error humano
- Catástrofes naturales

- Comunicar formalmente los incidentes a través de autoridades o canales apropiados tan pronto como sea posible.

- Contemplar los siguientes puntos en los procedimientos para los planes de contingencia normales (diseñados para recuperar sistemas y servicios tan pronto como sea posible):

- Definición de las primeras medidas a implementar
- Análisis e identificación de la causa del incidente.
- Planificación e implementación de soluciones para evitar la repetición del mismo, si fuera necesario.
- Comunicación formal con las personas afectadas o involucradas con la recuperación, del incidente.
- Notificación de la acción a la autoridad y/u Organismos pertinentes.

- Registrar pistas de auditoría y evidencia similar para:

- Análisis de problemas internos.
- Uso como evidencia en relación con una probable violación contractual o infracción normativa, o en marco de un proceso judicial (Ver capítulo 15.1. Categoría: Cumplimiento de Requisitos Legales).
- Negociación de compensaciones por parte de los proveedores de software y de servicios.

e) Implementar controles detallados y formalizados de las acciones de recuperación respecto de las violaciones de la seguridad y de corrección de fallas del sistema, garantizando:

1. Acceso a los sistemas y datos existentes sólo al personal claramente identificado y autorizado.
2. Documentación de todas las acciones de emergencia emprendidas en forma detallada.
3. Comunicación de las acciones de emergencia al titular de la Unidad Organizativa y revisión de su cumplimiento.
4. Constatación de la integridad de los controles y sistemas del Organismo en un plazo mínimo.

En los casos en los que se considere necesario, se solicitará la participación del Responsable del Área Jurídica del Organismo en el tratamiento de incidentes de seguridad ocurridos.

13.2.2 Aprendiendo a partir de los incidentes de la seguridad de la información

Se definirá un proceso que permita documentar, cuantificar y monitorear los tipos, volúmenes y costos de los incidentes y anomalías. Esta información se utilizará para identificar aquellos que sean recurrentes o de alto impacto. Esto será evaluado a efectos de establecer la necesidad de mejorar o agregar controles para limitar la frecuencia, daño y costo de casos futuros.

13.2.3 Procesos Disciplinarios

Se seguirá el proceso disciplinario formal contemplado en las normas estatutarias, escalafonarias y convencionales que rigen al personal de la Administración Pública Nacional, para los empleados que violen la Política, Normas y Procedimientos de Seguridad del Organismo (Ver capítulo 15 Cumplimiento)

14. Cláusula: Gestión de la Continuidad



Generalidades

La administración de la continuidad de las actividades es un proceso crítico que debe involucrar a todos los niveles del Organismo.

El desarrollo e implementación de planes de contingencia es una herramienta básica para garantizar que las actividades del Organismo puedan restablecerse dentro de los plazos requeridos.

Dichos planes deben mantenerse actualizados y transformarse en una parte integral del resto de los procesos de administración y gestión, debiendo incluir necesariamente controles destinados a identificar y reducir riesgos, atenuar las consecuencias de eventuales interrupciones de las actividades del organismo y asegurar la reanudación oportuna de las operaciones indispensables.

Objetivo

Minimizar los efectos de las posibles interrupciones de las actividades normales del Organismo (sean éstas resultado de desastres naturales, accidentes, fallas en el equipamiento, acciones deliberadas u otros hechos) y proteger los procesos críticos mediante una combinación de controles preventivos y acciones de recuperación.

Analizar las consecuencias de la interrupción del servicio y tomar las medidas correspondientes para la prevención de hechos similares en el futuro.

Maximizar la efectividad de las operaciones de contingencia del Organismo con el establecimiento de planes que incluyan al menos las siguientes etapas:

- a) Notificación/Activación: Consistente en la detección y determinación del daño y la activación del plan.
- b) Reanudación: Consistente en la restauración temporal de las operaciones y recuperación del daño producido al sistema original.
- c) Recuperación: Consistente en la restauración de las capacidades de proceso del sistema a las condiciones de operación normales.

Asegurar la coordinación con el personal del Organismo y los contactos externos que participarán en las estrategias de planificación de contingencias. Asignar funciones para cada actividad definida.

Alcance

Esta Política se aplica a todos los procesos críticos identificados del Organismo.

Responsabilidad

El Responsable de Seguridad de la Información participará activamente en la definición, documentación, prueba y actualización de los planes de contingencia.

Los Propietarios de la Información y el Responsable de Seguridad de la Información cumplirán las siguientes funciones:

- Identificar las amenazas que puedan ocasionar interrupciones de los procesos y/o las actividades del Organismo.
- Evaluar los riesgos para determinar el impacto de dichas interrupciones.
- Identificar los controles preventivos.
- Desarrollar un plan estratégico para determinar el enfoque global con el que se abordará la continuidad de las actividades del Organismo.
- Elaborar los planes de contingencia necesarios para garantizar la continuidad de las actividades del Organismo.

Los Responsables de Procesos revisarán periódicamente los planes bajo su incumbencia, como así también identificar cambios en las disposiciones relativas a las actividades del Organismo aún no reflejadas en los planes de continuidad.

Los administradores de cada plan verificarán el cumplimiento de los procedimientos implementados para llevar a cabo las acciones contempladas en cada plan de continuidad.

El Comité de Seguridad de la Información tendrá a cargo la coordinación del proceso de administración de la continuidad de la operatoria de los sistemas de tratamiento de información del Organismo frente a interrupciones imprevistas.

Política

14.1 Categoría: Gestión de continuidad del Organismo

Objetivo

Contraatacar las interrupciones a las actividades del organismo y proteger los procesos críticos de los efectos de fallas importantes o desastres en los sistemas de información y asegurar su reanudación oportuna.

14.1.1 Control: Proceso de Administración de la continuidad del Organismo

El Comité de Seguridad de la Información, será el responsable de la coordinación del desarrollo de los procesos que garanticen la continuidad de las actividades del Organismo.

Este Comité tendrá a cargo la coordinación del proceso de administración de la continuidad de la operatoria de los sistemas de tratamiento de información del Organismo frente a interrupciones imprevistas, lo cual incluye las siguientes funciones:

- a) Identificar y priorizar los procesos críticos de las actividades del Organismo.
- b) Asegurar que todos los integrantes del Organismo comprendan los riesgos que la misma enfrenta, en términos de probabilidad de ocurrencia e impacto de posibles amenazas, así como los efectos que una interrupción puede tener en la actividad del Organismo.
- c) Elaborar y documentar una estrategia de continuidad de las actividades del Organismo consecuente con los objetivos y prioridades acordados.
- d) Proponer planes de continuidad de las actividades del Organismo de conformidad con la estrategia de continuidad acordada.
- e) Establecer un cronograma de pruebas periódicas de cada uno de los planes de contingencia, proponiendo una asignación de funciones para su cumplimiento.
- f) Coordinar actualizaciones periódicas de los planes y procesos implementados.
- g) Considerar la contratación de seguros que podrían formar parte del proceso de continuidad de las actividades del Organismo.
- h) Proponer las modificaciones a los planes de contingencia.

14.1.2 Control: Continuidad de las Actividades y Análisis de los impactos

Con el fin de establecer un Plan de Continuidad de las Actividades del Organismo se deben contemplar los siguientes puntos:

- Identificar los eventos (amenazas) que puedan ocasionar interrupciones en los procesos de las actividades, por ejemplo, fallas en el equipamiento, comisión de ilícitos, interrupción del suministro de energía eléctrica, inundación e incendio, desastres naturales, destrucción edilicia, atentados, etc.
- Evaluar los riesgos para determinar el impacto de dichas interrupciones, tanto en términos de magnitud de daño como del período de recuperación. Dicha evaluación debe identificar los recursos críticos, los impactos producidos por una interrupción, los tiempos de interrupción aceptables o permitidos, y debe especificar las prioridades de recuperación.
- Identificar los controles preventivos, como por ejemplo sistemas de supresión de fuego, detectores de humo y fuego, contenedores resistentes al calor y a prueba de agua para los medios de backup, los registros no electrónicos vitales, etc.

Esta actividad será llevada a cabo con la activa participación de los propietarios de los procesos y recursos de información de que se trate y el Responsable de Seguridad de la Información, considerando todos los procesos de las actividades del Organismo y no limitándose a las instalaciones de procesamiento de la información.

Según los resultados de la evaluación de esta actividad, se desarrollará un plan estratégico para determinar el enfoque global con el que se abordará la continuidad de las actividades del Organismo. Una vez que se ha creado este plan, el mismo debe ser propuesto por el Comité de Seguridad de la Información a la máxima autoridad del Organismo para su aprobación.

14.1.3 Control: Elaboración e implementación de los planes de continuidad de las Actividades del Organismo

Los propietarios de procesos y recursos de información, con la asistencia del Responsable de Seguridad de la Información, elaborarán los planes de contingencia necesarios para garantizar la continuidad de las actividades del Organismo. Estos procesos deben ser propuestos por el Comité de Seguridad de la Información.

El proceso de planificación de la continuidad de las actividades considerará los siguientes puntos:

- a) Identificar y acordar respecto a todas las funciones y procedimientos de emergencia.
- b) Analizar los posibles escenarios de contingencia y definir las acciones correctivas a implementar en cada caso.
- c) Implementar procedimientos de emergencia para permitir la recuperación y restablecimiento en los plazos requeridos. Se debe dedicar especial atención a la evaluación de las dependencias de actividades externas y a los contratos vigentes.
- d) Documentar los procedimientos y procesos acordados.

e) Instruir adecuadamente al personal, en materia de procedimientos y procesos de emergencia acordados, incluyendo el manejo de crisis.

f) Instruir al personal involucrado en los procedimientos de reanudación y recuperación en los siguientes temas:

1. Objetivo del plan.
2. Mecanismos de coordinación y comunicación entre equipos (personal involucrado).
3. Procedimientos de divulgación.
4. Requisitos de la seguridad.
5. Procesos específicos para el personal involucrado.
6. Responsabilidades individuales.

g) Probar y actualizar los planes, guardando evidencia formal de las pruebas y sus resultados.

Asimismo, el proceso de planificación debe concentrarse en los objetivos de las actividades del Organismo requeridos, por ejemplo, restablecimiento de los servicios a los usuarios en un plazo aceptable. Deben considerarse los servicios y recursos que permitirán que esto ocurra, incluyendo, dotación de personal, recursos que no procesan información, así como acuerdos para reanudación de emergencia en sitios alternativos de procesamiento de la información.

14.1.4 Control: Marco para la Planificación de la continuidad de las Actividades del Organismo

Se mantendrá un solo marco para los planes de continuidad de las actividades del Organismo, a fin de garantizar que los mismos sean uniformes e identificar prioridades de prueba y mantenimiento.

Cada plan de continuidad especificará claramente las condiciones para su puesta en marcha, así como las personas a cargo de ejecutar cada componente del mismo. Cuando se identifiquen nuevos requerimientos, se modificarán los procedimientos de emergencia establecidos, por ejemplo, los planes de evacuación o los recursos de emergencia existentes.

El administrador de cada plan de continuidad será el encargado de coordinar las tareas definidas en el mismo.

Estas modificaciones deben ser propuestas por el Comité de Seguridad de la Información para su aprobación.

El marco para la planificación de la continuidad de las actividades del Organismo, tendrá en cuenta los siguientes puntos:

a) Prever las condiciones de implementación de los planes que describan el proceso a seguir (cómo evaluar la situación, qué personas estarán involucradas, etc.) antes de poner en marcha los mismos.

b) Definir los procedimientos de emergencia que describan las acciones a emprender una vez ocurrido un incidente que ponga en peligro las operaciones del Organismo y/o la vida humana. Esto debe incluir disposiciones con respecto a la gestión de las relaciones públicas y a vínculos eficaces a establecer con las autoridades públicas pertinentes, por ejemplo, la policía, bomberos y autoridades locales.

c) Realizar los procedimientos de emergencia que describan las acciones a emprender para el traslado de actividades esenciales del Organismo o de servicios de soporte a ubicaciones transitorias alternativas, y para el restablecimiento de los procesos en los plazos requeridos.

d) Redactar los procedimientos de recuperación que describan las acciones a emprender para restablecer las operaciones normales del Organismo.

e) Definir un cronograma de mantenimiento que especifique cómo y cuándo será probado el plan, y el proceso para el mantenimiento del mismo.

f) Efectuar actividades de concientización e instrucción al personal, diseñadas para propiciar la comprensión de los procesos de continuidad las actividades y garantizar que los procesos sigan siendo eficaces.

g) Documentar las responsabilidades y funciones de las personas, describiendo los responsables de la ejecución de cada uno de los componentes del plan y las vías de contacto posibles. Se deben mencionar alternativas cuando corresponda. Es de suma importancia definir a un responsable de declarar el estado de contingencia, lo cual dará inicio al plan.

Los administradores de los planes de contingencia son:

Plan de Contingencia	Administrador
.....	
.....	

El cumplimiento de los procedimientos implementados para llevar a cabo las acciones contempladas en cada plan de continuidad, deben contarse entre las responsabilidades de los administradores de cada plan. Las disposiciones de emergencia para servicios técnicos alternativos, como instalaciones de comunicaciones o de procesamiento de información, normalmente se cuentan entre las responsabilidades de los proveedores de servicios.

14.1.5 Control: Ensayo, Mantenimiento y Reevaluación de los Planes de continuidad del Organismo

Debido a que los planes de continuidad de las actividades del Organismo pueden fallar, por suposiciones incorrectas, errores o cambios en el equipamiento, se establecen las siguientes pautas de acción:

- El Comité de Seguridad de la Información establecerá un cronograma de pruebas periódicas de cada uno de los planes de contingencia.

- El cronograma indicará quiénes son los responsables de llevar a cabo cada una de las pruebas y de elevar el resultado obtenido al citado Comité.

Se deben utilizar diversas técnicas para garantizar que los planes de contingencia funcionarán ante un hecho real, y éstas incluirán por lo menos:

a) Efectuar pruebas de discusión de diversos escenarios (discutiendo medidas para la recuperación las actividades utilizando ejemplos de interrupciones).

b) Realizar simulaciones (especialmente para entrenar al personal en el desempeño de sus roles de gestión posterior a incidentes o crisis).

c) Efectuar pruebas de recuperación técnica (garantizando que los sistemas de información puedan ser restablecidos con eficacia).

d) Realizar ensayos completos probando que el Organismo, el personal, el equipamiento, las instalaciones y los procesos pueden afrontar las interrupciones.

Para las operaciones críticas del Organismo se tomarán en cuenta, además, los siguientes mecanismos:

a) Efectuar pruebas de recuperación en un sitio alternativo (ejecutando los procesos de las actividades del Organismo en paralelo, con operaciones de recuperación fuera del sitio principal).

b) Realizar pruebas de instalaciones y servicios de proveedores (garantizando que los productos y servicios de proveedores externos cumplan con los compromisos contraídos).

Todas las pruebas efectuadas deben ser documentadas, resguardándose la evidencia formal de la ejecución y de los resultados obtenidos.

Los planes de continuidad de las actividades del Organismo serán revisados y actualizados periódicamente, para garantizar su eficacia permanente. Se incluirán procedimientos en el programa de administración de cambios del Organismo para garantizar que se aborden adecuadamente los tópicos de continuidad de las actividades.

La periodicidad de revisión de los planes de contingencia es la siguiente:

Plan de Contingencia	Revisar cada	Responsable de Revisión

Cada uno de los Responsables de Procesos es el responsable de las revisiones periódicas de cada uno de los planes de continuidad de su incumbencia, como así también de la identificación de cambios en las disposiciones relativas a las actividades del Organismo aún no reflejadas en dichos planes.

Debe prestarse atención, especialmente, a los cambios de:

- a) Personal.
- b) Direcciones o números telefónicos.
- c) Estrategia del Organismo.
- d) Ubicación, instalaciones y recursos.
- e) Legislación.
- f) Contratistas, proveedores y clientes críticos.
- g) Procesos, o procesos nuevos/eliminados.
- h) Tecnologías.
- i) Requisitos operacionales.
- j) Requisitos de seguridad.
- k) Hardware, software y otros equipos (tipos, especificaciones, y cantidad).
- l) Requerimientos de los sitios alternativos.
- m) Registros de datos vitales.

Todas las modificaciones efectuadas serán propuestas por el Comité de Seguridad de la Información para su aprobación por el superior jerárquico que corresponda.

Por otra parte, el resultado de este proceso será dado a conocer a fin de que todo el personal involucrado tenga conocimiento de los cambios incorporados.

15. Cláusula: Cumplimiento



Generalidades

El diseño, operación, uso y administración de los sistemas de información están regulados por disposiciones legales y contractuales.

Los requisitos normativos y contractuales pertinentes a cada sistema de información deben estar debidamente definidos y documentados.

El Area Jurídica del Organismo, será responsable de encuadrar jurídicamente la formulación e implementación de la política.

Objetivos

Cumplir con las disposiciones normativas y contractuales a fin de evitar sanciones administrativas al Organismo y/o al empleado o que incurran en responsabilidad civil o penal como resultado de su incumplimiento.

Garantizar que los sistemas cumplan con la política, normas y procedimientos de seguridad del Organismo.

Revisar la seguridad de los sistemas de información periódicamente a efectos de garantizar la adecuada aplicación de la política, normas y procedimientos de seguridad, sobre las plataformas tecnológicas y los sistemas de información.

Optimizar la eficacia del proceso de auditoría de sistemas y minimizar los problemas que pudiera ocasionar el mismo, o los obstáculos que pudieran afectarlo.

Garantizar la existencia de controles que protejan los sistemas en producción y las herramientas de auditoría en el transcurso de las auditorías de sistemas.

Determinar los plazos para el mantenimiento de información y para la recolección de evidencia del Organismo.

Alcance

Esta Política se aplica a todo el personal del Organismo, cualquiera sea su situación de revista.

Asimismo se aplica a los sistemas de información, normas, procedimientos, documentación y plataformas técnicas del Organismo y a las auditorías efectuadas sobre los mismos.

Responsabilidad

El Responsable de Seguridad de la Información cumplirá las siguientes funciones:

- Definir normas y procedimientos para garantizar el cumplimiento de las restricciones legales al uso del material protegido por normas de propiedad intelectual y a la conservación de registros.

- Realizar revisiones periódicas de todas las áreas del Organismo a efectos de garantizar el cumplimiento de la política, normas y procedimientos de seguridad.

- Verificar periódicamente que los sistemas de información cumplan la política, normas y procedimientos de seguridad establecidos.

- Garantizar la seguridad y el control de las herramientas utilizadas para las revisiones de auditoría.

El Responsable del Area Jurídica del Organismo, con la asistencia del Responsable de Seguridad de la Información cumplirán las siguientes funciones:

- Definir y documentar claramente todos los requisitos normativos y contractuales pertinentes para cada sistema de información.

- Redactar un Compromiso de Confidencialidad a ser firmado por todo el personal.

Los Responsables de Unidades Organizativas velarán por la correcta implementación y cumplimiento de las normas y procedimientos de seguridad establecidos en la presente Política, dentro de su área de responsabilidad.

Todos los empleados de los mandos medios y superiores conocerán, comprenderán, darán a conocer, cumplirán y harán cumplir la presente Política y la normativa vigente.

Política

15.1 Categoría: Cumplimiento de Requisitos Legales

Objetivo

Evitar las violaciones a cualquier ley; regulación estatutaria, reguladora o contractual; y cualquier requerimiento de seguridad.

El diseño, operación, uso y gestión de los sistemas de información pueden estar sujetos a requerimientos de seguridad estatutarios, reguladores y contractuales.

15.1.1 Control: Identificación de la Legislación Aplicable

Se definirán y documentarán claramente todos los requisitos normativos y contractuales pertinentes para cada sistema de información. Del mismo modo se definirán y documentarán los controles específicos y las responsabilidades y funciones individuales para cumplir con dichos requisitos.

15.1.2 Control: Derechos de Propiedad Intelectual

Se implementarán procedimientos adecuados para garantizar el cumplimiento de las restricciones legales al uso del material protegido por normas de propiedad intelectual.

Los empleados únicamente podrán utilizar material autorizado por el Organismo.

El Organismo sólo podrá autorizar el uso de material producido por el mismo, o material autorizado o suministrado al mismo por su titular, conforme los términos y condiciones acordados y lo dispuesto por la normativa vigente.

La infracción a estos derechos puede tener como resultado acciones legales que podrían derivar en demandas penales.

Se deben tener presentes las siguientes normas:

- Ley de Propiedad Intelectual N° 11.723: Protege los derechos de autor de las obras científicas, literarias y artísticas, incluyendo los programas de computación fuente y objeto; las compilaciones de datos o de otros materiales.

- Ley de Marcas N° 22.362: Protege la propiedad de una marca y la exclusividad de su uso.

- Ley de Patentes de Invención y Modelos de Utilidad N° 24.481: Protege el derecho del titular de la patente de invención a impedir que terceros utilicen su producto o procedimiento.

Derecho de Propiedad Intelectual del Software

El software es considerado una obra intelectual que goza de la protección de la Ley 11.723 de Propiedad Intelectual.

Esta Ley establece que la explotación de la propiedad intelectual sobre los programas de computación incluirá, entre otras formas, los contratos de licencia para su uso o reproducción.

Los productos de software se suministran normalmente bajo acuerdos de licencia que suelen limitar el uso de los productos al equipamiento específico y su copia a la creación de copias de resguardo solamente.

El Responsable de Seguridad de la Información, con la asistencia del Area Jurídica, analizará los términos y condiciones de la licencia, e implementará los siguientes controles:

a) Definir normas y procedimientos para el cumplimiento del derecho de propiedad intelectual de software que defina el uso legal de productos de información y de software.

b) Divulgar las políticas de adquisición de software y las disposiciones de la Ley de Propiedad Intelectual, y notificar la determinación de tomar acciones disciplinarias contra el personal que las infrinja.

c) Mantener un adecuado registro de activos.

d) Conservar pruebas y evidencias de propiedad de licencias, discos maestros, manuales, etc.

e) Implementar controles para evitar el exceso del número máximo permitido de usuarios.

f) Verificar que sólo se instalen productos con licencia y software autorizado.

g) Elaborar y divulgar un procedimiento para el mantenimiento de condiciones adecuadas con respecto a las licencias.

h) Elaborar y divulgar un procedimiento relativo a la eliminación o transferencia de software a terceros.

i) Utilizar herramientas de auditoría adecuadas.

j) Cumplir con los términos y condiciones establecidos para obtener software e información en redes públicas.

15.1.3 Control: Protección de los Registros del Organismo

Los registros críticos del Organismo se protegerán contra pérdida, destrucción y falsificación. Algunos registros pueden requerir una retención segura para cumplir requisitos legales o normativos, así como para respaldar actividades esenciales del Organismo.

Los registros se clasificarán en diferentes tipos, por ejemplo registros contables, registros de base de datos, registros de auditoría y procedimientos operativos, cada uno de ellos detallando los períodos de retención y el tipo de medios de almacenamiento, por ejemplo papel, microfichas, medios magnéticos u ópticos.

Tipo de Registro	Sistema de Información	Período de Retención	Medio de Almacenamiento	Responsable

Las claves criptográficas asociadas con archivos cifrados se mantendrán en forma segura y estarán disponibles para su uso por parte de personas autorizadas cuando resulte necesario (Ver 0. 12.3 Categoría: Controles Criptográficos).

Se debe considerar la posibilidad de degradación de los medios utilizados para el almacenamiento de los registros. Los procedimientos de almacenamiento y manipulación se implementarán de acuerdo con las recomendaciones del fabricante. (Ver 0. 12.3.1 Control: Política de Utilización de Controles Criptográficos).

Si se seleccionan medios de almacenamiento electrónicos, se incluirán los procedimientos para garantizar la capacidad de acceso a los datos (tanto legibilidad de formato como medios) durante todo el período de retención, a fin de salvaguardar los mismos contra eventuales pérdidas ocasionadas por futuros cambios tecnológicos.

Los sistemas de almacenamiento de datos serán seleccionados de modo tal que los datos requeridos puedan recuperarse de una manera que resulte aceptable para un tribunal de justicia, por ejemplo que todos los registros requeridos puedan recuperarse en un plazo y un formato aceptable.

El sistema de almacenamiento y manipulación garantizará una clara identificación de los registros y de su período de retención legal o normativa. Asimismo, se permitirá una adecuada destrucción de los registros una vez transcurrido dicho período, si ya no resultan necesarios para el Organismo.

A fin de cumplir con estas obligaciones, se tomarán las siguientes medidas:

a) Elaborar y divulgar los lineamientos para la retención, almacenamiento, manipulación y eliminación de registros e información.

b) Preparar un cronograma de retención identificando los tipos esenciales de registros y el período durante el cual deben ser retenidos.

c) Mantener un inventario de programas fuentes de información clave.

d) Implementar adecuados controles para proteger la información y los registros esenciales contra pérdida, destrucción y falsificación.

En particular, se deben tener presente las siguientes normas:

- Etica en el Ejercicio de la Función Pública. Ley 25.188: Establece que las personas que se desempeñen en la función pública deben proteger y conservar la propiedad del Estado y sólo emplear sus bienes con los fines autorizados.

- Código de Etica de la Función Pública: Dispone que el funcionario público debe proteger y conservar los bienes del Estado y utilizar los que le fueran asignados para el desempeño de sus funciones de manera racional, evitando su abuso, derroche o desaprovechamiento.

- Código Penal Art. 255: Sanciona a quien sustrajere, ocultare, destruyere o inutilizare objetos destinados a servir de prueba ante la autoridad competente, registros o documentos confiados a la custodia de un funcionario o de otra persona en el interés del servicio público. Si el culpable fuere el mismo depositario, sufrirá además inhabilitación especial por doble tiempo.

- Ley N° 24.624. Artículo 30: Autoriza el archivo y la conservación en soporte electrónico u óptico indeleble de la documentación financiera, de personal y de control de la Administración Pública Nacional y otorga valor jurídico y probatorio a la documentación existente que se incorpore al Archivo General de la Administración, mediante la utilización de tecnología que garantice la estabilidad, perdurabilidad, inmutabilidad e inalterabilidad del soporte de guarda físico de la mencionada documentación.

- Decisión Administrativa 43/96: Reglamenta el Art. 30 de la Ley 24.624. Determina su ámbito de aplicación, define conceptos y precisa los requisitos de carácter general, los relacionados con los documentos en particular y con el soporte a utilizar en la redacción, producción o reproducción de aquéllos.

- Ley de Propiedad Intelectual N° 11.723: Protege los derechos de autor de las obras científicas, literarias y artísticas, incluyendo las compilaciones de datos o de otros materiales.

- Ley N° 25.506: Establece que la exigencia legal de conservar documentos, registros o datos, también queda satisfecha con la conservación de los correspondientes documentos digitales firmados digitalmente, según los procedimientos que determine la reglamentación, siempre que sean accesibles para su posterior consulta y permitan determinar fehacientemente el origen, destino, fecha y hora de su generación, envío y/o recepción.

- Código Penal: Sanciona a aquel que alterare, destruyere o inutilizare datos, documentos, programas o sistemas informáticos (Art. 183).

15.1.3 Control: Protección de Datos y Privacidad de la Información Personal

Todos los empleados deben conocer las restricciones al tratamiento de los datos y de la información respecto a la cual tengan conocimiento con motivo del ejercicio de sus funciones.

El Organismo redactará un "Compromiso de Confidencialidad", el cual debe ser suscrito por todos los empleados y contratistas. La copia firmada del compromiso será retenida en forma segura por el Organismo.

Mediante este instrumento el empleado se comprometerá a utilizar la información solamente para el uso específico al que se ha destinado y a no comunicar, diseminar o de alguna otra forma hacer pública la información a ninguna persona, firma, compañía o tercera persona, salvo autorización previa y escrita del Responsable del Activo de que se trate. A través del "Compromiso de Confidencialidad" se debe advertir al empleado que determinadas actividades pueden ser objeto de control y monitoreo. Estas actividades deben ser detalladas a fin de no violar el derecho a la privacidad del empleado (Ver 6-1-5 Control: Acuerdos de confidencialidad).

En particular, se deben tener presente las siguientes normas:

- Ley Marco de Regulación de Empleo Público Nacional. Ley 25.164: Establece que los Funcionarios Públicos deben observar el deber de fidelidad que se derive de la índole de las tareas que le fueron asignadas y guardar la discreción correspondiente o la reserva absoluta, en su caso, de todo asunto del servicio que así lo requiera.

- Convenio Colectivo de Trabajo General: Dispone que todos los agentes deben observar el deber de fidelidad que se derive de la índole de las tareas que le fueron asignadas y guardar la discreción correspondiente, con respecto a todos los hechos e informaciones de los cuales tenga conocimiento en el ejercicio o con motivo del ejercicio de sus funciones.

- Etica en el Ejercicio de la Función Pública. Ley 25.188: Obliga a todas las personas que se desempeñen en la función pública a abstenerse de utilizar información adquirida en el cumplimiento de sus funciones para realizar actividades no relacionadas con sus tareas oficiales o de permitir su uso en beneficio de intereses privados.

- Código de Etica de la Función Pública: Establece que el funcionario público debe abstenerse de difundir toda información que hubiera sido calificada como reservada o secreta conforme a las disposiciones vigentes, ni la debe utilizar, en beneficio propio o de terceros o para fines ajenos al servicio, información de la que tenga conocimiento con motivo o en ocasión del ejercicio de sus funciones y que no esté destinada al público en general.

- Protección de Datos Personales. Ley 25.326: Establece responsabilidades para aquellas personas que recopilan, procesan y divulgan información personal y define criterios para procesar datos personales o cederlos a terceros.

- Confidencialidad. Ley N° 24.766: Impide la divulgación a terceros, o su utilización sin previo consentimiento y de manera contraria a los usos comerciales honestos, de información secreta y con valor comercial que haya sido objeto de medidas razonables para mantenerla secreta.

- Código Penal: Sanciona a aquel que abriere o accediere indebidamente a una comunicación electrónica o indebidamente la suprimiere o desviare (Art. 153), al que a sabiendas accediere por cualquier medio, sin la debida autorización o excediendo la que posea, a un sistema o dato informático de acceso restringido (Art. 153 bis), al que el que hallándose en posesión de una correspondencia, una comunicación electrónica, un pliego cerrado, un despacho telegráfico, telefónico o de otra naturaleza, no destinados a la publicidad, los hiciere publicar indebidamente, si el hecho causare o pudiere causar perjuicios a terceros. (Art. 155), al que teniendo noticias de un secreto cuya divulgación pueda causar daño, lo revelare sin justa causa (Art. 156), al funcionario público que revelare hechos, actuaciones o documentos que por la ley deben quedar secretos (Art. 157), al que a sabiendas e ilegítimamente, o violando sistemas de confidencialidad y seguridad de datos, accediere, de cualquier forma, a un banco de datos personales, ilegítimamente proporcionare o revelare a otro información registrada en un archivo o en un banco de datos personales cuyo secreto estuviere obligado a preservar por disposición de la ley e ilegítimamente insertare o hiciere insertar datos en un archivo de datos personales (Art. 157 bis), al que alterare, destruyere o inutilizare datos, documentos, programas o sistemas informáticos (Art. 183), al que revelare secretos políticos o militares concernientes a la seguridad, a los medios de defensa o a las relaciones exteriores de la Nación, o al que por imprudencia o negligencia diere a conocer los secretos mencionados anteriormente, de los que se hallare en posesión en virtud de su empleo u oficio (Art. 222 y 223).

Asimismo, debe considerarse lo establecido en el Decreto 1172/03, que regula el acceso a la información pública por parte de los ciudadanos.

15.1.4 Control: Prevención del Uso Inadecuado de los Recursos de Procesamiento de Información

Los recursos de procesamiento de información del Organismo se suministran con un propósito determinado. Toda utilización de estos recursos con propósitos no autorizados o ajenos al destino por el cual fueron provistos debe ser considerada como uso indebido.

Todos los empleados deben conocer el alcance preciso del uso adecuado de los recursos informáticos y deben respetarlo.

En particular, se debe respetar lo dispuesto por las siguientes normas:

- Ley Marco de Regulación de Empleo Público Nacional. Ley 25.164: Prohíbe hacer uso indebido o con fines particulares del patrimonio estatal.

- Convenio Colectivo de Trabajo General: Obliga a los agentes a no hacer uso indebido o con fines particulares del patrimonio estatal.

- Etica en el Ejercicio de la Función Pública. Ley 25.188: Obliga a las personas que se desempeñen en la función pública a proteger y conservar la propiedad del Estado y sólo emplear sus bienes con los fines autorizados.

- Código de Etica de la Función Pública: Obliga al funcionario público a proteger y conservar los bienes del Estado y utilizar los que le fueran asignados para el desempeño de sus funciones de manera racional, evitando su abuso, derroche o desaprovechamiento.

- Código Penal: Sanciona a aquel que alterare, destruyere o inutilizare datos, documentos, programas o sistemas informáticos; o vendiere, distribuyere, hiciere circular o introdujere en un sistema informático, cualquier programa destinado a causar daños (Art. 183).

15.1.6 Regulación de Controles para el Uso de Criptografía

Al utilizar firmas digitales o electrónicas, se debe considerar lo dispuesto por la Ley 25.506 y su decreto reglamentario Decreto 2628/02, que establecen las condiciones bajo las cuales una firma digital es legalmente válida.

Respecto a la comercialización de controles criptográficos, nuestro país ha suscrito el acuerdo Wassennar, que establece un listado de materiales y tecnologías de doble uso, cuya comercialización puede ser considerada peligrosa.

El Decreto 603/92 regula el Régimen de Control de las Exportaciones Sensitivas y de Material Bélico, estableciendo un tratamiento especial para la exportación de determinados bienes que pueden ser comprendidos dentro del concepto de material bélico.

Se debe obtener asesoramiento antes de transferir a otro país información cifrada o controles criptográficos. Para ello se puede consultar a la Dirección General de Política, de la Secretaría de Asuntos Militares, Ministerio de Defensa, a fin de saber si el material exportable requiere algún tratamiento especial.

15.1.7 Recolección de Evidencia

Es necesario contar con adecuada evidencia para respaldar una acción contra una persona u organización. Siempre que esta acción responda a una medida disciplinaria interna, la evidencia necesaria estará descrita en los procedimientos internos.

Cuando la acción implique la aplicación de una ley, tanto civil como penal, la evidencia presentada debe cumplir con lo establecido por las normas procesales. Para lograr la validez de la evidencia, el Organismo garantizará que sus sistemas de información cumplen con la normativa y los estándares o códigos de práctica relativos a la producción de evidencia válida.

Para lograr la calidad y totalidad de la evidencia es necesaria una sólida pista de la misma. Esta pista se establecerá cumpliendo las siguientes condiciones:

a) Almacenar los documentos en papel originales en forma segura y mantener registros acerca de quién lo halló, dónde se halló, cuándo se halló y quién presenció el hallazgo. Cualquier investigación debe garantizar que los originales no sean alterados.

b) Copiar la información para garantizar su disponibilidad. Se mantendrá un registro de todas las acciones realizadas durante el proceso de copia. Se almacenará en forma segura una copia de los medios y del registro.

Cuando se detecta un incidente, puede no resultar obvio si éste derivará en una demanda legal por lo tanto se deben tomar todos los recaudos establecidos para la obtención y preservación de la evidencia.

Se debe tener presente lo dispuesto por el Reglamento de Investigaciones Administrativas, procedimiento administrativo especial, de naturaleza correctiva interna que constituye garantía suficiente para la protección de los derechos y correcto ejercicio de las responsabilidades impuestas a los agentes públicos. Este Decreto debe ser complementado por lo dispuesto en la Ley N° 19.549 (Ley de Procedimientos Administrativos) y por toda otra normativa aplicable, incluido el Código Penal, el que sanciona a quien sustrajere, alterare, ocultare, destruyere o inutilizare en todo o en parte objetos destinados a servir de prueba ante la autoridad competente, registros o documentos confiados a la custodia de un funcionario público o de otra persona en el interés del servicio público (Art. 255).

15.1.8 Delitos Informáticos

Todos los empleados deben conocer la existencia de la Ley 26.388 de Delitos Informáticos, a partir de cuyo dictado se castigan penalmente ciertas conductas cometidas mediante medios informáticos. En tal sentido, los agentes públicos deben conocer con exactitud el alcance de los nuevos tipos penales introducidos por la norma mencionada.

Cabe señalar que la mayoría de las conductas descritas por dicha norma vinculada ya han sido señaladas en los apartados precedentes.

15.2 Categoría: Revisiones de la Política de Seguridad y la Compatibilidad Técnica

Objetivo

Asegurar el cumplimiento de los sistemas con las políticas y estándares de seguridad organizacional.

La seguridad de los sistemas de información se debiera revisar regularmente.

Estas revisiones deben realizarse en base a las políticas de seguridad apropiadas y las plataformas técnicas, y los sistemas de información deben ser auditados en cumplimiento con los estándares de implementación de seguridad aplicables y los controles de seguridad documentados.

15.2.1 Control: Cumplimiento de la Política de Seguridad

Cada Responsable de Unidad Organizativa, velará por la correcta implementación y cumplimiento de las normas y procedimientos de seguridad establecidos, dentro de su área de responsabilidad.

El Responsable de Seguridad de la Información, realizará revisiones periódicas de todas las áreas del Organismo a efectos de garantizar el cumplimiento de la política, normas y procedimientos de seguridad. Entre las áreas a revisar se incluyen las siguientes:

- a) Sistemas de información.
- b) Proveedores de sistemas.
- c) Propietarios de información.
- d) Usuarios.

Los Propietarios de la Información brindarán apoyo a la revisión periódica del cumplimiento de la política, normas, procedimientos y otros requisitos de seguridad aplicables.

15.2.2 Verificación de la Compatibilidad Técnica

El Responsable de Seguridad de la Información verificará periódicamente que los sistemas de información cumplan con la política, normas y procedimientos de seguridad, las que incluirán la revisión de los sistemas en producción a fin de garantizar que los controles de hardware y software hayan sido correctamente implementados. En caso de ser necesario, estas revisiones contemplarán la asistencia técnica especializada.

El resultado de la evaluación se volcará en un informe técnico para su ulterior interpretación por parte de los especialistas. Para ello, la tarea podrá ser realizada por un profesional experimentado (en forma manual o con el apoyo de herramientas de software), o por un paquete de software automatizado que genere reportes que serán interpretados por un especialista técnico.

La verificación del cumplimiento comprenderá pruebas de penetración y tendrá como objetivo la detección de vulnerabilidades en el sistema y la verificación de la eficacia de los controles con relación a la prevención de accesos no autorizados. Se tomarán los recaudos necesarios en el caso de pruebas de penetración exitosas que comprometan la seguridad del sistema.

Las verificaciones de cumplimiento sólo serán realizadas por personas competentes, formalmente autorizadas y bajo la supervisión.

15.3 Consideraciones de Auditorías de Sistemas

Objetivo

Maximizar la efectividad de y minimizar la interferencia desde/hacia el proceso de auditoría del sistema de información.

Durante las auditorías de los sistemas de información debieran existir controles para salvaguardar los sistemas operacionales y herramientas de auditoría.

Con relación a las auditorías, serán de aplicación las Normas de Control Interno para Tecnologías de Información, aprobadas por la resolución SIGEN N° 48/05.

15.3.1 Controles de Auditoría de Sistemas

Cuando se realicen actividades de auditoría que involucren verificaciones de los sistemas en producción, se tomarán recaudos en la planificación de los requerimientos y tareas, y se acordará con las áreas involucradas a efectos de minimizar el riesgo de interrupciones en las operaciones.

Se contemplarán los siguientes puntos:

- a) Acordar con el Area que corresponda los requerimientos de auditoría.
- b) Controlar el alcance de las verificaciones. Esta función será realizada por el responsable de auditoría.
- c) Limitar las verificaciones a un acceso de sólo lectura del software y datos de producción. Caso contrario, se tomarán los resguardos necesarios a efectos de aislar y contrarrestar los efectos de las modificaciones realizadas, una vez finalizada la auditoría. Por ejemplo:
 - Eliminar archivos transitorios.
 - Eliminar entidades ficticias y datos incorporados en archivos maestros.
 - Revertir transacciones.

- Revocar privilegios otorgados

d) Identificar claramente los recursos de tecnologías de información (TI) para llevar a cabo las verificaciones, los cuales serán puestos a disposición de los auditores. A tal efecto, la Unidad de Auditoría o en su defecto quien sea propuesto por el Comité de Seguridad de la Información completará el siguiente formulario, el cual debe ser puesto en conocimiento de las áreas involucradas:

Recursos de TI a utilizar en la Verificación	
Sistemas de información
Base de datos
Hardware
Software de Auditoría
Medios Magnéticos
Personal de Auditoría
Interlocutores de las Areas de Informática
Interlocutores de las Areas Usuarías
Conexiones a Red
.....

- e) Identificar y acordar los requerimientos de procesamiento especial o adicional.
- f) Monitorear y registrar todos los accesos, a fin de generar una pista de referencia. Los datos a resguardar deben incluir como mínimo:
 - Fecha y hora.
 - Puesto de trabajo.
 - Usuario.
 - Tipo de acceso.
 - Identificación de los datos accedidos.
 - Estado previo y posterior.
 - Programa y/o función utilizada.
- g) Documentar todos los procedimientos de auditoría, requerimientos y responsabilidades.

15.3.2 Protección de los Elementos Utilizados por la Auditoría de Sistemas

Se protegerá el acceso a los elementos utilizados en las auditorías de sistemas, o sea archivos de datos o software, a fin de evitar el mal uso o el compromiso de los mismos.

Dichas herramientas estarán separadas de los sistemas en producción y de desarrollo, y se les otorgará el nivel de protección requerido.

Se tomarán los recaudos necesarios a efectos de cumplimentar las normas de auditoría dispuestas por la Sindicatura General de la Nación.

15.3.3 Sanciones Previstas por Incumplimiento

Se sancionará administrativamente a todo aquel que viole lo dispuesto en la presente Política de Seguridad conforme a lo dispuesto por las normas estatutarias, escalafonarias y convencionales que rigen al personal de la Administración Pública Nacional, y en caso de corresponder, se realizarán las acciones correspondientes ante el o los Organismos pertinentes.

Las sanciones sólo pueden imponerse mediante un acto administrativo que así lo disponga cumpliendo las formalidades impuestas por los preceptos constitucionales, la Ley de Procedimiento Administrativo y demás normativas específicas aplicables.

Amén de las sanciones disciplinarias o administrativas, el agente que no da debido cumplimiento a sus obligaciones pueden incurrir también en responsabilidad civil o patrimonial —cuando ocasiona un daño que debe ser indemnizado— y/o en responsabilidad penal —cuando su conducta constituye un comportamiento considerado delito por el Código Penal y leyes especiales.

Separatas de Legislación



ESTUPEFACIENTES



DERECHOS DEL PACIENTE



LEY DE CONTRATO DE TRABAJO



DERECHOS DE LAS PERSONAS CON DISCAPACIDAD



AVISOS OFICIALES

Nuevos



MINISTERIO DE JUSTICIA Y DERECHOS HUMANOS

DIRECCION NACIONAL DEL DERECHO DE AUTOR

Título, autor y demás recaudos por la Ley 11.723; 27-8-2013

Expediente				
5118564	Obra Publicada	Género: LETRA	Título: AMORES	Autor: RAUL JORGE ROJAS Editor: WELA QUINAJ DE RAUL JORGE ROJAS
5118565	Obra Publicada	Género: LETRA	Título: VOY A CELEBRAR	Autor: RAUL JORGE ROJAS Autor: NESTOR MIGUEL GONZALEZ Editor: WELA QUINAJ DE RAUL JORGE ROJAS
5118566	Obra Publicada	Género: MUSICA	Título: VOY A CELEBRAR	Autor: RAUL JORGE ROJAS Autor: NESTOR MIGUEL GONZALEZ Editor: WELA QUINAJ DE RAUL JORGE ROJAS
5118567	Obra Publicada	Género: LETRA	Título: YO NO VOY A OLVIDARTE	Autor: RAUL JORGE ROJAS Editor: WELA QUINAJ DE RAUL JORGE ROJAS
5118568	Obra Publicada	Género: MUSICA	Título: YO NO VOY A OLVIDARTE	Autor: RAUL JORGE ROJAS Editor: WELA QUINAJ DE RAUL JORGE ROJAS
5118569	Obra Publicada	Género: LETRA	Título: NO VUELVAS A CRUZARTE EN MI CAMINO	Autor: RAUL JORGE ROJAS Autor: NESTOR MIGUEL GONZALEZ Editor: WELA QUINAJ DE RAUL JORGE ROJAS
5118570	Obra Publicada	Género: MUSICA	Título: NO VUELVAS A CRUZARTE EN MI CAMINO	Autor: RAUL JORGE ROJAS Autor: NESTOR MIGUEL GONZALEZ Editor: WELA QUINAJ DE RAUL JORGE ROJAS
5118571	Obra Publicada	Género: LETRA	Título: SUEÑO	Autor: RAUL JORGE ROJAS Autor: ANTONIO GABRIEL IZQUIERDO Autor: DANIEL ALEJANDRO CUEVAS AMAYA Editor: WELA QUINAJ DE RAUL JORGE ROJAS
5118572	Obra Publicada	Género: MUSICA	Título: SUEÑO	Autor: RAUL JORGE ROJAS Autor: ANTONIO GABRIEL IZQUIERDO Autor: DANIEL ALEJANDRO CUEVAS AMAYA Editor: WELA QUINAJ DE RAUL JORGE ROJAS
5118573	Obra Publicada	Género: LETRA	Título: HOY HE LLEGADO A LA CIUDAD	Autor: RAUL JORGE ROJAS Autor: NESTOR MIGUEL GONZALEZ Editor: WELA QUINAJ DE RAUL JORGE ROJAS
5118574	Obra Publicada	Género: LETRA	Título: AL BORDE DEL DELIRIO	Autor: RAUL JORGE ROJAS Autor: NESTOR MIGUEL GONZALEZ Editor: WELA QUINAJ DE RAUL JORGE ROJAS
5118575	Obra Publicada	Género: MUSICA	Título: AL BORDE DEL DELIRIO	Autor: RAUL JORGE ROJAS Autor: NESTOR MIGUEL GONZALEZ Editor: WELA QUINAJ DE RAUL JORGE ROJAS
5118576	Obra Publicada	Género: LETRA	Título: NO DIGAS ADIOS	Autor: RAUL JORGE ROJAS Autor: MARIO ALFREDO ROJAS Autor: LUCIO ROJAS Editor: WELA QUINAJ DE RAUL JORGE ROJAS
5118577	Obra Publicada	Género: MUSICA	Título: NO DIGAS ADIOS	Autor: RAUL JORGE ROJAS Autor: MARIO ALFREDO ROJAS Autor: LUCIO ROJAS Editor: WELA QUINAJ DE RAUL JORGE ROJAS
5118578	Obra Publicada	Género: LETRA	Título: VIVO PARA AMARTE	Autor: RAUL JORGE ROJAS Editor: WELA QUINAJ DE RAUL JORGE ROJAS
5118579	Obra Publicada	Género: MUSICA	Título: OJITOS DE CARNAVAL	Autor: RAUL JORGE ROJAS Editor: WELA QUINAJ DE RAUL JORGE ROJAS
5118580	Obra Publicada	Género: LETRA	Título: VOY A CELEBRAR	Autor: NESTOR MIGUEL GONZALEZ Autor: RAUL JORGE ROJAS Editor: PUBLISONG EDICIONES Editor: PUBLITRACK SRL Editor: KRISTOF GROUP DE ARIEL MARCELO NACACHE POLAT
5118581	Obra Publicada	Género: MUSICA	Título: VOY A CELEBRAR	Autor: NESTOR MIGUEL GONZALEZ Autor: RAUL JORGE ROJAS Editor: PUBLISONG EDICIONES Editor: PUBLITRACK SRL Editor: KRISTOF GROUP DE ARIEL MARCELO NACACHE POLAT
5118582	Obra Publicada	Género: LETRA	Título: NO VUELVAS A CRUZARTE EN MI CAMINO	Autor: NESTOR MIGUEL GONZALEZ Autor: RAUL JORGE ROJAS Editor: PUBLISONG EDICIONES Editor: PUBLITRACK SRL Editor: KRISTOF GROUP DE ARIEL MARCELO NACACHE POLAT
5118583	Obra Publicada	Género: MUSICA	Título: NO VUELVAS A CRUZARTE EN MI CAMINO	Autor: NESTOR MIGUEL GONZALEZ Autor: RAUL JORGE ROJAS Editor: PUBLISONG EDICIONES Editor: PUBLITRACK SRL Editor: KRISTOF GROUP DE ARIEL MARCELO NACACHE POLAT
5118584	Obra Publicada	Género: MUSICA	Título: HOY HE LLEGADO A LA CIUDAD	Autor: RAUL JORGE ROJAS Autor: NESTOR MIGUEL GONZALEZ Editor: WELA QUINAJ DE RAUL JORGE ROJAS
5118585	Obra Publicada	Género: LETRA	Título: MI RELIGION	Autor: RAUL JORGE ROJAS Autor: ALEJANDRO ROMERO Autor: CARLOS MARCELO ROSELLI MAJUL Editor: WELA QUINAJ DE RAUL JORGE ROJAS
5118586	Obra Publicada	Género: MUSICA	Título: MI RELIGION	Autor: RAUL JORGE ROJAS Autor: ALEJANDRO ROMERO Autor: CARLOS MARCELO ROSELLI MAJUL Editor: WELA QUINAJ DE RAUL JORGE ROJAS

5118587	Obra Publicada	Género: LETRA	Título: UNO MISMO	Autor: RAUL JORGE ROJAS Editor: WELA QUINAJ DE RAUL JORGE ROJAS
5118588	Obra Publicada	Género: LETRA	Título: EL SECRETO DE TU VIDA	Autor: RAUL JORGE ROJAS Autor: NESTOR MIGUEL GONZALEZ Editor: WELA QUINAJ DE RAUL JORGE ROJAS
5118589	Obra Publicada	Género: MUSICA	Título: EL SECRETO DE TU VIDA	Autor: RAUL JORGE ROJAS Autor: NESTOR MIGUEL GONZALEZ Editor: WELA QUINAJ DE RAUL JORGE ROJAS
5118590	Obra Publicada	Género: LETRA	Título: HERMANO MIO	Autor: RAUL JORGE ROJAS Autor: NESTOR RUBEN GOMEZ Editor: WELA QUINAJ DE RAUL JORGE ROJAS
5118591	Obra Publicada	Género: LETRA	Título: NUEVAMENTE	Autor: RAUL JORGE ROJAS Editor: WELA QUINAJ DE RAUL JORGE ROJAS
5118592	Obra Publicada	Género: MUSICA	Título: NUEVAMENTE	Autor: LUCIO ROJAS Editor: WELA QUINAJ DE RAUL JORGE ROJAS
5118593	Obra Publicada	Género: LETRA	Título: AL VIOLIN MAYOR	Autor: RAUL JORGE ROJAS Autor: MARIO ALFREDO ROJAS Editor: WELA QUINAJ DE RAUL JORGE ROJAS
5118594	Obra Publicada	Género: MUSICA	Título: AL VIOLIN MAYOR	Autor: RAUL JORGE ROJAS Autor: MARIO ALFREDO ROJAS Editor: WELA QUINAJ DE RAUL JORGE ROJAS
5118595	Obra Publicada	Género: LETRA	Título: LAMENTO DE LA URPILITA	Autor: RAUL JORGE ROJAS Autor: LUCIO ROJAS Editor: WELA QUINAJ DE RAUL JORGE ROJAS
5118596	Obra Publicada	Género: MUSICA	Título: LAMENTO DE LA URPILITA	Autor: RAUL JORGE ROJAS Autor: LUCIO ROJAS Editor: WELA QUINAJ DE RAUL JORGE ROJAS
5118597	Obra Publicada	Género: LETRA	Título: MONTE ADENTRO	Autor: RAUL JORGE ROJAS Autor: MARIO ALFREDO ROJAS Editor: WELA QUINAJ DE RAUL JORGE ROJAS
5118598	Obra Publicada	Género: MUSICA	Título: MONTE ADENTRO	Autor: RAUL JORGE ROJAS Autor: MARIO ALFREDO ROJAS Editor: WELA QUINAJ DE RAUL JORGE ROJAS
5118599	Obra Publicada	Género: LETRA	Título: UNA ZAMBA EN EL CIELO	Autor: RAUL JORGE ROJAS Autor: MARIO ALFREDO ROJAS Editor: WELA QUINAJ DE RAUL JORGE ROJAS
5118600	Obra Publicada	Género: MUSICA	Título: UNA ZAMBA EN EL CIELO	Autor: RAUL JORGE ROJAS Autor: MARIO ALFREDO ROJAS Editor: WELA QUINAJ DE RAUL JORGE ROJAS
5118601	Obra Publicada	Género: LETRA	Título: EL ULTIMO DESEO DE NAVIDAD	Autor: RAUL JORGE ROJAS Editor: WELA QUINAJ DE RAUL JORGE ROJAS
5118602	Obra Publicada	Género: MUSICA	Título: EL ULTIMO DESEO DE NAVIDAD	Autor: RAUL JORGE ROJAS Editor: WELA QUINAJ DE RAUL JORGE ROJAS
5118603	Obra Publicada	Género: LETRA	Título: POR SI VOLVIERAS	Autor: RAUL JORGE ROJAS Autor: ABEL FEDERICO PINTOS Editor: WELA QUINAJ DE RAUL JORGE ROJAS
5118640	Obra Publicada	Género: ENSAYO	Título: PADRES EN FUGA. ESCUELAS HUERFANAS. LA CONFLICTIVA RELACION DE LAS ESCUELAS CON LAS FAMILIAS.	Autor: MONICA CORONADO Editor: EDICIONES NOVEDADES EDUCATIVAS CENTRO DE PUBLICACIONES EDUCATIVAS Y MA
5118641	Obra Publicada	Género: DIDACTICO	Título: ENSEÑAR A ESTUDIAR A NIÑOS Y ADOLESCENTES. COMO DESARROLLAR ESTRATEGIAS Y HABITOS PARA EL APRENDIZAJ	Autor: MARIA TRESCA Editor: EDICIONES NOVEDADES EDUCATIVAS DEL CENTRO DE PUBLICACIONES EDUCATIVAS
5118642	Obra Publicada	Género: ENSAYO	Título: JUVENTUD, MEMORIA Y TRANSMISION. PENSANDO JUNTO A WALTER BENJAMIN. FRACTURA SOCIAL Y LAZOS INTERGENE	Autor: HECTOR DANIEL KORINFELD Autor: ALEJANDRO VILLA Editor: EDICIONES NOVEDADES EDUCATIVAS DEL CENTRO DE PUBLICACIONES EDUCATIVAS
5118643	Obra Publicada	Género: DIDACTICO	Título: CONSTRUYENDO LA CLASE VIRTUAL. METODOS, ESTRATEGIAS Y RECURSOS TECNOLOGICOS PARA BUENAS PRACTICAS DO	Autor: GABRIELA ASINSTEN Autor: JUAN CARLOS ASINSTEN Autor: MARIA SUSANA ESPIRO Editor: EDICIONES NOVEDADES EDUCATIVAS DEL CENTRO DE PUBLICACIONES EDUCATIVAS
5118644	Obra Publicada	Género: INFANTIL	Título: MAESTROS: NARRADORES DE LA CIENCIA.	Autor: EDUARDO WOLOVELSKY Autor: PABLO BOLAÑOS Editor: EDICIONES NOVEDADES EDUCATIVAS DEL CENTRO DE PUBLICACIONES EDUCATIVAS
5118645	Obra Publicada	Género: DIDACTICO	Título: ACTIVIDADES ESCOLARES CON TIC. HERRAMIENTAS PARA EL AULA Y SELECCION DE RECURSOS.	Autor: MAGDALENA GARZON Autor: MARIA XIMENA GARCIA TELLERIA Autor: MARTA LIBEDINSKY Autor: NATALIA LOPEZ Autor: PAULA PEREZ Editor: EDICIONES NOVEDADES EDUCATIVAS DEL CENTRO DE PUBLICACIONES EDUCATIVAS
5118646	Obra Publicada	Género: ENSAYO	Título: SEXUALIDAD Y FAMILIA. CRISIS Y DESAFIOS FRENTE AL SIGLO XXI	Autor: ANTONIO DONINI Autor: ELEONOR FAUR Autor: ANTONIO DANIEL GARCIA ROJAS Autor: ALEJANDRO VILLA Editor: EDICIONES NOVEDADES EDUCATIVAS DEL CENTRO DE PUBLICACIONES EDUCATIVAS
5118647	Obra Publicada	Género: ENSAYO	Título: DISEÑO DE PROYECTOS DE INVESTIGACION CUALITATIVA.	Autor: ROSA MARIA CIFUENTES GIL Editor: EDICIONES NOVEDADES EDUCATIVAS DEL CENTRO DE PUBLICACIONES EDUCATIVAS
5118648	Obra Publicada	Género: DIDACTICO	Título: EL PLACER DE ENSEÑAR TECNOLOGIA. ACTIVIDADES DE AULA PARA DOCENTES INQUIETOS.	Autor: CARLOS MARIA MARPEGAN Autor: MARIA JOSEFA MANDON Autor: JUAN CARLOS PINTOS Editor: EDICIONES NOVEDADES EDUCATIVAS DEL CENTRO DE PUBLICACIONES EDUCATIVAS
5118649	Obra Publicada	Género: DIDACTICO	Título: EDUCACION FISICA EN EL JARDIN DE INFANTES "EL DIA MAS Lindo"	Autor: ELSA SCARINCI Autor: ANDREA MELLE Editor: EDICIONES NOVEDADES EDUCATIVAS DEL CENTRO DE PUBLICACIONES EDUCATIVAS
5118650	Obra Publicada	Género: DIDACTICO	Título: LOS CHICOS APRENDEN A ESCRIBIR TEXTOS. DESAFIOS Y PROPUESTAS PARA	Autor: VERONICA SANCHEZ ABCHI Autor: BEATRIZ ALICIA MEDRANO Autor: ANA MARIA BORZONE Editor: EDICIONES NOVEDADES EDUCATIVAS DEL CENTRO DE PUBLICACIONES EDUCATIVAS
5118651	Obra Publicada	Género: DIDACTICO	Título: COMO REDACTAR UN PAPER. LA ESCRITURA DE ARTICULOS CIENTIFICOS.	Autor: SILVIA RAMIREZ GELBES Editor: EDICIONES NOVEDADES EDUCATIVAS DEL CENTRO DE PUBLICACIONES EDUCATIVAS
5118652	Obra Publicada	Género: DIDACTICO	Título: CONTACTO NIÑO-ANIMAL. LA CONMOVEDORA EXPERIENCIA DEL LAZO ENTRE ANIMALES Y NIÑOS CON AUTISMO Y OTRAS	Autor: JUAN VASEN Editor: EDICIONES NOVEDADES EDUCATIVAS CENTRO DE PUBLICACIONES EDUCATIVAS Y MA

5118653	Obra Publicada	Género: DIDACTICO	Título: ESTRATEGIAS PARA COMPRENDER Y PRODUCIR ENSAYOS. ANALISIS Y ESCRITURA DE UN GENERO DISCURSIVO	Autor: NORMA MATTEUCCI Editor: EDICIONES NOVEDADES EDUCATIVAS DEL CENTRO DE PUBLICACIONES EDUCATIVAS
5118654	Obra Publicada	Género: DIDACTICO	Título: LECTURAS PARA INVENTAR Y DISFRUTAR. PROYECTOS Y ACTIVIDADES DE MEDIACION LITERARIA.	Autor: MARIA JULIETA SANCHEZ Editor: EDICIONES NOVEDADES EDUCATIVAS DEL CENTRO DE PUBLICACIONES EDUCATIVAS
5118655	Obra Publicada	Género: LITERARIO	Título: EL MAYOR DE MIS DEFECTOS Y OTROS CUENTOS	Autor: ROBERTO FONTANARROSA Autor: FELIPE NOE Editor: GRUPO EDITORIAL PLANETA SAIC
5118656	Obra Publicada	Género: LITERARIO	Título: TE DIGO MAS Y OTROS CUENTOS	Autor: ROBERTO FONTANARROSA Autor: HERMENEGILDO SABAT Editor: GRUPO EDITORIAL PLANETA SAIC
5118657	Obra Publicada	Género: INFANTIL	Título: LA CEBRA QUE SOBRA: POESIAS	Autor: FLORENCIA ESSES Autor: PAIO ZULOAGA Director: ADELA BASCH Editor: EDICIONES ABRAN CANCHA DE ADELA BASCH
5118658	Obra Publicada	Género: HISTORICO	Título: 1983 EL AÑO DE LA DEMOCRACIA	Autor: GERMAN FERRARI Editor: GRUPO EDITORIAL PLANETA SAIC
5118659	Obra Publicada	Género: HISTORICO	Título: HISTORIA Y PASION	Autor: JOSE PABLO FEINMANN Autor: HORACIO GONZALEZ Editor: GRUPO EDITORIAL PLANETA SAIC
5118660	Obra Publicada	Género: LITERARIO	Título: EL CENTRO DEL MUNDO	Autor: ERCOLE LISSARDI Editor: GRUPO EDITORIAL PLANETA SAIC
5118661	Obra Publicada	Género: LITERARIO	Título: ESTERTORES DE UNA DECADA	Autor: MANUEL PUIG Editor: BOOKET DE GRUPO EDITORIAL PLANETA SAIC
5118665	Obra Publicada	Género: INTERES GENERAL	Título: QUEBRADA DE HUMAHUACA, NATURALEZA Y CULTURA	Autor: SANDRA FIGONI PRADO Autor: CHRISTIAN SCHWARZ Autor: KEVIN ZAOUALI Traductor: MARIA PATRICIA ANDRADA Traductor: PILAR LOPEZ Editor: TILCARALLAJTA DE SANDRA FIGONI PRADO
5118666	Obra Publicada	Género: INTERES GENERAL	Título: QUEBRADA DE HUMAHUACA, NATURALEZA Y CULTURA	Autor: SANDRA FIGONI PRADO Autor: CHRISTIAN SCHWARZ Autor: KEVIN ZAOUALI Traductor: MARIA PATRICIA ANDRADA Traductor: PILAR LOPEZ Editor: TILCARALLAJTA DE SANDRA FIGONI PRADO
5118695	Obra Publicada	Género: FONOGRAMA	Título: IDEARIO	Productor: FLAVIO ANDRES ROMERO
5118697	Obra Publicada	Género: ARTISTICO	Título: JOHN LENNON. MIND GAMES	Autor: PAUL DU NOYER Autor: DIEGO MANRIQUE Editor: AGUILAR ALTEA TAURUS ALFAGUARA SA DE EDICIONES
5118698	Obra Publicada	Género: MAPA	Título: GUIAS VISUALES TOP 10-BEIJING	Autor: DORLING KINDERSLEY LIMITED (Q)(DE OBRA ORIGINAL) Editor: AGUILAR ALTEA TAURUS ALFAGUARA SA DE EDICIONES
5118714	Obra Publicada	Género: INTERES GENERAL	Título: INVERTARTE	Autor: LEONARDO EMANUEL ROCCO Editor: SAT INVESTMENT SA
5118759	Obra Publicada	Género: LITERARIO	Título: EL MUNDO SECRETO DE LAS SECTAS	Autor: RISHI SANLON Editor: EDITORIAL ENRIQUE SANTIAGO RUEDA
5118779	Obra Publicada	Género: MUSICA	Título: HOY HE LLEGADO A LA CIUDAD	Autor: NESTOR MIGUEL GONZALEZ Autor: RAUL JORGE ROJAS Editor: PUBLISONG EDICIONES Editor: PUBLITRACK SRL Editor: KRISTOF GROUP DE ARIEL MARCELO NACACHE POLAT
5118780	Obra Publicada	Género: LETRA	Título: HOY HE LLEGADO A LA CIUDAD	Autor: NESTOR MIGUEL GONZALEZ Autor: RAUL JORGE ROJAS Editor: PUBLISONG EDICIONES Editor: PUBLITRACK SRL Editor: KRISTOF GROUP DE ARIEL MARCELO NACACHE POLAT
5118781	Obra Publicada	Género: LETRA	Título: EL SECRETO DE TU VIDA	Autor: NESTOR MIGUEL GONZALEZ Autor: RAUL JORGE ROJAS Editor: PUBLISONG EDICIONES Editor: PUBLITRACK SRL Editor: KRISTOF GROUP DE ARIEL MARCELO NACACHE POLAT
5118782	Obra Publicada	Género: MUSICA	Título: EL SECRETO DE TU VIDA	Autor: NESTOR MIGUEL GONZALEZ Autor: RAUL JORGE ROJAS Editor: PUBLISONG EDICIONES Editor: PUBLITRACK SRL Editor: KRISTOF GROUP DE ARIEL MARCELO NACACHE POLAT
5118783	Obra Publicada	Género: PAGINA WEB	Título: CONOCELAPROVINCIA.COM	Autor/Titular: FABIAN EDUARDO DIAZ
5118788	Obra Publicada	Género: PAGINA WEB	Título: NUEVO CICLO	Autor/Titular: MARIO JOSE BRUNO
5118789	Obra Publicada	Género: PAGINA WEB	Título: BOEDOWEB	Autor/Titular: CLAUDIA ALEJANDRA MARMOL
5118798	Obra Publicada	Género: PAGINA WEB	Título: PAGINA WEB CON ENSEÑANZAS DE LA PALABRA DE DIOS	Autor/Titular: EDUARDO OSCAR DI NOTO
5118824	Obra Publicada	Género: LITERARIO	Título: ¡SEÑOR, QUIERO ESTAR SANO! ¿QUE DEBO HACER?	Autor: ROSALIA SENDEROWICZ DE GALLARDO Editor: ROSALIA SENDEROWICZ
5118841	Obra Publicada	Género: PAGINA WEB	Título: HUMANASVIRTUAL	Autor: OBRA COLECTIVA Autor/Titular: UNIVERSIDAD NACIONAL DEL CENTRO - FACULTAD DE CIENCIAS HUMANAS (Q)
5118842	Obra Publicada	Género: TECNICO	Título: LA ARGENTINA, GEOGRAFIA ECONOMICA Y HUMANA	Autor: ISIDRO J. F. CARLEVARI Autor: RICARDO D. CARLEVARI Editor: ALFAOMEGA GRUPO EDITOR ARGENTINO SA
5118843	Obra Publicada	Género: JURIDICO	Título: DICCIONARIO DE CIENCIAS JURIDICAS, POLITICAS, SOCIALES Y DE ECONOMIA	Autor: OBRA COLECTIVA Director: VICTOR DE SANTO Editor: 20XII GRUPO EDITORIAL DE ALFREDO RAMON TESEIRA FERREIRA
5118848	Obra Publicada	Género: PROGRAMA COMPUTACION	Título: EL ULTIMO HOMBRE "EUH"	Autor/Titular: DANIEL ALBERTO DAZA ARIAS
5118849	Obra Publicada	Género: PAGINA WEB	Título: EL ULTIMO HOMBRE "EUH"	Autor/Titular: DANIEL ALBERTO DAZA ARIAS
5118850	Obra Publicada	Género: FONOGRAMA	Título: TIENE QUE SER ASI	Productor: CRISTIAN DAMIAN LOPEZ
5118887	Obra Publicada	Género: LITERARIO	Título: EXTRAÑAS COSAS QUE LE PASAN A LOS HOMBRES	Autor: EMILIANO GONZALO RODRIGUEZ Editor: ESPEJO TRECE DE RODRIGUEZ EMILIANO GONZALO

ADMINISTRACION FEDERAL DE INGRESOS PUBLICOS**DIRECCION GENERAL DE ADUANAS****DIVISION ADUANA DE POSADAS****Código Aduanero - Ley 22.415 - Artículo 1112 inc. a).**

Por ignorarse los domicilios se notifica a las personas que más abajo se mencionan, que en las actuaciones tramitadas por ante esta dependencia en las que se encuentran involucradas como imputados, han recaído Fallos de condena al pago de las multas referidas supra y/o al comiso —en caso de corresponder art. 864-947-977-985-986-987 del C.A.— de las mercaderías oportunamente secuestradas, por la comisión de la infracción mencionada para cada caso, intimándose al pago de la multa impuesta dentro del plazo de quince (15) días bajo apercibimiento del procedimiento de ejecución establecido por el art. 1122 y sgtes. del citado texto legal, registrándose el antecedente infraccional correspondiente. Asimismo se les hace saber que contra el referido Fallo podrán interponer Demanda Contenciosa y/o Recurso de Apelación ante la Justicia Federal y/o Tribunal Fiscal de la Nación respectivamente en el plazo mencionado (art. 1132 y 1133 C.A.).

SC 46-	IMPUTADO	DOCUMENTO	FALLO N°	ART.	MULTA
884/02	MORAND JUAN DOMINGO	DNI:12.264.928	834/09	864	81457,20
288/06	PICAGUA BENITEZ FELIPE	CIP: 680.757	47/10	864	10695764,76
175/10	SANCHEZ RICARDO RUBEN	DNI: 24.828.363	168/13	986/7	3438,89
364/10	GONZALEZ GABRIEL	DNI: 35.838.628	107/13	985	61422,55
329/10	GAUTO RUDI WALDEMAR	DNI: 33.074.690	136/13	985	133549,2
352/10	ESCOBAR PABLO HERNAN	DNI: 31.874.328	108/13	985	94475,4
156/10	MERELE LUIS ALBERTO	DNI: 29.658.854	74/13	985	27196,66
155/10	HEIN NELSON HUGO	DNI: 21.814.222	75/13	985	139576,35
179/10	VIVAS ARIEL OSCAR	DNI: 27.847.224	039/13	985	113524,55
180/10	VIVAS ARIEL OSCAR	DNI: 27.847.224	036/13	985	146159
43/10	MOREL HECTOR GABRIEL	DNI: 25.519.306	126/13	986/7	3522,86
147/10	GAUTO RUDI WALDEMAR	DNI: 33.074.690	072/13	985	70023,3
153/10	GONZALEZ GABRIEL	DNI: 35.838.628	032/13	985	113438,40
363/10	MOREL HILDA ROSA	DNI: 24.880.528	109/13	985	25938,67
65/10	VEGA MARISABEL	DNI: 30.644.012	212/13	986/7	3117,56
226/11	CASCO JUAN	CIP: 1.426.586	289/13	977	7722,11
128/11	SANTA CRUZ VILLALBA MARTHA	CIP: 706.271	287/13	977	27570,15
228/11	TORRES BARRIOS JOSE	CIP: 2.672.249	262/13	977	4608,68
225/11	HOLZ JAMES LEANDRO	CIBR: 7041534517	250/13	977	4514,40
94/12-5	VILLALBA CHRISTIAN ALEJANDRO	CIP: 4.582.830	255/13	985	26682,36
391/10	GONZALEZ GRACIELA	DNI: 18.027.729	038/13	985	15004,90
389/10	GONZALEZ HECTOR LUIS	DNI: 29.356.538	030/13	985	122944,15
374/10	LEAL RUBEN	DNI: 29.830.068	035/13	985	23562,66
289/10	SILVEIRA CLAUDIO ANDRES	DNI: 30.903.954	028/13	985	84764,37
336/08	ENRIQUES GUILLERMO FABIAN	DNI: 18.559.355	124/13	986/7	10800,90
405/09	FERNANDEZ VILLALBA ALCIDEZ	DNI: 24.248.822	727/12	947	49084,26
146/10	GAUTO RUDI WALDEMAR	DNI: 33.074.690	85/13	985	141759,70
120/08	MESCHER MIGUEL ANGEL	DNI: 18.480.236	170/13	987	8728,77
404/10	GONZALEZ ALEJANDRO ANDRES	DNI: 92.886.224	169/13	986/7	3391,97
344/08	HEIN NELSON HUGO	DNI: 21.814.222	398/10	985	70179,33
154/10	HEIN NELSON HUGO	DNI: 21.814.222	83/13	985	75044,05
148/10	AGHELIN VICTOR MIGUEL	DNI: 27.047.748	82/13	985	75425,70
451/09	BELLO FLORENTINO CIPRIANO	DNI: 11.629.003	487/10	986/7	4908,35
176/11	RYNAS ELISEO GUSTAVO	DNI: 29.612.145	493/12	985	2053,85
317/10	HEIN NELSON HUGO	DNI: 21.814.222	125/13	985	62612,10
432/10	FLORINDO JORGE ALFREDO	DNI: 10.000.196	187/13	977	3087,39
426/10	SILVA ALBERTO CARLOS	DNI: 14.540.632	565/12	986/7	8108,02
256/12	GAUNA SERGIO DANIEL	DNI: 23.349.820	221/13	985	14132,30
85/12-5	CARVALLO OSCAR RAUL	DNI: 32.040.163	197/13	985	17135,12
69/12-1	KOZACHIK DARIO HERNAN	DNI: 27.398.268	222/13	985	5516,90
244/11	ACOSTA DARIO ALBERTO	DNI: 22.613.504	213/13	986/7	2715,38
303/10	GONZALEZ VICTOR HUGO	DNI: 32.375.502	135/13	985	123637,15
181/10	MONTES JUAN HUMBERTO	DNI: 11.154.109	127/13	986/7	10151,23
77/12	MARTINEZ VILLALBA EUSTANCIANA	DNI: 92.751.021	205/13	987	9474,03
68/10	ROMERA GABRIEL AGUSTIN	DNI: 22.613.504	098/13	986/7	9506,14
129/11-3	CABRAL ANIBAL	DNI: 27.675.269	468/12	985	2021,44
100/11-8	CACERES VICTOR MANUEL	DNI: 14.943.303	551/12	985	3414,67
136/10	BARRETO SERGIO RAMON	DNI: 22.642.859	43/13	985	117950,45
330/10	GAUTO RUDI WALDEMAR	DNI: 33.074.690	120/13	985	61597,75
463/09	GARCIA PABLO JAVIER	DNI: 22.899.236	486/10	986/7	18295,12
218/11	PERCIS ROJA ARIBERTO	DNI: 24.748.598	150/13	986/7	18304,22
15/10	AYALA RAMON ERNESTO	DNI: 18.618.806	105/13	986	31323,95
316/10	GAUTO RUDI WALDEMAR	DNI: 33.074.690	121/13	985	124064,00

Ab. FEDERICO M. SCHEWZOW, Firma Responsable, División Aduana de Posadas.
e. 02/09/2013 N° 66423/13 v. 02/09/2013

ADMINISTRACION FEDERAL DE INGRESOS PUBLICOS**DIRECCION GENERAL DE ADUANAS****DIRECCION REGIONAL ADUANERA SALTA****DIVISION ADUANA DE JUJUY**

Se notifica en los términos del Art. 1013 inc. h) del C.A. a los imputados, de la Apertura y Corrida de Vista de los Sumarios Contenciosos en trámite por ante esta Aduana, sito en calle Senador Pérez N° 531 2do. Piso, S.S.de Jujuy, para que en el plazo de diez (10) días hábiles de notificados, más los que les correspondan en razón de la distancia (Art. 1036 del C.A.), comparezcan a los efectos de evacuar defensa y ofrecer pruebas bajo apercibimiento de rebeldía (Art. 1001 al 1005 C.A.). Dentro del mismo plazo el supuesto responsable podrá impugnar las actuaciones sumariales cumplidas, con fundamentos en los defectos de forma de que adolecieren, no pudiendo hacerlo en lo sucesivo conforme el art. 1104 del C.A. De igual manera se les hace saber que en la primera presentación deberán constituir domicilio dentro del radio urbano de esta ciudad, conforme lo prescripto por los art. 1001 al 1003 del C.A., bajo apercibimiento de proceder conforme lo establecido en los Arts. 1006 al 1010 del C.A. El que concurriere en su representación deberá acreditar personería jurídica conforme lo establecido por el Art. 10130 y ss. del Código Aduanero. En caso de que se planteen o debatan cuestiones jurídicas será obligatorio el patrocinio letrado conforme art. 1034 del C.A. Por último se les hace saber que si en ese plazo depositan el mínimo de la multa se extinguirá la acción penal y no se registrarán antecedentes, de conformidad a lo dispuesto en el Art. 930 de la Ley 22.415.

SUMARIO	IMPUTADO	DNI	ART. C.A.	MULTA MINIMA
031SC-754-2012/5	MEDINA, Gerardo Cesar	12.567.559	970	\$143.325,00
031SC-770-2012/9	ZAINA, Patricio	26.945.758	970	\$48.930,00
031SC-774-2012/1	PANTOJA, Valeria Elizabeth	26.030.315	986/987	\$2.003,11
031SC-775-2012/k	PACO, Sandra Marisa	24.613.066	986	\$5.147,69
031SC-775-2012/k	QUINTEROS, Jairo Emanuel	35.896.832	986	\$5.147,69
031SC-775-2012/k	MAMANI, Ricardo Daniel	26.582.213	986/987	\$5.147,69
031SC-144-2013/0	CARLOS, Walter Alejandro	20.805.369	986/987	\$13.320,50
031SC-244-2013/4	PUCA, Norma	35.826.768	986/987	\$2.581,13
031SC-378-2013/k	ORTEGA, Orlando	18.793.895	987	\$19.500,04
031SC-380-2013/2	SOLIZ SERRUDO, Tito	93.696.003	987	\$16.075,08
031SC-381-2013/0	LOPEZ GARCIA, Manuel	93.275.609	987	\$3.348,96
031SC-383-2013/7	ACHACOLLO CRUZ, Julia	93.938.999	986/987	\$54.583,30
031SC-384-2013/5	RAMOS QUISPE, Ventura	92.947.781	987	\$4.430,47
031SC-389-2013/1	VILTE, Ricardo Alejandro	26.175.303	986/987	\$4.152,23
031SC-391-2013/9	RAMOS, Rosana Miriam	34.009.602	987	\$4.484,25
031SC-393-2013/5	QUISPE, Cristian Rubén	31.268.685	987	\$2.492,82
031SC-442-2013/4	QUISPE LOPEZ, Hilda Viviana	18.807.110	986/987	\$2.072,00
031SC-453-2012/2	MAIDANA, Carmen Yolanda	17.355.379	986/987	\$10.060,68

JAVIER BACH, Administrador, División Aduana de Jujuy.
e. 02/09/2013 N° 67226/13 v. 02/09/2013

ADMINISTRACION FEDERAL DE INGRESOS PUBLICOS

22/8/2013

La Administración Federal de Ingresos Públicos cita por diez (10) días a parientes del exagente fallecido Darío Javier LOUREIRO (D.N.I. N° 21.066.044), alcanzados por el beneficio establecido en el artículo 173 del Convenio Colectivo de Trabajo N° 56/92 "E" Laudo N° 16/92 (T.O. Resolución S.T. N° 924/10), para que dentro de dicho término se presenten a hacer valer sus derechos en Hipólito Yrigoyen N° 370, 5° Piso, Oficina N° 5648, Ciudad Autónoma de Buenos Aires. — Lic. CECILIA G. SILVESTRO, Jefa (Int.), Sección Jubilaciones - División Beneficios.

NOTA: La publicación deberá efectuarse por tres (3) días hábiles consecutivos.
e. 02/09/2013 N° 66266/13 v. 04/09/2013

ADMINISTRACION FEDERAL DE INGRESOS PUBLICOS**DIRECCION DE ANALISIS DE FISCALIZACION ESPECIALIZADA****RESOLUCION GENERAL N° 2300 - TITULO II**

REGISTRO FISCAL DE OPERADORES EN LA COMPRAVENTA DE GRANOS Y LEGUMBRES SECAS.

"La resolución administrativa de exclusión se encuentra disponible en el servicio "Registro Fiscal de Operadores de Granos" de la página web institucional (www.afip.gov.ar) al que se accede mediante Clave Fiscal, así como en el expediente administrativo obrante en la dependencia de este Organismo en la cual cada responsable se encuentra inscripto, excepto para las exclusiones previstas en los incisos a), c), d) y f) del artículo 47".

Exclusión Productor		
CUIT	APELLIDO Y NOMBRE, DENOMINACION O RAZON SOCIAL	NORMA
20062743094	CHINELLATO ELIODORO SANTIAGO	Art: 40 Inciso/s: b)-An. VI B) 8.
20076840238	CARNEVALE CARLOS ROMAN	Art: 40 Inciso/s: b)-An. VI B) 8.
20077733036	ROUBAKHINE ERNESTO JUAN	Art: 40 Inciso/s: b)-An. VI B) 8.
20080028769	GALLO ALBERTO PABLO	Art: 40 Inciso/s: b)-An. VI B) 8.
20108584220	SUCESION DE CIANCAGLINI	Art: 40 Inciso/s: b)-An. VI B) 8.
20119681104	GUITART JORGE ANSELMO	Art: 40 Inciso/s: b)-An. VI B) 8.
20131720123	MENZELLA MIGUEL ANGEL	Art: 40 Inciso/s: b)-An. VI B) 8.
20134224976	PRIETO JOSE LUIS	Art: 40 Inciso/s: b)-An. VI B) 8.
20161023486	ARRACHEA PABLO ENRIQUE	Art: 40 Inciso/s: b)-An. VI B) 8.
20164388582	SPEIER MARCOS MAXIMO	Art: 40 Inciso/s: b)-An. VI B) 8.
20182607550	LOPEZ DE ARMENTIA ESTEBAN	Art: 40 Inciso/s: b) An. VI B) 8.
20208308131	TRAVERSA JOSE MARIA	Art: 40 Inciso/s: b)-An. VI B) 8.
20216037481	ANDRES JAVIER ERNESTO	Art: 40 Inciso/s: b)-An. VI B) 8.
20217858659	SPERONI SILVIO GASTON	Art: 40 Inciso/s: b)-An. VI B) 8.
20218435182	ALVAREZ ARIEL HERNAN	Art: 40 Inciso/s: b)-An. VI B) 8.
20234377516	ACTIS FACUNDO HERNAN	Art: 40 Inciso/s: b)-An. VI B) 8.
20253560690	BALLINI GUILLERMO ARIEL	Art: 40 Inciso/s: b)-An. VI B) 8.
20276233050	GIOVAGNOLA GUILLERMO RODOLFO	Art: 40 Inciso/s: b)-An. VI B) 8.
20293639079	MARTORELLI ESTEBAN ALEJANDRO	Art: 40 Inciso/s: b)-An. VI B) 8.

20297548310	RASPI MATIAS EDUARDO	Art: 40 Inciso/s: b) An. VI B.8
23062377429	WEBER LILIANO	Art: 40 Inciso/s: b)-An. VI B) 8.
23239280994	GUIDONI MARIELA VERONICA	Art: 40 Incisb/s: b)-An. VI B) 8.
24140571160	ROSSI HECTOR ANTONIO	Art: 40 Incisb/s: b)-An. VI B) 8.
27115349444	PICCHI MARIA MARGARITA	Art: 40 Incisb/s: b)-An. VI B) 8.
27136101604	GIECO ADRIANA ELSA	Art: 40 Incisb/s: b)-An. VI B) 8.
27277670297	MUSCOLO MARINA	Art: 40 Incisb/s: b)-An. VI B) 8.
27290763822	MONTES MARIA AGUSTINA	Art: 40 Inciso/s: b)-An. VI B) 8.
30685490680	GHERBEZZA EDUARDO F Y MORI RAUL A	Art: 40 Incisb/s: b)-An. VI B) 8.
30707241728	SEVEN HEADS SA	Art: 40 Incisb/s: b)-An. VI B) 8.
30708178159	LARRALDE ERNESTO DANIEL Y FALOTICO JORGE LUIS	Art: 40 Incisb/s: b)-An. VI B) 8.
30708400099	RASE S.A	Art: 40 Incisb/s: b)-An. VI B) 8.
30708880848	INSERVICES S.A.	Art: 40 Incisb/s: b)-An. VI B) 8.
30708968044	SERGRAN S.R.L	Art: 40 Inciso/s: b)-An. VI B) 8.
30709659134	LA SUERTE S.H. DE PERALTA, ANA CARINA Y KRAUEL, PABLO OSCAR	Art: 40 Incisb/s: b)-An. VI B) 8.
30710754906	EL AURA S.R.L.	Art: 40 Inciso/s: b)-An. VI B) 8.
30711400784	RECA AGRO SOCIEDAD DE HECHO DE OSVALDO RECA Y SANTIAGO RECA	Art: 40 Inciso/s: b) An. VI B.8
30711407002	EL VISTAZO S.R.L.	Art: 40 Inciso/s: b) An. VI B.8
30711910324	FIDECAMPO	Art: 40 Inciso/s: b)-An. VI B) 8.

Exclusión Acopiador

CUIT	APELLIDO Y NOMBRE, DENOMINACION O RAZON SOCIAL	NORMA
30658337595	EUSKA S.A.	Art: 40 Inciso/s: b)-An. VI B) 13.
30709094765	ACONDICIONAR SA	Art: 40 Inciso/s: b)-An. VI B) 16.

Cont. Púb. ALFREDO R. SAMPERI, Director (Int.), Dirección de Análisis de Fiscalización Especializada.

e. 02/09/2013 N° 67514/13 v. 02/09/2013

ADMINISTRACION FEDERAL DE INGRESOS PUBLICOS

DIRECCION DE ANALISIS DE FISCALIZACION ESPECIALIZADA

RESOLUCION GENERAL N° 2300 - TITULO II

REGISTRO FISCAL DE OPERADORES EN LA COMPRAVENTA DE GRANOS Y LEGUMBRES SECAS

Suspensión Productor

CUIT	APELLIDO Y NOMBRE, DENOMINACION O RAZON SOCIAL	NORMA
20044433967	PEREYRA LUCENA JAVIER	Art: 40 Inciso/s: b)-An. VI B) 1.
20050487270	SUCESION DE FERNANDEZ ELOY	Art: 40 Inciso/s: b)-An. VI B) 8.
20104560645	ZANTEDESCHI OMAR RAMON	Art: 40 Inciso/s: b) - An. VI B.13
20124011419	ELISSONDO LUCIANO	Art: 40 Inciso/s: b)-An. VI B) 1.

ADMINISTRACION FEDERAL DE INGRESOS PUBLICOS

DIRECCION DE FISCALIZACION DE EXPORTACION

Listado de Preajustes de valor aplicables de conformidad al Art. 748 inc. C) del C.A.

P.A. SIM. 3826.00.00.100L

MERCADERIA: BIODISEL

EXPORTADOR: OLEAGINOSA MORENO HNOS C.U.I.T. 33-50223222-9, DESPACHANTE: FANJUL ALICIA VICTORIA C.U.I.T. 27-05701189-6

DESTINACION	ITEM	PAIS	FOB DECLARADO	B.I. DECLARADA	B.I. AJUSTADA	% AJUSTE	DIFERENCIA US\$
12057EC01009275R	1 - 0	ESPAÑA	1.051.820,00	850.775,13	873.568,80	2,68%	5.386,15
12057EC01009276S	1 - 0	ESPAÑA	1.059.760,00	857.197,47	873.568,80	1,91%	3.868,54
12057EC01009277T	1 - 0	ESPAÑA	5.141.150,00	4.158.496,29	4.367.871,00	5,03%	49.475,24
12057EC01009278U	1 - 0	PAISES BAJOS	1.050.500,00	849.712,68	873.574,20	2,81%	5.638,48

20126310448	SOSA RODOLFO URBANO	Art: 40 Inciso/s: b)-An. VI B) 8.
20139035128	JACA ADRIAN DANTE	Art: 40 Inciso/s: b)-An. VI B) 8.
20163375290	MARDARAS FEDERICO VICTOR	Art: 40 Inciso/s: b) - An. VI B.13
20179854032	RAMPOLDI DANIEL OSVALDO	Art: 40 Inciso/s: b)-An. VI B) 8.
20181110261	SCORTECHINI SERGIO MARCELO	Art: 40 Inciso/s: b)-An. VI B) 8.
20219676108	BELLINI JOSE DOMINGO	Art: 40 Inciso/s: b)-An. VI B) 8.
20225936537	DHO ALEJANDRO JOSE	Art: 40 Inciso/s: b)-An. VI B) 8.
20271806311	BAR FEDERICO ALBINO	Art: 40 inc. b) -- Anexo VI b) 8.
20288956589	ROCCO HERNANDO ANDRES	Art: 40 Inciso/s: b)-An. VI B) 8.
20327035100	CARROZZA LEONARDO	Art: 40 Inciso/s: b)-An. VI B) 8.
20339413364	PELAYO CRISTIAN EMANUEL	Art: 40 Inciso/s: b)-An. VI B) 5.
23115689339	MARTINEZ OSCAR ALFREDO	Art: 40 Inciso/s: b) - An. VI B.13
23937000359	CREA FRANCISCO SALVADOR	Art: 40 Inciso/s: b) An. VI B.8
27249398212	LIBANO ANALIA ROXANA	Art: 40 Inciso/s: b)-An. VI B) 5.
30554517095	RESCHINI ABEL RUFINO Y JUAN CARLOS S.R.L.	Art: 40 inc. b) -- Anexo VI b) 8.
30613784981	TIMAJU S R L	Art: 40 Inciso/s: b) An. VI B.8
30707017216	CHUMILLO RUBEN CHUMILO CLAUDIO CHUMILO HERNAN CHUMILO DIEGO	Art: 40 Inciso/s: b)-An. VI B) 8.
30708298383	CONDE, PERLA ROSA Y BODDA, ROSA SOC. DE HECHO	Art: 40 Inciso/s: b)-An. VI B) 8.
30708320133	TESTA COMBUSTIBLES SRL	Art: 40 Inciso/s: b) An. VI B.8
30708691395	SALTPER SRL	Art: 40 Inciso/s: b) An. VI B.8
30709181412	AGROPECUARIA SAN GIMINIANO SOCIEDAD ANONIMA	Art: 40 Inciso/s: b)-An. VI B) 8.
30709339253	FAVARO, MARCELA-FAVARO, MARIO Y HERRERA, MATÍAS S. DE HECHO	Art: 40 Inciso/s: b)-An. VI B) 8.
30709715638	MARABU S.R.L.	Art: 40 Inciso/s: b) An. VI B.8
30709882933	MARINI HNOS. SOC. DE HECHO	Art: 40 Inciso/s: b)-An. VI B) 8.
30710172338	"AGRO ACTIVO S.A."	Art: 40 Inciso/s: b)-An. VI B) 8.
30710220839	FIDEICOMISO AGRICOLA UBAJAY	Art: 40 Inciso/s: b)-An. VI B) 5.
30710227280	ESTABLECIMIENTO SAN PATRICIO S.A.	Art: 40 Inciso/s: b)-An. VI B) 8.
30710562942	AGROCOMODITIES SA	Art: 40 Inciso/s: b)-An. VI B) 8.
30710756852	LAS CUATRO PUERTAS S.R.L.	Art: 40 Inciso/s: b) - An. VI B.13
30711018014	ALASIA, ALDO JAVIER - BELICH, FABIAN ANIBAL Y DRAGONETTI, AL	Art: 40 Inciso/s: b)-An. VI B) 8.
30711505918	AGRO 25 S.R.L.	Art: 40 Inciso/s: b)-An. VI B) 8.

Suspensión Acopiador

CUIT	APELLIDO Y NOMBRE, DENOMINACION O RAZON SOCIAL	NORMA
30711626588	AGRO CONSTITUCION S.R.L	Art: 40 Inciso/s: b)-An. VI B) 3., b)-An. VI B) 12., b)-An. VI B) 4., b)-An. VI B) 16.
33666352799	AGROPECUARIA MAREN SOCIEDAD ANONIMA	Art: 40 Inciso/s: b)-An. VI B) 5.

Cont. Púb. ALFREDO R. SAMPERI, Director (Int.), Dirección de Análisis de Fiscalización Especializada.

e. 02/09/2013 N° 67516/13 v. 02/09/2013

DESTINACION	ITEM	PAIS	FOB DECLARADO	B.I. DECLARADA	B.I. AJUSTADA	% AJUSTE	DIFERENCIA US\$
12057EC01009429S	1 - 0	ESPAÑA	449.650,00	363.706,15	371.269,04	2,08%	1.787,11
12057EC01010056G	1 - 0	ESPAÑA	529.660,00	428.423,44	436.787,10	1,95%	1.976,33
12057EC01010329J	1 - 0	ESPAÑA	5.286.700,00	4.276.253,03	4.367.898,00	2,14%	21.655,71
12057EC03001881Y	1 - 0	PERU	812.575,35	647.812,25	658.832,75	1,70%	2.604,14
12057EC03001894S	1 - 0	PERU	4.248.760,00	3.387.253,60	3.444.877,14	1,70%	13.616,44
12057EC03002006E	1 - 0	ESPAÑA	5.296.600,00	4.227.739,39	4.311.376,03	1,98%	19.763,34
12057EC03002009H	1 - 0	ESPAÑA	1.588.980,00	1.267.227,59	1.292.318,58	1,98%	5.929,00
12057EC03002021B	1 - 0	ESPAÑA	4.968.100,00	3.963.036,08	4.312.384,88	8,82%	82.551,12
12057EC03002118X	1 - 0	PERU	1.411.948,13	1.127.263,15	1.131.753,86	0,40%	1.061,16

P.A. SIM. 3826.00.00.100L

MERCADERIA: BIODISEL

EXPORTADOR: ACEITERA GENERAL DEHEZA C.U.I.T. 30-50287435-5, DESPACHANTE ANGEL GUSTAVO MIGUEL, C.U.I.T. 20-13238476-3

DESTINACION	ITEM	DESTINO	FOB DECLARADO	B.I. DECLARADA	B.I. AJUSTADA	% AJUSTE	DIFERENCIA US\$
12057EC03001756P	1 - 0	PERU	9.425.062,50	7.516.359,04	7.551.817,44	0,47%	8.378,82

P.A. SIM. 3826.00.00.100L

MERCADERIA: BIODISEL

EXPORTADOR: VICENTIN S.A., C.U.I.T. 30-50095962-9, DESPACHANTE: FANJUL ALICIA VICTORIA C.U.I.T. 27-05701189-6

DESTINACION	ITEM	DESTINO	FOB DECLARADO	B.I. DECLARADA	B.I. AJUSTADA	% AJUSTE	DIFERENCIA US\$
12057EC01010377M	1 - 0	ESPAÑA	571.649,19	462.387,02	496.522,10	7,38%	8.066,12
12057EC01010379Y	1 - 0	ESPAÑA	2.514.375,00	2.033.789,93	2.183.935,50	7,38%	35.479,40
12057EC01010380G	1 - 0	ESPAÑA	3.515.498,00	2.843.563,29	2.970.152,28	4,45%	29.912,98
12057EC01010381H	1 - 0	ESPAÑA	1.654.352,00	1.338.147,43	1.397.718,72	4,45%	14.076,70
12057EC03001768S	1 - 0	PAISES BAJOS	1.035.070,00	825.323,83	861.666,14	4,40%	8.587,69
12057EC03001769T	1 - 0	ESPAÑA	1.640.095,36	1.252.251,26	1.293.809,96	3,32%	9.820,32
12057EC03001771M	1 - 0	ESPAÑA	7.784.614,63	6.214.207,61	6.411.489,92	3,17%	46.617,81
12057EC03001772N	1 - 0	ESPAÑA	1.035.070,00	826.134,67	862.476,98	4,40%	8.587,69
12057EC03001793Z	1 - 0	ESPAÑA	6.194.520,00	4.936.404,58	5.167.319,36	4,68%	54.565,16
12057EC03001899A	1 - 0	PERU	5.061.335,35	4.040.954,28	4.109.598,33	1,70%	16.220,59
12057EC03002022C	1 - 0	ESPAÑA	1.987.240,00	1.585.214,43	1.724.953,95	8,82%	33.020,45
12057EC03002056J	1 - 0	ESPAÑA	1.942.725,81	1.549.967,30	1.665.977,79	7,48%	27.413,28

Cont. Púb. GABRIEL E. BALLARINO, Director (Int.), Dirección de Fiscalización de Exportación.

e. 02/09/2013 N° 67552/13 v. 02/09/2013

ADMINISTRACION FEDERAL DE INGRESOS PUBLICOS**DIRECCION DE FISCALIZACION DE EXPORTACION****Listado de Preajustes de Valor aplicables de conformidad al Art. 748 inc. c) del C.A.**

P.A. SIM. 3826.00.00.100L

MERCADERIA: BIODISEL

EXPORTADOR: MOLINOS RIO DE LA PLATA C.U.I.T. 30-50085862-8, DESPACHANTE: PELLICCIOTTI GAZZANIGA C.U.I.T. 27-11271797-3

DESTINACION	ITEM	PAIS	FOB DECLARADO	B.I. DECLARADA	B.I. AJUSTADA	% AJUSTE	DIFERENCIA US\$
12057EC03001732J	1 - 0	ESPAÑA	1.065.000,00	850.143,28	862.276,27	1,43%	2.867,03
12057EC03001733K	1 - 0	ESPAÑA	2.080.000,00	1.659.843,26	1.724.552,54	3,90%	15.290,80
12057EC03001735M	1 - 0	PAISES BAJOS	709.290,00	566.168,55	574.249,12	1,43%	1.909,44
12057EC03001747P	1 - 0	ESPAÑA	1.196.000,00	952.814,37	990.022,20	3,91%	8.792,21
12057EC03001750J	1 - 0	PAISES BAJOS	884.000,00	703.864,30	731.365,74	3,91%	6.498,59
12057EC03001795S	1 - 0	PAISES BAJOS	379.204,80	300.440,70	312.237,85	3,93%	2.787,67
12057EC03001796T	1 - 0	PAISES BAJOS	478.795,20	361.322,81	376.218,24	4,12%	3.519,79
12057EC03001834M	1 - 0	ESPAÑA	449.650,00	358.012,99	365.575,89	2,11%	1.787,11
12057EC03001877T	1 - 0	PERU	5.061.335,35	4.040.901,48	4.109.545,61	1,70%	16.220,61
12057EC03002032D	1 - 0	ESPAÑA	1.569.465,00	1.252.841,02	1.293.717,06	3,26%	9.659,01
12057EC03002033E	1 - 0	ESPAÑA	1.046.310,00	832.927,86	860.178,56	3,27%	6.439,34
12057EC03002084K	1 - 0	PERU	2.787.750,00	2.225.785,94	2.264.004,86	1,72%	9.031,13

Cont. Púb. GABRIEL E. BALLARINO, Director (Int.), Dirección de Fiscalización de Exportación.

e. 02/09/2013 N° 67553/13 v. 02/09/2013

ADMINISTRACION FEDERAL DE INGRESOS PUBLICOS**DIRECCION DE FISCALIZACION DE EXPORTACION****Listado de Preajustes de valor aplicables de conformidad al Art. 748 inc. C) del C.A.**

P.A. SIM. 3826.00.00.100L

MERCADERIA: BIODISEL

EXPORTADOR: MOLINOS RIO DE LA PLATA - C.U.I.T. 30-50085862-8 - DESPACHANTE: PELLICCIOTTI GAZZANIGA - C.U.I.T. 27-11271797-3

DESTINACION	ITEM	PAIS	FOB DECLARADO	B.I. DECLARADA	B.I. AJUSTADA	% AJUSTE	DIFERENCIA US\$
12057EC03001267M	1 - 0	PAISES BAJOS	2.074.000,00	1.705.599,25	1.827.265,43	7,13%	24.333,24
12057EC03001268N	1 - 0	PAISES BAJOS	1.055.180,00	867.949,56	913.632,71	5,26%	9.136,63
12057EC03001270G	1 - 0	PAISES BAJOS	1.555.500,00	1.279.199,44	1.370.449,08	7,13%	18.249,93

DESTINACION	ITEM	PAIS	FOB DECLARADO	B.I. DECLARADA	B.I. AJUSTADA	% AJUSTE	DIFERENCIA US\$
12057EC03001306G	1 - 0	PERU	1.899.324,00	1.554.335,89	1.636.565,56	5,29%	16.445,93
12057EC03001307H	1 - 0	PERU	1.420.724,73	1.168.784,88	1.217.872,41	4,20%	9.817,51
12057EC03001308X	1 - 0	PERU	2.156.400,00	1.774.265,64	1.827.265,43	2,99%	10.599,96
12057EC03001309J	1 - 0	PERU	1.911.756,55	1.572.476,45	1.660.070,64	5,57%	17.518,84
12057EC03001310B	1 - 0	PERU	3.305.600,00	2.713.951,81	2.919.284,32	7,57%	41.066,50
12057EC03001311C	1 - 0	PERU	516.500,00	424.054,97	456.138,18	7,57%	6.416,64
12057EC03001328K	1 - 0	PAISES BAJOS	1.776.705,27	1.461.638,71	1.523.025,74	4,20%	12.277,41
12057EC03001331E	1 - 0	PAISES BAJOS	345.321,00	283.982,27	304.239,69	7,13%	4.051,48
12057EC03001344X	1 - 0	ESPAÑA	2.110.360,00	1.723.172,17	1.814.538,48	5,30%	18.273,26
12057EC03001345J	1 - 0	ESPAÑA	2.110.360,00	1.726.158,92	1.817.525,22	5,29%	18.273,26
12057EC03001348M	1 - 0	ESPAÑA	2.321.396,00	1.908.787,83	2.009.290,76	5,27%	20.100,59
12057EC03001365L	1 - 0	PAISES BAJOS	1.728.679,00	1.410.970,38	1.512.379,14	7,19%	20.281,75
12057EC03001375M	1 - 0	ESPAÑA	647.035,20	531.340,55	563.239,42	6,00%	6.379,77
12057EC03001390J	1 - 0	ESPAÑA	646.800,00	530.716,70	546.716,64	3,01%	3.199,99
12057EC03001391K	1 - 0	ESPAÑA	1.161.836,00	953.317,51	982.057,98	3,01%	5.748,09
12057EC03001392L	1 - 0	DINAMARCA	347.363,94	285.021,40	293.614,17	3,01%	1.718,55
12057EC03001393M	1 - 0	ESPAÑA	539.000,00	443.323,71	456.656,99	3,01%	2.666,66
12057EC03001394N	1 - 0	ESPAÑA	1.078.000,00	886.647,42	913.313,98	3,01%	5.333,31
12057EC03001395Y	1 - 0	ESPAÑA	2.156.000,00	1.773.667,58	1.827.000,70	3,01%	10.666,62
12057EC03001396P	1 - 0	ESPAÑA	1.078.000,00	886.647,42	913.313,98	3,01%	5.333,31
12057EC03001403E	1 - 0	ESPAÑA	2.048.597,50	1.685.545,47	1.689.630,87	0,24%	817,08
12057EC03001404F	1 - 0	ESPAÑA	34.720,95	28.548,49	30.139,36	5,57%	318,17
12057EC03001405G	1 - 0	ESPAÑA	1.101.090,00	905.889,01	913.313,98	0,82%	1.484,99
12057EC03001406H	1 - 0	ESPAÑA	660.654,00	543.533,41	547.988,39	0,82%	891,00
12057EC03001407X	1 - 0	ESPAÑA	1.186.721,77	976.340,00	984.342,41	0,82%	1.600,48
12057EC03001409K	1 - 0	ESPAÑA	354.804,23	291.904,62	294.297,16	0,82%	478,51
12057EC03001410C	1 - 0	ESPAÑA	349.753,23	285.546,13	302.110,04	5,80%	3.312,78
12057EC03001411D	1 - 0	ESPAÑA	630.186,00	518.143,51	547.988,39	5,76%	5.968,98
12057EC03001412E	1 - 0	ESPAÑA	735.217,00	600.247,12	635.066,15	5,80%	6.963,81
12057EC03001413F	1 - 0	ESPAÑA	700.556,77	572.759,88	605.937,43	5,79%	6.635,51
12057EC03001414G	1 - 0	ESPAÑA	420.124,00	345.429,01	365.325,60	5,76%	3.979,32
12057EC03001415H	1 - 0	ESPAÑA	315.093,00	259.071,76	273.994,20	5,76%	2.984,49
12057EC03001441G	1 - 0	ESPAÑA	1.093.000,00	897.027,79	911.194,40	1,58%	2.833,32
12057EC03001443X	1 - 0	ESPAÑA	1.644.240,00	1.352.671,03	1.369.970,96	1,28%	3.459,99
12057EC03001444J	1 - 0	PAISES BAJOS	2.192.320,00	1.803.561,37	1.826.627,94	1,28%	4.613,31
12057EC03001445K	1 - 0	PAISES BAJOS	1.093.000,00	894.285,32	908.451,93	1,58%	2.833,32
12057EC03001446L	1 - 0	PAISES BAJOS	2.192.320,00	1.803.561,38	1.826.627,95	1,28%	4.613,31
12057EC03001447M	1 - 0	ESPAÑA	1.093.000,00	894.285,32	908.451,93	1,58%	2.833,32
12057EC03001448N	1 - 0	ESPAÑA	1.093.000,00	894.285,32	908.451,93	1,58%	2.833,32
12057EC03001495P	1 - 0	PAISES BAJOS	1.621.500,00	1.205.848,89	1.238.803,44	2,73%	6.590,91
12057EC03001533X	1 - 0	PAISES BAJOS	540.500,00	403.196,21	414.181,06	2,72%	2.196,97
12057EC03001534J	1 - 0	PAISES BAJOS	2.702.500,00	2.015.981,05	2.070.905,31	2,72%	10.984,85
12057EC03001577Z	1 - 0	ESPAÑA	5.101.200,00	3.632.577,43	3.703.486,92	1,95%	14.181,90

Cont. Púb. GABRIEL E. BALLARINO, Director (Int.), Dirección de Fiscalización de Exportación.

e. 02/09/2013 N° 67554/13 v. 02/09/2013

ADMINISTRACION FEDERAL DE INGRESOS PUBLICOS**DIRECCION DE FISCALIZACION DE EXPORTACION****Listado de Preajustes de Valor aplicables de conformidad al Art. 748 Inc. c) del C.A.**

P.A. SIM. 3826.00.00.100L

MERCADERIA: BIODISEL

EXPORTADOR: LDC ARGENTINA S.A. C.U.I.T. 30-52671276-9, DESPACHANTE: OUZADE ALEJANDRO C.U.I.T. 23-23805102-9

DESTINACION	ITEM	PAIS	FOB DECLARADO	B.I. DECLARADA	B.I. AJUSTADA	% AJUSTE	DIFERENCIA US\$
12052EC03001115W	1 - 1	PAISES BAJOS	3.617.385,00	2.969.383,44	3.150.770,21	6,11%	36.277,35
12052EC03001115W	1 - 2	PAISES BAJOS	8.447.250,00	6.934.349,66	7.336.598,05	5,80%	80.449,68
12052EC03001117B	1 - 0	PAISES BAJOS	1.050.000,00	861.893,23	911.893,03	5,80%	9.999,96
12052EC03001223W	1 - 0	PAISES BAJOS	674.975,00	532.278,30	536.361,62	0,77%	816,66
12052EC03001224A	1 - 1	PAISES BAJOS	4.097.125,80	3.232.292,91	3.257.078,81	0,77%	4.957,18
12052EC03001224A	1 - 2	PAISES BAJOS	2.052.750,00	1.614.934,72	1.712.684,32	6,05%	19.549,92
12052EC03001224A	1 - 3	PAISES BAJOS	591.470,00	465.188,00	495.846,21	6,59%	6.131,64
12052EC03001253C	1 - 0	PERU	5.250.000,00	4.129.145,28	4.379.144,28	6,05%	49.999,80
12052EC03001255E	1 - 0	PERU	5.250.000,00	4.248.020,35	4.498.019,35	5,89%	49.999,80
12052EC03001256F	1 - 0	PERU	1.785.000,00	1.487.252,98	1.572.252,64	5,72%	16.999,93
12052EC03001257G	1 - 0	PERU	3.150.000,00	2.624.564,09	2.774.563,49	5,72%	29.999,88
12052EC03001258H	1 - 0	PAISES BAJOS	5.250.000,00	4.374.273,49	4.624.272,49	5,72%	49.999,80
12052EC03001260A	1 - 0	ESPAÑA	3.150.000,00	2.624.564,09	2.774.563,49	5,72%	29.999,88
12052EC03001262C	1 - 0	ESPAÑA	5.250.000,00	4.374.273,49	4.624.272,49	5,72%	49.999,80
12052EC03001265F	1 - 0	ESPAÑA	2.290.186,50	1.908.171,83	2.017.227,89	5,72%	21.811,21
12052EC03001269J	1 - 0	ESPAÑA	5.250.000,00	4.374.273,49	4.624.272,49	5,72%	49.999,80
12052EC03001363E	1 - 0	PERU	2.204.000,00	1.789.756,47	1.803.089,75	0,74%	2.666,66
12052EC03001364F	1 - 0	PERU	3.216.000,00	2.626.748,22	2.721.747,84	3,62%	18.999,92
12052EC03001366H	1 - 0	PERU	3.216.000,00	2.626.226,80	2.721.226,42	3,62%	18.999,92
12052EC03001367X	1 - 0	PERU	2.680.000,00	2.188.522,34	2.267.688,69	3,62%	15.833,27
12052EC03001541C	1 - 0	PERU	157.500,00	112.495,77	119.313,95	6,06%	1.363,64
12052EC03001586L	1 - 0	ITALIA	1.785.000,00	1.274.952,04	1.352.224,69	6,06%	15.454,53
12052EC03001587M	1 - 0	ITALIA	2.992.500,00	2.137.419,58	2.266.964,91	6,06%	25.909,06
12052EC03001587M	2 - 0	ITALIA	1.207.500,00	862.467,55	914.740,23	6,06%	10.454,54
12052EC03001605D	1 - 0	ITALIA	1.365.000,00	974.963,32	1.034.054,17	6,06%	11.818,17

DESTINACION	ITEM	PAIS	FOB DECLARADO	B.I. DECLARADA	B.I. AJUSTADA	% AJUSTE	DIFERENCIA US\$
12052EC03001606E	1 - 0	ITALIA	1.050.000,00	749.971,79	795.426,29	6,06%	9.090,90
12052EC03001607F	1 - 0	ESPAÑA	735.000,00	524.980,25	556.798,40	6,06%	6.363,63
12052EC03001608G	1 - 0	ESPAÑA	1.050.000,00	753.826,72	799.281,22	6,03%	9.090,90

P.A. SIM. 3826.00.00.100L

MERCADERIA: BIODISEL

EXPORTADOR: MOLINOS RIO DE LA PLATA C.U.I.T. 30-50085862-8, DESPACHANTE: PELLICCIOTTI GAZZANIGA C.U.I.T. 27-11271797-3

DESTINACION	ITEM	PAIS	FOB DECLARADO	B.I. DECLARADA	B.I. AJUSTADA	% AJUSTE	DIFERENCIA US\$
12052EC01007273X	1 - 0	PAISES BAJOS	1.157.365,00	964.466,98	1.017.495,93	5,50%	10.605,79
12052EC01007275K	1 - 0	PAISES BAJOS	1.592.100,00	1.326.744,69	1.387.494,45	4,58%	12.149,95
12052EC01007276L	1 - 0	PAISES BAJOS	5.768.620,00	4.807.164,10	5.087.479,65	5,83%	56.063,11
12052EC01007277M	1 - 0	PAISES BAJOS	1.098.932,80	915.773,67	969.951,12	5,92%	10.835,49
12052EC03001606E	1 - 0	ITALIA	1.050.000,00	749.971,79	795.426,29	6,06%	9.090,90
12052EC03001607F	1 - 0	ESPAÑA	735.000,00	524.980,25	556.798,40	6,06%	6.363,63
12052EC03001608G	1 - 0	ESPAÑA	1.050.000,00	753.826,72	799.281,22	6,03%	9.090,90

Cont. Púb. GABRIEL E. BALLARINO, Director (Int.), Dirección de Fiscalización de Exportación.

e. 02/09/2013 N° 67555/13 v. 02/09/2013

ADMINISTRACION FEDERAL DE INGRESOS PUBLICOS**DIRECCION DE FISCALIZACION DE EXPORTACION****Listado de Preajustes de valor aplicables de conformidad al Art. 748 inc. C) del C.A.**

P.A. SIM. 3826.00.00.100L

MERCADERIA: BIODISEL

EXPORTADOR: VICENTIN S.A. C.U.I.T. 30-50095962-9, DESPACHANTE: FANJUL ALICIA VICTORIA, C.U.I.T. 27-05701189-6

DESTINACION	ITEM	DESTINO	FOB DECLARADO	B.I. DECLARADA	B.I. AJUSTADA	% AJUSTE	DIFERENCIA US\$
12057EC03001280H	1 - 0	PAISES BAJOS	4.291.960,00	3.529.889,76	3.653.255,93	3,49%	24.673,23
12057EC03001282J	1 - 0	PAISES BAJOS	3.250.710,00	2.673.867,21	2.739.941,95	2,47%	13.214,95
12057EC03001284L	1 - 0	PAISES BAJOS	3.144.900,00	2.585.692,57	2.739.941,95	5,97%	30.849,88
12057EC03001290X	1 - 0	PAISES BAJOS	9.712.440,00	7.988.526,76	8.219.825,84	2,90%	46.259,81
12057EC03001359Y	1 - 0	ESPAÑA	2.479.538,00	1.951.999,23	2.013.217,32	3,14%	12.243,62
12057EC03001381J	1 - 0	ESPAÑA	5.261.350,00	4.138.988,29	4.379.529,00	5,81%	48.108,14
12057EC03001385N	1 - 0	ESPAÑA	1.226.950,24	964.292,80	1.024.463,28	6,24%	12.034,10
12057EC03001386Y	1 - 0	ESPAÑA	2.442.099,76	2.006.495,14	2.126.273,03	5,97%	23.955,58
12057EC03001387P	1 - 0	ESPAÑA	1.870.400,00	1.471.697,68	1.531.780,77	4,08%	12.016,62
12057EC03001389R	1 - 0	ESPAÑA	2.667.600,00	2.098.773,50	2.188.273,14	4,26%	17.899,93
12057EC03001401C	1 - 0	ESPAÑA	2.494.741,00	1.966.034,36	2.014.583,33	2,47%	9.709,79
12057EC03001402D	1 - 0	ESPAÑA	1.056.010,00	830.914,31	875.905,80	5,41%	8.998,30
12057EC03001419L	1 - 0	PAISES BAJOS	3.300.000,00	2.602.691,11	2.627.691,01	0,96%	4.999,98
12057EC03001420D	1 - 0	PAISES BAJOS	1.572.450,00	1.236.720,80	1.313.845,49	6,24%	15.424,94
12057EC03001427K	1 - 0	ESPAÑA	1.880.812,50	1.481.413,70	1.532.819,74	3,47%	10.281,21
12057EC03001428L	1 - 0	PAISES BAJOS	536.495,00	422.527,73	437.948,50	3,65%	3.084,15

Cont. Púb. GABRIEL E. BALLARINO, Director (Int.), Dirección de Fiscalización de Exportación.

e. 02/09/2013 N° 67556/13 v. 02/09/2013

ADMINISTRACION FEDERAL DE INGRESOS PUBLICOS**DIRECCION DE FISCALIZACION DE EXPORTACION****Listado de Preajustes de Valor aplicables de conformidad al Art. 748 Inc. c) del C.A.**

P.A. SIM. 3826.00.00.100L

MERCADERIA: BIODISEL

EXPORTADOR: OLEAGINOSA MORENO HNOS C.U.I.T. 33-50223222-9, DESPACHANTE: FANJUL ALICIA VICTORIA C.U.I.T. 27-05701189-6

DESTINACION	ITEM	PAIS	FOB DECLARADO	B.I. DECLARADA	B.I. AJUSTADA	% AJUSTE	DIFERENCIA US\$
12057EC03001264J	1 - 0	PAISES BAJOS	2.167.140,00	1.782.578,14	1.826.627,97	2,47%	8.809,96
12057EC03001265K	1 - 0	PAISES BAJOS	1.064.610,00	875.489,13	913.313,98	4,32%	7.564,97
12057EC03001274K	1 - 0	PAISES BAJOS	660.510,00	543.413,41	547.988,39	0,84%	915,00
12057EC03001276M	1 - 0	PAISES BAJOS	541.785,00	445.644,53	456.656,99	2,47%	2.202,49
12057EC03001319K	1 - 0	PAISES BAJOS	5.056.200,00	4.156.665,23	4.568.163,59	9,90%	82.299,67
12057EC03001356L	1 - 0	ESPAÑA	2.057.800,00	1.692.099,31	1.827.265,43	7,99%	27.033,23
12057EC03001357M	1 - 0	ESPAÑA	3.004.020,00	2.469.249,24	2.740.898,15	11,00%	54.329,78
12057EC03001358N	1 - 0	ESPAÑA	885.428,00	728.194,67	776.587,81	6,65%	9.678,63
12057EC03001382K	1 - 0	ESPAÑA	812.677,50	668.466,80	684.985,49	2,47%	3.303,74
12057EC03001383L	1 - 0	ESPAÑA	660.510,00	543.413,41	547.988,39	0,84%	915,00
12057EC03001398R	1 - 0	ESPAÑA	1.074.750,00	884.091,80	913.466,68	3,32%	5.874,98
12057EC01006927S	1 - 0	PAISES BAJOS	219.442,00	182.867,60	184.999,26	1,17%	426,33
12057EC01006956U	1 - 0	ESPAÑA	2.116.000,00	1.763.326,28	1.849.992,60	4,91%	17.333,26
12057EC01006958W	1 - 0	PAISES BAJOS	3.291.630,00	2.743.014,03	2.774.988,90	1,17%	6.394,97
12057EC01007066N	1 - 0	ESPAÑA	215.876,00	179.895,95	184.999,26	2,84%	1.020,66
12057EC01007070X	1 - 0	ESPAÑA	863.504,00	719.583,79	739.997,04	2,84%	4.082,65
12057EC01007465Z	1 - 0	PAISES BAJOS	542.555,00	411.023,39	420.451,35	2,29%	1.885,59
12057EC01007474Z	1 - 0	PAISES BAJOS	2.170.220,00	1.644.093,57	1.681.805,40	2,29%	7.542,37

P.A. SIM. 3826.00.00.100L

MERCADERIA: BIODISEL

EXPORTADOR: UNITEC BIO S.A. C.U.I.T 30-70990095-8, DESPACHANTE: MASTRANGELO TOMAS C.U.I.T. 20-27957556-4

DESTINACION	ITEM	DESTINO	FOB DECLARADO	B.I. DECLARADA	B.I. AJUSTADA	% AJUSTE	DIFERENCIA US\$
12057EC03001450G	1 - 0	ESPAÑA	10.900.000,00	8.940.443,96	9.107.109,96	1,86%	33.333,20
12057EC03001576P	1 - 0	ESPAÑA	4.872.300,00	3.539.683,50	3.607.411,15	1,91%	13.545,53
12057EC03001577Z	1 - 0	ESPAÑA	5.101.200,00	3.632.577,43	3.703.486,92	1,95%	14.181,90

Cont. Púb. GABRIEL E. BALLARINO, Director (Int.), Dirección de Fiscalización de Exportación.

e. 02/09/2013 N° 67558/13 v. 02/09/2013

ADMINISTRACION FEDERAL DE INGRESOS PUBLICOS**DIRECCION DE FISCALIZACION DE EXPORTACION****Listado de Preajustes de Valor aplicables de conformidad al Art. 748 Inc. C) del C.A.**

P.A. SIM. 3826.00.00.100L

MERCADERIA: BIODISEL

EXPORTADOR: LDC ARGENTINA S.A., C.U.I.T. 30-52671276-9, DESPACHANTE: OUZADE ALEJANDRO C.U.I.T. 23-23805102-9

DESTINACION	ITEM	PAIS	FOB DECLARADO	B.I. DECLARADA	B.I. AJUSTADA	% AJUSTE	DIFERENCIA US\$
12052EC03001784L	1 - 0	PERU	1.207.500,00	920.859,08	948.764,92	3,03%	6.594,15
12052EC03001784L	2 - 0	PERU	1.271.623,00	968.792,47	1.015.590,97	4,83%	11.058,49
12052EC03001784L	3 - 0	PERU	3.799.950,00	2.904.504,37	2.992.322,84	3,02%	20.751,51
12052EC03001990K	1 - 0	ESPAÑA	12.012.000,00	9.511.589,65	10.278.393,67	8,06%	181.195,79
12052EC03002074E	1 - 0	PERU	7.275.000,00	5.753.702,82	6.421.016,44	11,60%	157.686,21
12052EC03002151A	1 - 0	ESPAÑA	2.328.000,00	1.841.184,90	2.054.725,26	11,60%	50.459,59
12052EC03002154D	1 - 0	ESPAÑA	242.500,00	191.790,09	214.033,88	11,60%	5.256,21
12052EC03002166G	1 - 0	ESPAÑA	892.500,00	707.136,92	727.763,10	2,92%	4.873,97
12052EC03002167H	1 - 0	ESPAÑA	4.704.500,00	3.720.881,96	4.152.414,10	11,60%	101.971,05
12052EC03002167H	2 - 0	ESPAÑA	3.877.954,50	3.073.984,90	3.163.606,64	2,92%	21.177,62
12052EC03002197K	1 - 0	PERU	2.578.800,00	2.045.130,63	2.104.727,81	2,91%	14.082,81
12052EC03002197K	2 - 0	PERU	2.671.200,00	2.118.408,93	2.180.141,50	2,91%	14.587,41
12052EC03002198L	1 - 0	PERU	525.000,00	416.353,96	428.486,93	2,91%	2.867,02
12052EC03002224B	1 - 0	PAISES BAJOS	2.053.800,00	1.628.776,69	1.676.240,88	2,91%	11.215,79
12052EC03002224B	2 - 0	PAISES BAJOS	2.635.584,00	2.089.600,39	2.180.141,50	4,33%	21.394,86
12052EC03002225C	1 - 0	PAISES BAJOS	518.000,00	410.691,90	428.486,93	4,33%	4.204,97

P.A. SIM. 3826.00.00.100L

MERCADERIA: BIODISEL

EXPORTADOR: VILUCO SOCIEDAD ANONIMA, C.U.I.T 30-50617627-8, DESPACHANTE: PUJOL JUAN EDUARDO C.U.I.T. 20-18339611-1

DESTINACION	ITEM	PAIS	FOB DECLARADO	B.I. DECLARADA	B.I. AJUSTADA	% AJUSTE	DIFERENCIA US\$
12052EC01012093E	1 - 0	ESPAÑA	2.138.480,00	1.729.752,32	1.747.159,20	1,01%	4.113,25

Cont. Púb. GABRIEL E. BALLARINO, Director (Int.), Dirección de Fiscalización de Exportación.

e. 02/09/2013 N° 67223/13 v. 02/09/2013

AUTORIDAD FEDERAL DE SERVICIOS DE COMUNICACION AUDIOVISUAL**Resolución N° 1005/2013**

Bs. As., 23/8/2013

VISTO el Expediente N° 800/13 del registro de la AUTORIDAD FEDERAL DE SERVICIOS DE COMUNICACION AUDIOVISUAL, y

CONSIDERANDO:

Que las actuaciones del Visto documentan la solicitud formulada por el MINISTERIO DE CULTURA Y EDUCACION, de la provincia de FORMOSA, tendiente a obtener autorización para la instalación, funcionamiento y explotación de una estación de radiodifusión sonora por modulación de frecuencia, conforme lo dispuesto por el artículo 149 de la Ley N° 26.522 y en el marco de Convenio de Cooperación ME N° 797/11, celebrado entre el MINISTERIO DE EDUCACION DE LA NACION, la COMISION NACIONAL DE COMUNICACIONES y esta AUTORIDAD FEDERAL.

Que el artículo 149 de la Ley N° 26.522 establece que "...La autoridad de aplicación podrá otorgar, en forma directa por razones fundadas, autorizaciones para la operación de servicios de radiodifusión a establecimientos educativos de gestión estatal. El titular de la autorización será la autoridad educativa jurisdiccional, quién seleccionará para cada localidad los establecimientos que podrán operar el servicio de comunicación audiovisual".

Que en ese orden, el peticionante seleccionó para tal fin a la ESCUELA PROVINCIAL DE NIVEL EDUCACION SECUNDARIA N° 32, de la localidad de GENERAL LUCIO V. MANSILLA, provincia de FORMOSA.

Que, por su parte, la COMISION NACIONAL DE COMUNICACIONES asignó para el presente trámite el canal 233, frecuencia 94.5 MHz., con categoría "F", y señal distintiva LRR813, para la localidad de GENERAL LUCIO V. MANSILLA, provincia de FORMOSA.

Que la Dirección General de Asuntos Jurídicos y Regulatorios ha tomado la intervención que le compete.

Que el DIRECTORIO de la AUTORIDAD FEDERAL DE SERVICIOS DE COMUNICACION AUDIOVISUAL acordó el dictado del presente acto administrativo, mediante la suscripción del acta correspondiente.

Que la presente medida se dicta de conformidad con las atribuciones conferidas por los artículos 12, inciso 8) y 149 de la Ley N° 26.522.

Por ello,

EL DIRECTORIO DE LA AUTORIDAD FEDERAL DE SERVICIOS DE COMUNICACION AUDIOVISUAL RESUELVE:

ARTICULO 1° — Autorízase al MINISTERIO DE CULTURA Y EDUCACION, de la provincia de FORMOSA, a la instalación, funcionamiento y explotación de una estación de radiodifusión sonora por modulación de frecuencia, en el ámbito de la ESCUELA PROVINCIAL DE NIVEL EDUCACION SECUNDARIA N° 32, de la localidad de GENERAL LUCIO V. MANSILLA, provincia de FORMOSA.

ARTICULO 2° — Asignase al servicio autorizado en el artículo 1°, el canal 233, frecuencia 94.5 MHz., con categoría "F", y señal distintiva LRR813, para la localidad de GENERAL LUCIO V. MANSILLA, provincia de FORMOSA.

ARTICULO 3° — Exceptúase al MINISTERIO DE CULTURA Y EDUCACION, de la provincia de FORMOSA, del pago del gravamen establecido por el artículo 94 de la Ley N° 26.522, con relación a la prestación del servicio autorizado en el artículo 1°.

ARTICULO 4° — Regístrese, comuníquese a las áreas pertinentes y a la COMISION NACIONAL DE COMUNICACIONES, notifíquese, publíquese, dése a la DIRECCION NACIONAL DEL REGISTRO OFICIAL y archívese. — MARTIN SABBATELLA, Presidente del Directorio, Autoridad Federal de Servicios de Comunicación Audiovisual.

e. 02/09/2013 N° 67479/13 v. 02/09/2013

AUTORIDAD FEDERAL DE SERVICIOS DE COMUNICACION AUDIOVISUAL**Resolución N° 1006/2013**

Bs. As., 23/8/2013

VISTO el Expediente N° 798/13 del registro de la AUTORIDAD FEDERAL DE SERVICIOS DE COMUNICACION AUDIOVISUAL, y

CONSIDERANDO:

Que las actuaciones del Visto documentan la solicitud formulada por el MINISTERIO DE CULTURA Y EDUCACION, de la provincia de FORMOSA, tendiente a obtener autorización para la instalación, funcionamiento y explotación de una estación de radiodifusión sonora por modulación de frecuencia, conforme lo dispuesto por el artículo 149 de la Ley N° 26.522 y en el marco de Convenio de Cooperación ME N° 797/11, celebrado entre el MINISTERIO DE EDUCACION DE LA NACION, la COMISION NACIONAL DE COMUNICACIONES y esta AUTORIDAD FEDERAL.

Que el artículo 149 de la Ley N° 26.522 establece que "...La autoridad de aplicación podrá otorgar, en forma directa por razones fundadas, autorizaciones para la operación de servicios de radiodifusión a establecimientos educativos de gestión estatal. El titular de la autorización será la autoridad educativa jurisdiccional, quién seleccionará para cada localidad los establecimientos que podrán operar el servicio de comunicación audiovisual".

Que en ese orden, el peticionante seleccionó para tal fin a la ESCUELA DE EDUCACION SECUNDARIA MODALIDAD INTERCULTURAL BILINGÜE N° 5, de la localidad de MARIA CRISTINA, provincia de FORMOSA.

Que, por su parte, la COMISION NACIONAL DE COMUNICACIONES asignó para el presente trámite el canal 205, frecuencia 88.9 MHz., con categoría "F", y señal distintiva LRR812, para la localidad de MARIA CRISTINA, provincia de FORMOSA.

Que la Dirección General de Asuntos Jurídicos y Regulatorios ha tomado la intervención que le compete.

Que el DIRECTORIO de la AUTORIDAD FEDERAL DE SERVICIOS DE COMUNICACION AUDIOVISUAL acordó el dictado del presente acto administrativo, mediante la suscripción del acta correspondiente.

Que la presente medida se dicta de conformidad con las atribuciones conferidas por los artículos 12, inciso 8) y 149 de la Ley N° 26.522.

Por ello,

EL DIRECTORIO DE LA AUTORIDAD FEDERAL
DE SERVICIOS DE COMUNICACION AUDIOVISUAL
RESUELVE:

ARTICULO 1° — Autorízase al MINISTERIO DE CULTURA Y EDUCACION, de la provincia de FORMOSA, a la instalación, funcionamiento y explotación de una estación de radiodifusión sonora por modulación de frecuencia, en el ámbito de la ESCUELA DE EDUCACION SECUNDARIA MODALIDAD INTERCULTURAL BILINGÜE N° 5, de la localidad de MARIA CRISTINA, provincia de FORMOSA.

ARTICULO 2° — Asígnase al servicio autorizado en el artículo 1°, el canal 205, frecuencia 88.9 MHz., con categoría "F", y señal distintiva LRR812, para la localidad de MARIA CRISTINA, provincia de FORMOSA.

ARTICULO 3° — Exceptúase al MINISTERIO DE CULTURA Y EDUCACION, de la provincia de FORMOSA, del pago del gravamen establecido por el artículo 94 de la Ley N° 26.522, con relación a la prestación del servicio autorizado en el artículo 1°.

ARTICULO 4° — Regístrese, comuníquese a las áreas pertinentes y a la COMISION NACIONAL DE COMUNICACIONES, notifíquese, publíquese, dése a la DIRECCION NACIONAL DEL REGISTRO OFICIAL y archívese. — MARTIN SABBATELLA, Presidente del Directorio, Autoridad Federal de Servicios de Comunicación Audiovisual.

e. 02/09/2013 N° 67482/13 v. 02/09/2013

AUTORIDAD FEDERAL DE SERVICIOS DE COMUNICACION AUDIOVISUAL**Resolución N° 1007/2013**

Bs. As., 23/8/2013

VISTO el Expediente N° 724/13 del registro de la AUTORIDAD FEDERAL DE SERVICIOS DE COMUNICACION AUDIOVISUAL, y

CONSIDERANDO:

Que las actuaciones del Visto documentan la solicitud formulada por la COMUNIDAD ABORIGEN AIM MOKOILEK, perteneciente al Pueblo MOCOVI, radicada en la localidad de COLONIA DOLORES, departamento de SAN JUSTO, provincia de SANTA FE, tendiente a obtener autorización para la instalación, funcionamiento y explotación de una estación de radiodifusión sonora por modulación de frecuencia, en la localidad y provincia mencionadas.

Que la Ley N° 26.522, de Servicios de Comunicación Audiovisual, establece como primordial objetivo la promoción y garantía del libre ejercicio del derecho de toda persona a investigar, buscar, recibir y difundir informaciones, opiniones e ideas, sin censura, en el marco del respeto al Estado de Derecho democrático y los derechos humanos, conforme las obligaciones emergentes de la Convención Americana sobre Derechos Humanos y demás tratados incorporados o que sean incorporados en el futuro a la Constitución Nacional, y que es su espíritu administrar el espectro radioeléctrico en base a criterios democráticos y republicanos que garanticen una igualdad de oportunidades para todos los individuos en su acceso por medio de las asignaciones respectivas.

Que su Artículo 3° inciso ñ) establece como objetivo la preservación y promoción de la identidad y los valores culturales de los Pueblos Originarios.

Que el Artículo 151 de la citada ley dispone que los Pueblos Originarios podrán ser autorizados para la instalación y funcionamiento de servicios de comunicación audiovisual.

Que la COMISION NACIONAL DE COMUNICACIONES asignó para el presente trámite el canal 203, frecuencia 88.5 MHz., con categoría "F", con la señal distintiva LRS839, para la localidad de COLONIA DOLORES, provincia de SANTA FE, de acuerdo a lo establecido en la reglamentación técnica vigente.

Que la comunidad solicitante cumple con la presentación de la Propuesta Comunicacional acorde a los objetivos de la Ley N° 26.522, donde se contemplan, entre otras especificaciones de carácter técnico, el plan de programación y su forma de financiamiento.

Que el INSTITUTO NACIONAL DE ASUNTOS INDIGENAS certifica que la COMUNIDAD ABORIGEN AIM MOKOILEK, posee personería jurídica, inscripta en el Registro Nacional de Comunidades Indígenas mediante Resolución INAI N° 553/2008, de fecha 17 de Octubre de 2008.

Que la Dirección General de Asuntos Jurídicos y Regulatorios ha tomado la intervención que le compete.

Que el DIRECTORIO de la AUTORIDAD FEDERAL DE SERVICIOS DE COMUNICACION AUDIOVISUAL acordó el dictado del presente acto administrativo, mediante la suscripción del acta correspondiente.

Que la presente medida se dicta de conformidad con las atribuciones conferidas por los artículos 12, inciso 8) y 151 de la Ley N° 26.522.

Por ello,

EL DIRECTORIO DE LA AUTORIDAD FEDERAL
DE SERVICIOS DE COMUNICACION AUDIOVISUAL
RESUELVE:

ARTICULO 1° — Autorízase a la COMUNIDAD ABORIGEN AIM MOKOILEK, perteneciente al pueblo MOCOVI, radicado en la localidad de COLONIA DOLORES, departamento de SAN JUSTO, provincia de SANTA FE, a la instalación, funcionamiento y explotación de una estación de radiodifusión sonora por modulación de frecuencia, en la localidad y provincia mencionadas.

ARTICULO 2° — Asígnase al servicio autorizado en el artículo 1°, el canal 203, frecuencia 88.5 MHz., con categoría "F", y señal distintiva LRS839, para la localidad de COLONIA DOLORES, provincia de SANTA FE.

ARTICULO 3° — Exceptúase a la COMUNIDAD ABORIGEN AIM MOKOILEK, perteneciente al Pueblo MOCOVI, radicado en la localidad de COLONIA DOLORES, departamento de SAN JUSTO, provincia de SANTA FE, del pago del gravamen establecido por el artículo 94 de la Ley N° 26.522, con relación a la prestación del servicio autorizado en el artículo 1°.

ARTICULO 4° — Regístrese, comuníquese a las áreas pertinentes, a la COMISION NACIONAL DE COMUNICACIONES y al INSTITUTO NACIONAL DE ASUNTOS INDIGENAS, notifíquese a la COMUNIDAD ABORIGEN AIM MOKOILEK, publíquese, dése a la DIRECCION NACIONAL DEL REGISTRO OFICIAL y archívese. — MARTIN SABBATELLA, Presidente del Directorio, Autoridad Federal de Servicios de Comunicación Audiovisual.

e. 02/09/2013 N° 67485/13 v. 02/09/2013

AUTORIDAD FEDERAL DE SERVICIOS DE COMUNICACION AUDIOVISUAL**Resolución N° 1008/2013**

Bs. As., 23/8/2013

VISTO el Expediente N° 641/13 del registro de la AUTORIDAD FEDERAL DE SERVICIOS DE COMUNICACION AUDIOVISUAL, y

CONSIDERANDO:

Que las actuaciones del Visto documentan la solicitud formulada por el MINISTERIO DE EDUCACION, de la provincia de CORDOBA, tendiente a obtener autorización para la instalación, funcionamiento y explotación de una estación de radiodifusión sonora por modulación de frecuencia, conforme lo dispuesto por el artículo 149 de la Ley N° 26.522 y en el marco de Convenio de Cooperación ME N° 797/11, celebrado entre el MINISTERIO DE EDUCACION DE LA NACION, la COMISION NACIONAL DE COMUNICACIONES y esta AUTORIDAD FEDERAL.

Que el artículo 149 de la Ley N° 26.522 establece que "...La autoridad de aplicación podrá otorgar, en forma directa por razones fundadas, autorizaciones para la operación de servicios de radiodifusión a establecimientos educativos de gestión estatal. El titular de la autorización será la autoridad educativa jurisdiccional, quién seleccionará para cada localidad los establecimientos que podrán operar el servicio de comunicación audiovisual".

Que en ese orden, el peticionante seleccionó para tal fin al INSTITUTO PROVINCIAL DE ENSEÑANZA MEDIA N° 271 "Doctor Dalmacio Vélez Sarsfield", de la localidad de SANTA ROSA DE CALAMUCHITA, provincia de CORDOBA.

Que, por su parte, la COMISION NACIONAL DE COMUNICACIONES asignó para el presente trámite el canal 219, frecuencia 91.7 MHz., con una PRE máxima de 0,3 Kw. y una HMA máxima de 40 metros y señal distintiva LRT413, para la localidad de SANTA ROSA DE CALAMUCHITA, provincia de CORDOBA.

Que la Dirección General de Asuntos Jurídicos y Regulatorios ha tomado la intervención que le compete.

Que el DIRECTORIO de la AUTORIDAD FEDERAL DE SERVICIOS DE COMUNICACION AUDIOVISUAL acordó el dictado del presente acto administrativo, mediante la suscripción del acta correspondiente.

Que la presente medida se dicta de conformidad con las atribuciones conferidas por los artículos 12, inciso 8) y 149 de la Ley N° 26.522.

Por ello,

EL DIRECTORIO DE LA AUTORIDAD FEDERAL
DE SERVICIOS DE COMUNICACION AUDIOVISUAL
RESUELVE:

ARTICULO 1° — Autorízase al MINISTERIO DE EDUCACION, de la provincia de CORDOBA, a la instalación, funcionamiento y explotación de una estación de radiodifusión sonora por modu-

lación de frecuencia, en el ámbito del INSTITUTO PROVINCIAL DE ENSEÑANZA MEDIA N° 271 "Doctor Dalmacio Vélez Sarsfield", de la localidad de SANTA ROSA DE CALAMUCHITA, provincia de CORDOBA.

ARTICULO 2° — Asignase al servicio autorizado en el artículo 1°, el canal 219, frecuencia 91.7 MHz., con una PRE máxima de 0,3 Kw. y una HMA máxima de 40 metros y señal distintiva LRT413, para la localidad de SANTA ROSA DE CALAMUCHITA, provincia de CORDOBA.

ARTICULO 3° — Exceptúase al MINISTERIO DE EDUCACION, de la provincia de CORDOBA, del pago del gravamen establecido por el artículo 94 de la Ley N° 26.522, con relación a la prestación del servicio autorizado en el artículo 1°.

ARTICULO 4° — Regístrese, comuníquese a las áreas pertinentes y a la COMISION NACIONAL DE COMUNICACIONES, notifíquese, publíquese, dése a la DIRECCION NACIONAL DEL REGISTRO OFICIAL y archívese. — MARTIN SABBATELLA, Presidente del Directorio, Autoridad Federal de Servicios de Comunicación Audiovisual.

e. 02/09/2013 N° 67488/13 v. 02/09/2013

AUTORIDAD FEDERAL DE SERVICIOS DE COMUNICACION AUDIOVISUAL

Resolución N° 1009/2013

Bs. As., 23/8/2013

VISTO el Expediente N° 1244/13 del registro de la AUTORIDAD FEDERAL DE SERVICIOS DE COMUNICACION AUDIOVISUAL, y

CONSIDERANDO:

Que las actuaciones del Visto documentan la solicitud formulada por el MINISTERIO DE EDUCACION, CULTURA, CIENCIA Y TECNOLOGIA, de la provincia del CHACO, tendiente a obtener autorización para la instalación, funcionamiento y explotación de una estación de radiodifusión sonora por modulación de frecuencia, conforme lo dispuesto por el artículo 149 de la Ley N° 26.522 y en el marco de Convenio de Cooperación ME N° 797/11, celebrado entre el MINISTERIO DE EDUCACION DE LA NACION, la COMISION NACIONAL DE COMUNICACIONES y esta AUTORIDAD FEDERAL.

Que el artículo 149 de la Ley N° 26.522 establece que "...La autoridad de aplicación podrá otorgar, en forma directa por razones fundadas, autorizaciones para la operación de servicios de radiodifusión a establecimientos educativos de gestión estatal. El titular de la autorización será la autoridad educativa jurisdiccional, quién seleccionará para cada localidad los establecimientos que podrán operar el servicio de comunicación audiovisual".

Que en ese orden, el peticionante seleccionó para tal fin a la ESCUELA DE EDUCACION SECUNDARIA N° 129 "Pampa Cejas", de la localidad de CHARATA, departamento de CHACABUCO, provincia del CHACO.

Que, por su parte, la COMISION NACIONAL DE COMUNICACIONES asignó para el presente trámite el canal 201, frecuencia 88.1 MHz., con categoría "F", y señal distintiva LRR810, para la localidad de CHARATA (Colonia Juan Larrea), provincia del CHACO.

Que la Dirección General de Asuntos Jurídicos y Regulatorios ha tomado la intervención que le compete.

Que el DIRECTORIO de la AUTORIDAD FEDERAL DE SERVICIOS DE COMUNICACION AUDIOVISUAL acordó el dictado del presente acto administrativo, mediante la suscripción del acta correspondiente.

Que la presente medida se dicta de conformidad con las atribuciones conferidas por los artículos 12, inciso 8) y 149 de la Ley N° 26.522.

Por ello,

EL DIRECTORIO DE LA AUTORIDAD FEDERAL DE SERVICIOS DE COMUNICACION AUDIOVISUAL RESUELVE:

ARTICULO 1° — Autorízase al MINISTERIO DE EDUCACION, CULTURA, CIENCIA Y TECNOLOGIA, de la provincia del CHACO, a la instalación, funcionamiento y explotación de una estación de radiodifusión sonora por modulación de frecuencia, en el ámbito de la ESCUELA DE EDUCACION SECUNDARIA N° 129 "Pampa Cejas", de la localidad de CHARATA, departamento de CHACABUCO, provincia del CHACO.

ARTICULO 2° — Asignase al servicio autorizado en el artículo 1°, el canal 201, frecuencia 88.1 MHz., con categoría "F", y señal distintiva LRR810, para la localidad de CHARATA (Colonia Juan Larrea), provincia del CHACO.

ARTICULO 3° — Exceptúase al MINISTERIO DE EDUCACION, CULTURA, CIENCIA, Y TECNOLOGIA, de la provincia del CHACO, del pago del gravamen establecido por el artículo 94 de la Ley N° 26.522, con relación a la prestación del servicio autorizado en el artículo 1°.

ARTICULO 4° — Regístrese, comuníquese a las áreas pertinentes y a la COMISION NACIONAL DE COMUNICACIONES, notifíquese, publíquese, dése a la DIRECCION NACIONAL DEL REGISTRO OFICIAL y archívese. — MARTIN SABBATELLA, Presidente del Directorio, Autoridad Federal de Servicios de Comunicación Audiovisual.

e. 02/09/2013 N° 67490/13 v. 02/09/2013

AUTORIDAD FEDERAL DE SERVICIOS DE COMUNICACION AUDIOVISUAL

Resolución N° 995/2013

Bs. As., 23/8/2013

VISTO el Expediente N° 1916/12 del registro de la AUTORIDAD FEDERAL DE SERVICIOS DE COMUNICACION AUDIOVISUAL, y

CONSIDERANDO:

Que las actuaciones del Visto documentan la solicitud formulada por el MINISTERIO DE EDUCACION Y DERECHOS HUMANOS, de la provincia de RIO NEGRO, tendiente a obtener autorización para la instalación, funcionamiento y explotación de una estación de radiodifusión sonora por modulación de frecuencia, conforme lo dispuesto por el artículo 149 de la Ley N° 26.522 y en el marco de Convenio de Cooperación ME N° 797/11, celebrado entre el MINISTERIO DE EDUCACION DE LA NACION, la COMISION NACIONAL DE COMUNICACIONES y esta AUTORIDAD FEDERAL.

Que el artículo 149 de la Ley N° 26.522 establece que "...La autoridad de aplicación podrá otorgar, en forma directa por razones fundadas, autorizaciones para la operación de servicios de radiodifusión a establecimientos educativos de gestión estatal. El titular de la autorización será la autoridad educativa jurisdiccional, quién seleccionará para cada localidad los establecimientos que podrán operar el servicio de comunicación audiovisual".

Que en ese orden, el peticionante seleccionó para tal fin al CENTRO DE EDUCACION MEDIA N° 75, de la localidad de CHICHINALES, provincia de RIO NEGRO.

Que, por su parte, la COMISION NACIONAL DE COMUNICACIONES asignó para el presente trámite el canal 204, frecuencia 88.7 MHz., con categoría "F", y señal distintiva LRG997, para la localidad de CHICHINALES, provincia de RIO NEGRO.

Que la Dirección General de Asuntos Jurídicos y Regulatorios ha tomado la intervención que le compete.

Que el DIRECTORIO de la AUTORIDAD FEDERAL DE SERVICIOS DE COMUNICACION AUDIOVISUAL acordó el dictado del presente acto administrativo, mediante la suscripción del acta correspondiente.

Que la presente medida se dicta de conformidad con las atribuciones conferidas por los artículos 12, inciso 8) y 149 de la Ley N° 26.522.

Por ello,

EL DIRECTORIO DE LA AUTORIDAD FEDERAL DE SERVICIOS DE COMUNICACION AUDIOVISUAL RESUELVE:

ARTICULO 1° — Autorízase al MINISTERIO DE EDUCACION Y DERECHOS HUMANOS, de la provincia de RIO NEGRO, a la instalación, funcionamiento y explotación de una estación de radiodifusión sonora por modulación de frecuencia, en el ámbito del CENTRO DE EDUCACION MEDIA N° 75, de la localidad de CHICHINALES, provincia de RIO NEGRO.

ARTICULO 2° — Asignase al servicio autorizado en el artículo 1°, el canal 204, frecuencia 88.7 MHz., con categoría "F", y señal distintiva LRG997, para la localidad de CHICHINALES, provincia de RIO NEGRO.

ARTICULO 3° — Exceptúase al MINISTERIO DE EDUCACION Y DERECHOS HUMANOS, de la provincia de RIO NEGRO, del pago del gravamen establecido por el artículo 94 de la Ley N° 26.522, con relación a la prestación del servicio autorizado en el artículo 1°.

ARTICULO 4° — Regístrese, comuníquese a las áreas pertinentes y a la COMISION NACIONAL DE COMUNICACIONES, notifíquese, publíquese, dése a la DIRECCION NACIONAL DEL REGISTRO OFICIAL y archívese. — MARTIN SABBATELLA, Presidente del Directorio, Autoridad Federal de Servicios de Comunicación Audiovisual.

e. 02/09/2013 N° 67450/13 v. 02/09/2013

Colección Fallos Plenarios



DERECHO DEL TRABAJO



DERECHO COMERCIAL



DERECHO PENAL Y PROCESAL PENAL



DERECHO CIVIL

BOLETIN OFICIAL
DE LA REPUBLICA ARGENTINA

Nueva compilación de jurisprudencia plenaria. Incluye índices cronológico, alfabético y temático.

COMISION NACIONAL DE REGULACION DEL TRANSPORTE**Resolución N° 389/2013**

Bs. As. 26/8/2013

VISTO el Expediente N° S01:0090092/2013 del Registro del MINISTERIO DEL INTERIOR Y TRANSPORTE, y

CONSIDERANDO:

Que por Decreto N° 660 de fecha 24 de junio de 1996, se fusionó la COMISION NACIONAL DE TRANSPORTE AUTOMOTOR, creada por el Decreto N° 104 de fecha 26 de enero de 1993 y la COMISION NACIONAL DE TRANSPORTE FERROVIARIA, creada por el Decreto N° 1836 de fecha 1° de septiembre de 1993, en la COMISION NACIONAL DE REGULACION DEL TRANSPORTE, la que actúa como organismo descentralizado en el ámbito de actual SECRETARIA DE TRANSPORTE del MINISTERIO DEL INTERIOR Y TRANSPORTE, asumiendo las competencias, facultades, derechos y obligaciones de las entidades fusionadas.

Que a través del Decreto N° 1388 de fecha 29 de noviembre de 1996, se aprobó el Estatuto de la mencionada Comisión Nacional y —entre otras— se establecieron sus objetivos, funciones y competencias y se aprobó su organigrama funcional.

Que en el Anexo III del Decreto aludido precedentemente, asimismo, se fijaron las responsabilidades primarias de cada dependencia del Organismo, como también las acciones a su cargo.

Que, en ese sentido, se previó como responsabilidad primaria de la GERENCIA DE ASUNTOS JURIDICOS ejercer la representación judicial y administrativa, y asesorar jurídicamente a la COMISION NACIONAL DE REGULACION DEL TRANSPORTE en su relación con los organismos gubernamentales y respecto de terceros, tanto en sede administrativa como judicial y, entre las diversas acciones a su cargo, representar y defender los intereses del Organismo en todo tipo de conflicto legal, tanto judicial como extrajudicialmente y efectuar la procuración y diligenciamiento de las actuaciones judiciales que eventualmente lo requirieran.

Que la Gerencia aludida, en consecuencia, ejerce la representación en juicio de la Comisión Nacional, a través de los letrados apoderados que la integran y conforme a las normas que regulan aquella actividad.

Que por el Artículo 40 del Decreto N° 34.952 del 8 de noviembre de 1947 se reconoce el derecho de los representantes del ESTADO NACIONAL en juicio a percibir los honorarios que se regulen a su favor cuando estén a cargo de la parte contraria y sea ésta quien los abone, de acuerdo con las disposiciones que reglan la materia en los organismos que representen.

Que cabe incluir entre estos honorarios, a aquellos que se acuerdan con los demandados como consecuencia de su adhesión a alguna de las modalidades de pago del crédito reclamado previstas en las distintas resoluciones de esta Comisión Nacional.

Que en múltiples servicios jurídicos permanentes de la Administración Pública Nacional, se han establecido regímenes de percepción y distribución de honorarios, sobre cuya validez se ha pronunciado reiteradamente la PROCURACION DEL TESORO DE LA NACION, organismo descentralizado del PODER EJECUTIVO NACIONAL (Dictámenes 200:209, 202:3, 231:320, 263:309, 278:166, entre otros).

Que el referido órgano asesor, en tal sentido, ha expresado que tales regímenes han respondido, por lo general, a la intención de estimular la labor profesional y premiar con equidad el esfuerzo mancomunado de los componentes de las asesorías, como asimismo a contribuir a optimizar el funcionamiento del servicio mismo, dotando a su plantel de mejores condiciones para el desenvolvimiento de sus tareas (Dictámenes 237:013 y 278:166), como también, que la circunstancia de que los honorarios pertenezcan al profesional no constituye óbice para que sean objeto, una vez cobrados, de un compromiso previamente asumido, por el cual el beneficiario se obligará a entregar las sumas obtenidas al organismo para el que trabaja, a los fines del cumplimiento de la resolución interna que establece su prorrateo, para distinguir —seguidamente— que, desde esa perspectiva conceptual, es posible diferenciar dos momentos lógicos y cronológicos: en el primero, el profesional adquiere los honorarios fijados a su nombre y los incorpora a su patrimonio; en el segundo, se encuentra constreñido a disponer de ellos en la forma estipulada por su empleador, como consecuencia de un deber jurídico previamente contraído (Dictámenes 200:209 y 278:166).

Que mediante la implementación de dichos regímenes, se ha logrado un sistema proporcional y equitativo de participación de los honorarios judiciales en las asesorías jurídicas.

Que la PROCURACION DEL TESORO DE LA NACION, en el Artículo 3° de la Resolución N° 57/2000, invitó a los Servicios Jurídicos que integran el Cuerpo de Abogados del Estado a adoptar, en sus respectivos ámbitos de competencia, un régimen similar al aprobado en dicha Resolución.

Que, conforme surge de los antecedentes obrantes en las presentes actuaciones en diferentes oportunidades a lo largo de la existencia de esta Comisión Nacional y en base a la existencia de diferentes gestiones se generaron convenios de participación y distribución de honorarios profesionales.

Que, respecto de los mismos, los distintos profesionales han prestado su conformidad existiendo, asimismo, rotación de aquéllos siendo necesario receptor un nuevo régimen dotándolo de las formas sugeridas por la Procuración del Tesoro de la Nación.

Que, hasta la presente resolución se encontraba vigente el convenio suscripto con fecha 14 de agosto de 2008.

Que, a fin de asegurar un mejor ordenamiento de las cuestiones tratadas, contemplando el acuerdo oportunamente celebrado y de manera de resguardar los derechos de los profesionales intervinientes se estipula que el convenio que por la presente se aprueba regirá respecto de las causas en las que el Organismo sea parte, y que devenguen honorarios a partir del 1 de julio de 2013.

Que se considera que el régimen que se aprueba prevé criterios justos y equitativos de participación, toda vez que el abogado que se desempeña en relación de dependencia del ESTADO NACIONAL, o está vinculado al mismo con un contrato de locación, o prestación de servicios, no obtiene por sí el trabajo profesional, sino que éste le es asignado por pertenecer al servicio jurídico estatal, de manera tal que es el ESTADO NACIONAL y no su propio esfuerzo de captación, el que le provee el acceso a la retribución profesional.

Que la Administración Pública Nacional, asimismo, le suministra la infraestructura necesaria para su labor y, por ende, le ahorra los gastos y erogaciones que habitualmente realiza el profesional para afrontar y mantener la organización de medios materiales y humanos que le permiten trabajar.

Que el abogado estatal, por otra parte, recibe la colaboración de sus compañeros, profesionales y administrativos, debiendo desarrollar el ejercicio de sus funciones con responsabilidad y eficiencia de acuerdo con las normas que rigen la materia.

Que, asimismo, su función se encuentra supervisada por la Procuración del Tesoro de la Nación como así también de otros organismos de control.

Que mediante el régimen que se aprueba en la presente, se asegura que la participación en los honorarios de los abogados que llevan las causas judiciales sea razonablemente, a fin de compensar su responsabilidad y estimular su desempeño.

Que se prevé, igualmente, la participación del personal administrativo en la distribución, en una proporcionalidad menor, con el objetivo de reconocer el esfuerzo de quienes integran la infraestructura de apoyo necesaria para el ejercicio profesional sin que ello le genere un derecho adquirido atento a la naturaleza jurídica que ostentan los honorarios profesionales, por lo que de incorporarse sistemas que permitan la evaluación sobre el rendimiento laboral la participación podrá ser modificada en cada caso y para cada agente.

Que se ha previsto el carácter excepcional y no remunerativo de los montos que se perciben.

Que el sistema que se implementa resguarda adecuadamente los créditos estatales al privilegiarlos respecto de los honorarios regulados en juicio, ya que en ningún caso la relación entre los honorarios regulados y los percibidos podrá ser superior a la que haya entre el crédito reconocido al ESTADO NACIONAL por la sentencia judicial y el monto que efectivamente ingrese al patrimonio público.

Que la GERENCIA DE ASUNTOS JURIDICOS dependiente la COMISION NACIONAL DE REGULACION DEL TRANSPORTE ha tomado la intervención que le compete.

Que el presente acto se dicta conforme a lo dispuesto por los Artículos 40 del Decreto N° 34.952/1947 —reglamentario de la Ley del Cuerpo de Abogados del Estado N° 12.954—, el Artículo 3° de la Resolución N° 57/2000 de la PROCURACION DEL TESORO DE LA NACION, el Artículo 7° del Decreto 1204 de fecha 24 de septiembre de 2001, el Estatuto aprobado por el Decreto N° 1388/1996, el Decreto N° 454 de fecha 24 de abril de 2001 y el Decreto N° 893 de fecha 5 de julio de 2013.

Por ello,

EL INTERVENTOR
DE LA COMISION NACIONAL DE REGULACION DEL TRANSPORTE
RESUELVE:

ARTICULO 1° — Apruébase el Régimen de Percepción y Distribución de Honorarios Judiciales de la GERENCIA DE ASUNTOS JURIDICOS dependiente de la COMISION NACIONAL DE REGULACION DEL TRANSPORTE que como Anexo forma parte integrante de la presente resolución que regirá para las causas en las que el Organismo es o sea parte.

ARTICULO 2° — Comuníquese a la PROCURACION DEL TESORO DE LA NACION, en virtud de lo dispuesto en la Resolución N° 57 del 18 de agosto de 2000 de ese órgano.

ARTICULO 3° — Regístrese, comuníquese, publíquese, dése a la Dirección Nacional del Registro Oficial y archívese. — Dr. FERNANDO MANZANARES, Interventor, Comisión Nacional de Regulación del Transporte.

ANEXO

REGIMEN DE PERCEPCION Y DISTRIBUCION DE HONORARIOS DEPENDIENTE DE LA COMISION NACIONAL DE REGULACION DEL TRANSPORTE JUDICIALES DE LOS INTEGRANTES DE LA GERENCIA DE ASUNTOS JURIDICOS.

ARTICULO 1°.- Establécese el Régimen de Percepción y Distribución de Honorarios Judiciales de los integrantes de la GERENCIA DE ASUNTOS JURIDICOS de la COMISION NACIONAL DE REGULACION DEL TRANSPORTE.

ARTICULO 2°.- El presente régimen se aplicará a los honorarios que sean regulados o acordados a favor de los abogados pertenecientes a la GERENCIA DE ASUNTOS JURIDICOS de la COMISION NACIONAL DE REGULACION DEL TRANSPORTE, por su actuación en juicio —sin distinción de jurisdicción o tipo de proceso— y sea cual fuere su condición de revista, cuando aquéllos estén a cargo de la parte contraria no estatal y sean abonados por ella.

ARTICULO 3°.- En todos los procesos en los cuales el ESTADO NACIONAL sea actor y su pretensión sea pecuniaria, la relación entre los honorarios regulados y los percibidos en ningún caso podrá ser superior a la relación entre el crédito reconocido al ESTADO NACIONAL por la sentencia judicial y/o acuerdo celebrado por las partes y el monto que ingrese efectivamente al patrimonio público.

ARTICULO 4°.- La distribución de honorarios se efectuará teniendo en cuenta las siguientes categorías:

- Personal profesional (abogados).
- Personal administrativo.

ARTICULO 5°.- El monto neto de honorarios será distribuido conforme los parámetros que se fijan a continuación

a) El veinte POR CIENTO (20%) al letrado a cuyo nombre se haya hecho la regulación o que tuviera a su cargo el proceso en todos los procesos que no constituyan ejecución fiscal.

Si hubiera más de un profesional con regulación a su nombre, cada uno percibirá el mismo porcentaje para el caso de tener la misma actuación, caso contrario el porcentaje será distribuido proporcionalmente conforme a la participación en cada etapa del proceso.

b) El TREINTA POR CIENTO (30%) se dividirá entre los letrados litigantes pertenecientes a la Subgerencia de Contenciosos de la GERENCIA DE ASUNTOS JURIDICOS, porcentaje que para el caso de tratarse de procesos de ejecución fiscal se incrementará en un CINCUENTA (50%) ya que no regirá en su caso, el porcentaje al firmante previsto en el punto a) del presente.

c) El VEINTICINCO POR CIENTO (25%) se dividirá entre los letrados profesionales del resto de las áreas pertenecientes a la GERENCIA DE ASUNTOS JURIDICOS.

d) El VEINTE POR CIENTO (20%) se distribuirá entre el personal administrativo de la GERENCIA DE ASUNTOS JURIDICOS.

e) El CINCO POR CIENTO (5%) destinado a un fondo a ser creado para responder a multas o reclamos por responsabilidad profesional emergente del accionar de los letrados de la GERENCIA DE ASUNTOS JURIDICOS.

Las sumas derivadas de este porcentaje serán facturadas y percibidas en forma proporcional por cada letrado litigante asumiendo cada uno de ellos la obligación de ponerlo a disposición de la Subgerencia de Contenciosos para el caso de darse la condición establecida en el presente inciso y fuera, consecuentemente, necesario efectuar alguna reparación patrimonial; ello, sin perjuicio de las responsabilidades personales que pudieren existir.

Todo letrado litigante que deje de ostentar el carácter de tal, por la causa que fuera, deberá hacer entrega del monto al agente que lo reemplace en el tratamiento de sus causas. En caso de que las mismas se distribuyeran entre varios letrados, en cabeza del de mayor antigüedad. La falta de cumplimiento con lo establecido en el presente hará incurrir al responsable en falta grave dando lugar al inicio de las acciones pertinentes.

ARTICULO 6°.- Las sumas que se distribuyan en concepto de honorarios tendrán carácter excepcional y no remunerativo.

ARTICULO 7°.- El personal, mencionado en el artículo 4° del presente, puede renunciar al crédito que le corresponda sobre el monto neto de honorarios a distribuir. En tal caso, el monto resultante de la renuncia será distribuido entre el resto del personal con derecho a participar en la distribución, en las proporciones establecidas en el artículo 5° del presente.

ARTICULO 8°.- Los profesionales, que pertenezcan o hayan pertenecido a la GERENCIA DE ASUNTOS JURIDICOS y a quienes se les hayan regulado honorarios alcanzados por el presente régimen, deberán dentro de los CINCO (5) días hábiles administrativos posteriores a la notificación judicial o personal pertinente informar por escrito al titular de la SUBGERENCIA DE CONTENCIOSOS DE LA GERENCIA DE ASUNTOS JURIDICOS acerca de la regulación practicada. En dicha información se deberá individualizar el proceso, tribunal, fuero y la fecha e importe de la regulación y si ésta, está firme o apelada.

Cuando los honorarios fueran acordados con la contraparte por la adhesión a un plan de pagos previsto en las resoluciones de la Comisión Nacional que regulan la materia, el SUBGERENTE DE CONTENCIOSOS deberá poner en conocimiento de tal situación al GERENTE DE ASUNTOS JURIDICOS en igual plazo.

ARTICULO 9°.- El profesional a cuyo nombre se hubieran regulado honorarios alcanzados por este régimen no podrá renunciar a ellos, ni cederlos, ni acordar quitas o esperas o pagos en cuotas con relación a ello.

ARTICULO 10.- De las sumas percibidas y depositadas se deducirán los importes necesarios para pagar o completar el pago, de los tributos de cualquier jurisdicción que sean aplicables, los aportes previsionales cuando correspondan y cualquier otra erogación que debieran afrontar los profesionales intervinientes en el pleito por su actuación profesional en él. La suma resultante conformará el importe neto a distribuir entre quienes estén habilitados para participar en el acto de distribución.

Todo agente que perciba sumas derivadas del objeto del presente convenio, se obliga a otorgar las facturas correspondientes a los montos efectivamente percibidos, como así también a dar efectivo cumplimiento con sus obligaciones impositivas y provisionales. La Subgerencia de Contenciosos será la encargada de efectuar las acciones tendientes al cumplimiento de las cláusulas establecidas en la presente.

Dentro del plazo de 30 días de suscripta la presente, la Subgerencia de Contenciosos de la Gerencia de Asuntos Jurídicos deberá presentar un reglamento interno operativo de las condiciones establecidas en la presente, el cual deberá ser conformado por todos los letrados litigantes y por todos los agentes que participen en la distribución de los honorarios profesionales como requisito indispensable para poder percibirlos. En dicho reglamento también deberá contemplarse la creación del fondo aludido en el artículo 5, inc. e) de la presente resolución, quedando a cargo de la Subgerencia de Contenciosos la administración del mismo y su operatividad.

ARTICULO 11.- El derecho a participar en la distribución de honorarios se genera a partir de haberse cumplido DOCE (12) meses de prestación efectiva y continua de servicios en la GERENCIA DE ASUNTOS JURIDICOS y en relación a los honorarios que se distribuyan a partir de ese momento.

Cesará el derecho a percibir honorarios no devengados a los DOCE (12) meses de haber dejado de prestar servicios en las condiciones establecidas en el párrafo precedente.

El derecho a participar en cada distribución caduca para el personal que haya sido cesanteado, exonerado o que se encuentre gozando de adscripciones, con licencia superior a 60 días o afectado a otra Gerencia.

Las limitaciones establecidas en el primer párrafo de este Artículo no regirán para el profesional a cuyo nombre se haya practicado la regulación de los honorarios percibidos, quien conservará en todo tiempo su derecho a participar en su distribución.

La aceptación y adhesión de este régimen deberá ser comunicada mediante nota firmada por cada letrado y dirigida a La GERENCIA DE ADMINISTRACION Y RECURSOS HUMANOS.

Instrúyese a la GERENCIA DE ADMINISTRACION Y RECURSOS HUMANOS de la COMISION NACIONAL DE REGULACION DEL TRANSPORTE, a fin de que recabe de los profesionales las conformidades y aceptaciones mencionadas al presente régimen.

ARTICULO 12.- Los abogados de la GERENCIA DE ASUNTOS JURIDICOS deberán dar cuenta de este régimen en la primera presentación que hagan en todos los litigios en que actúan, patrocinando o representando a la COMISION NACIONAL DE REGULACION DEL TRANSPORTE. En esas presentaciones, los profesionales deberán: a) transcribir textualmente el Artículo 40 del Decreto N° 34.952 del 8 de noviembre de 1947, Reglamentario de la Ley del Cuerpo de Abogados del Estado N° 12.954, y el Artículo 7° del Decreto N° 1204 de fecha 24 de septiembre de 2001; b) manifestar expresamente su conformidad con el presente régimen;

ARTICULO 13.- El incumplimiento de las obligaciones resultantes de este régimen será considerado una falta disciplinaria o contractual, según corresponda; a tales efectos, se aplicará la normativa vigente al momento del incumplimiento.

e. 02/09/2013 N° 67701/13 v. 02/09/2013

MINISTERIO DE DESARROLLO SOCIAL

INSTITUTO NACIONAL DE ASOCIATIVISMO Y ECONOMIA SOCIAL

El INSTITUTO NACIONAL DE ASOCIATIVISMO Y ECONOMIA SOCIAL, con domicilio en Av. Belgrano N° 1656, de la Ciudad Autónoma de Buenos Aires, notifica que por medio de la Disposición N° 1825, se ha resuelto declarar por cerrada la etapa instructoria y hacerles saber que en el plazo de DIEZ (10) días de notificados podrán presentar alegatos sobre el mérito de las pruebas producidas (artículo 60 del Decreto N° 1759/72 —T.O. 1991— y artículo 28 de la Resolución N° 3098/98 - T.O. Resolución N° 3792/10), a las entidades que a continuación se detallan: ASOCIACION MUTUAL ENTRE SOCIOS Y NO SOCIOS DE LA VECINAL SALADILLO SUD, Matrícula SF 666 (Expte. N° 2731/2008, Resolución N° 3045/2008) y ASOCIACION MUTUAL 25 DE MAYO, Matrícula BA 891 (Expte. 3548/2008, Resolución N° 335/2009). De acuerdo con las normas de vigor, se fija el plazo de DIEZ días para que, de considerarlo pertinente, las entidades procedan a tomar vista de las actuaciones sumariales, en los términos y a los efectos previstos en el art. 60 del Decreto 1759/12. El presente deberá publicarse por TRES DIAS EN EL BOLETIN OFICIAL, de acuerdo con lo dispuesto en el art. 42 del Decreto Reglamentario N° 1759/72 (T.O. 1991). — Dr. RICARDO R. PEYRANO, Coordinador de Intervenciones y Liquidaciones, Instituto Nacional de Asociativismo y Economía Social.

e. 02/09/2013 N° 67357/13 v. 04/09/2013

MINISTERIO DE AGRICULTURA, GANADERIA Y PESCA

INSTITUTO NACIONAL DE SEMILLAS

En cumplimiento del Art. 32 del Decreto N° 2183/91, se comunica a terceros interesados la solicitud de inscripción en el Registro Nacional de la Propiedad de Cultivares, de la creación fitogenética de Rosa (Rosa L.) de nombre TAN 07463 obtenida por Rosen Tantau KG.

Solicitante: Rosen Tantau KG

Representante legal: Edgardo Héctor Lalic

Patrocinante: Ing. Agr. Eduardo Enzo Casella

Fundamentación de novedad: El cultivar inédito de nombre comercial TAN 07463 es similar a los cultivares TANAFIRA Y MEIVRITA, pero difiere en las siguientes características:

	TAN 07463	MEIVRITA	TANOLLIPA
Flor:			
Color externo	Blanco tiza	Rosado suave	-
Tamaño de hoja	Intermedio	-	Grande
Tamaño de pétalo	Intermedio a	Grande a muy	Medio
	Grande	Grande	

Fecha de verificación de estabilidad: 2011

Se recibirán las impugnaciones que se presenten dentro de los TREINTA (30) días de aparecido este aviso.

Ing. Agr. RAIMUNDO LAVIGNOLLE, Director de Registro de Variedades, Instituto Nacional de Semillas.

e. 02/09/2013 N° 67373/13 v. 02/09/2013

MINISTERIO DE AGRICULTURA, GANADERIA Y PESCA

INSTITUTO NACIONAL DE SEMILLAS

En cumplimiento del Art. 32 del Decreto N° 2183/91, se comunica a terceros interesados la solicitud de inscripción en el Registro Nacional de la Propiedad de Cultivares, de Maíz (Zea Mays L.) de nombre C5185Z obtenida por Monsanto NL B.V.

Solicitante: Monsanto NL B.V.

Representante legal: Miguel Alvarez Arancedo

Patrocinante: Ing. Agr. Miguel Alvarez Arancedo

Fundamentación de novedad:

El nuevo cultivar C5185Z se caracteriza por presentar una altura de planta de 217 cm y una altura de inserción de la espiga de 83 cm. Posee 14 hojas en promedio, son de color verde medio con posición normal respecto al tallo. No presenta macollos, y tiene una leve tendencia a tener 2 espigas por planta. La panoja presenta un N° de 5 ramificaciones primarias con anteras de color rosado. Los estigmas son de color verde y el porte de la espiga a cosecha es erecta.

Fecha de verificación de estabilidad: 10/09/2010.

Se recibirán las impugnaciones que se presenten dentro de los TREINTA (30) días de aparecido este aviso.

Ing. Agr. RAIMUNDO LAVIGNOLLE, Director de Registro de Variedades, Instituto Nacional de Semillas.

e. 02/09/2013 N° 67161/13 v. 02/09/2013

MINISTERIO DE AGRICULTURA, GANADERIA Y PESCA

INSTITUTO NACIONAL DE SEMILLAS

En cumplimiento del Art. 32 del Decreto N° 2183/91, se comunica a terceros interesados la solicitud de inscripción en el Registro Nacional de la Propiedad de Cultivares, de Maíz (Zea Mays L.) de nombre C4204Z obtenida por Monsanto NL B.V.

Solicitante: Monsanto NL B.V.

Representante legal: Miguel Alvarez Arancedo

Patrocinante: Ing. Agr. Miguel Alvarez Arancedo

Fundamentación de novedad:

El nuevo cultivar C4204Z se caracteriza por presentar una altura de planta de 191 cm y una altura de inserción de la espiga de 86 cm. Posee 15 hojas en promedio, son de color verde medio con posición normal respecto al tallo. No presenta macollos, y tiene una leve tendencia a tener dos espigas por planta. La panoja presenta un N° de 9 ramificaciones primarias con anteras de color rosado. Los estigmas son de color verde y el porte de la espiga a cosecha es erecta.

Fecha de verificación de estabilidad: 10/10/2009.

Se recibirán las impugnaciones que se presenten dentro de los TREINTA (30) días de aparecido este aviso.

Ing. Agr. RAIMUNDO LAVIGNOLLE, Director de Registro de Variedades, Instituto Nacional de Semillas.

e. 02/09/2013 N° 67162/13 v. 02/09/2013

Solicitante: Monsanto NL B.V.

Representante legal: Miguel Alvarez Arancedo

Patrocinante: Ing. Agr. Miguel Alvarez Arancedo

Fundamentación de novedad:

El nuevo cultivar C3463Z se caracteriza por presentar una altura de planta de 223 cm y una altura de inserción de la espiga de 100 cm. Posee 14 hojas en promedio, son de color verde medio con posición normal respecto al tallo. No presenta macollos, y tiene una leve tendencia a tener 2 espigas por planta. La panoja presenta un N° de 6 ramificaciones primarias con anteras de color púrpura. Los estigmas son de color verde y el porte de la espiga a cosecha es erecta.

Fecha de verificación de estabilidad: 10/10/2009.

Se recibirán las impugnaciones que se presenten dentro de los TREINTA (30) días de aparecido este aviso.

Ing. Agr. RAIMUNDO LAVIGNOLLE, Director de Registro de Variedades, Instituto Nacional de Semillas.

e. 02/09/2013 N° 67175/13 v. 02/09/2013

MINISTERIO DE AGRICULTURA, GANADERIA Y PESCA

INSTITUTO NACIONAL DE SEMILLAS

En cumplimiento del Art. 32 del Decreto N° 2183/91, se comunica a terceros interesados la solicitud de inscripción en el Registro Nacional de la Propiedad de Cultivares, de Maíz (Zea Mays L.) de nombre C4383Z obtenida por Monsanto NL B.V.

Solicitante: Monsanto NL B.V.

Representante legal: Miguel Alvarez Arancedo

Patrocinante: Ing. Agr. Miguel Alvarez Arancedo

Fundamentación de novedad:

El nuevo cultivar C4383Z se caracteriza por presentar una altura de planta de 173 cm y una altura de inserción de la espiga de 70 cm. Posee 14 hojas en promedio, son de color verde medio con posición normal respecto al tallo. No presenta macollos, y tiene una leve tendencia a tener 2 espigas por planta. La panoja presenta un N° de 9 ramificaciones primarias con anteras de color rosado. Los estigmas son de color verde y el porte de la espiga a cosecha es erecta.

Fecha de verificación de estabilidad: 10/10/2009.

Se recibirán las impugnaciones que se presenten dentro de los TREINTA (30) días de aparecido este aviso.

Ing. Agr. RAIMUNDO LAVIGNOLLE, Director de Registro de Variedades, Instituto Nacional de Semillas.

e. 02/09/2013 N° 67167/13 v. 02/09/2013

MINISTERIO DE AGRICULTURA, GANADERIA Y PESCA

INSTITUTO NACIONAL DE SEMILLAS

En cumplimiento del Art. 32 del Decreto N° 2183/91, se comunica a terceros interesados la solicitud de inscripción en el Registro Nacional de la Propiedad de Cultivares, de Maíz (Zea Mays L.) de nombre C4553Z obtenida por Monsanto NL B.V.

Solicitante: Monsanto NL B.V.

Representante legal: Miguel Alvarez Arancedo

Patrocinante: Ing. Agr. Miguel Alvarez Arancedo

Fundamentación de novedad:

El nuevo cultivar C4553Z se caracteriza por presentar una altura de planta de 196 cm y una altura de inserción de la espiga de 77 cm. Posee 14 hojas en promedio, son de color verde medio con posición normal respecto al tallo. No presenta macollos, y tiene una fuerte tendencia a tener 2 espigas por planta. La panoja presenta anteras de color púrpura y un N° de 3 ramificaciones primarias. Los estigmas son de color rosado y el porte de la espiga a cosecha es colgante.

Fecha de verificación de estabilidad: 10/09/2010.

Se recibirán las impugnaciones que se presenten dentro de los TREINTA (30) días de aparecido este aviso.

Ing. Agr. RAIMUNDO LAVIGNOLLE, Director de Registro de Variedades, Instituto Nacional de Semillas.

e. 02/09/2013 N° 67171/13 v. 02/09/2013

MINISTERIO DE AGRICULTURA, GANADERIA Y PESCA

INSTITUTO NACIONAL DE SEMILLAS

En cumplimiento del Art. 32 del Decreto N° 2183/91, se comunica a terceros interesados la solicitud de inscripción en el Registro Nacional de la Propiedad de Cultivares, de Maíz (Zea Mays L.) de nombre C3463Z obtenida por Monsanto NL B.V.

MINISTERIO DE AGRICULTURA, GANADERIA Y PESCA

INSTITUTO NACIONAL DE SEMILLAS

En cumplimiento del Art. 32 del Decreto N° 2183/91, se comunica a terceros interesados la solicitud de inscripción en el Registro Nacional de la Propiedad de Cultivares, de Maíz (Zea Mays L.) de nombre C2482Z obtenida por Monsanto NL B.V.

Solicitante: Monsanto NL B.V.

Representante legal: Miguel Alvarez Arancedo

Patrocinante: Ing. Agr. Miguel Alvarez Arancedo

Fundamentación de novedad:

El nuevo cultivar C2482Z se caracteriza por presentar una altura de planta de 247 cm y una altura de inserción de la espiga de 129 cm. Posee 16 hojas en promedio, son de color verde medio con posición normal respecto al tallo. No presenta macollos, y tiene una leve tendencia a tener dos espigas por planta. La panoja presenta un N° de 12 ramificaciones primarias con anteras de color amarillo. Los estigmas son de color verde y el porte de la espiga a cosecha es erecta.

Fecha de verificación de estabilidad: 15/10/2008.

Se recibirán las impugnaciones que se presenten dentro de los TREINTA (30) días de aparecido este aviso.

Ing. Agr. RAIMUNDO LAVIGNOLLE, Director de Registro de Variedades, Instituto Nacional de Semillas.

e. 02/09/2013 N° 67177/13 v. 02/09/2013

MINISTERIO DE AGRICULTURA, GANADERIA Y PESCA

INSTITUTO NACIONAL DE SEMILLAS

En cumplimiento del Art. 32 del Decreto N° 2183/91, se comunica a terceros interesados la solicitud de inscripción en el Registro Nacional de la Propiedad de Cultivares, de Maíz (Zea Mays L.) de nombre C2389Z obtenida por Monsanto NL B.V.

Solicitante: Monsanto NL B.V.

Representante legal: Miguel Alvarez Arancedo

Patrocinante: Ing. Agr. Miguel Alvarez Arancedo

Fundamentación de novedad:

El nuevo cultivar C2389Z se caracteriza por presentar una altura de planta de 193 cm y una altura de inserción de la espiga de 80 cm. Posee 14 hojas en promedio, son de color verde medio con posición normal respecto al tallo. No presenta macollos, y tiene una fuerte tendencia a tener dos espigas por planta. La panoja presenta un N° de 5 ramificaciones primarias con anteras de color amarillo. Los estigmas son de color verde y el porte de la espiga a cosecha es erecta.

Fecha de verificación de estabilidad: 10/10/2006.

Se recibirán las impugnaciones que se presenten dentro de los TREINTA (30) días de aparecido este aviso.

Ing. Agr. RAIMUNDO LAVIGNOLLE, Director de Registro de Variedades, Instituto Nacional de Semillas.

e. 02/09/2013 N° 67179/13 v. 02/09/2013

MINISTERIO DE AGRICULTURA, GANADERIA Y PESCA

INSTITUTO NACIONAL DE SEMILLAS

En cumplimiento del Art. 32 del Decreto N° 2183/91, se comunica a terceros interesados la solicitud de inscripción en el Registro Nacional de la Propiedad de Cultivares, de Maíz (Zea Mays L.) de nombre C2152Z obtenida por Monsanto NL B.V.

Solicitante: Monsanto NL B.V.

Representante legal: Miguel Alvarez Arancedo

Patrocinante: Ing. Agr. Miguel Alvarez Arancedo

Fundamentación de novedad:

El nuevo cultivar C2152Z se caracteriza por presentar una altura de planta de 188 cm y una altura de inserción de la espiga de 76 cm. Posee 12 hojas en promedio, son de color verde medio con posición normal respecto al tallo. No presenta macollos, y tiene una leve tendencia a tener 2 espigas por planta. La panoja presenta un N° de 10 ramificaciones primarias con anteras de color púrpura. Los estigmas son de color rosado y el porte de la espiga a cosecha es erecta.

Fecha de verificación de estabilidad: 10/10/2009.

Se recibirán las impugnaciones que se presenten dentro de los TREINTA (30) días de aparecido este aviso.

Ing. Agr. RAIMUNDO LAVIGNOLLE, Director de Registro de Variedades, Instituto Nacional de Semillas.

e. 02/09/2013 N° 67183/13 v. 02/09/2013

MINISTERIO DE AGRICULTURA, GANADERIA Y PESCA

INSTITUTO NACIONAL DE SEMILLAS

En cumplimiento del Art. 32 del Decreto N° 2183/91, se comunica a terceros interesados la solicitud de inscripción en el Registro Nacional de la Propiedad de Cultivares, de Maíz (Zea Mays L.) de nombre C6953Z obtenida por Monsanto NL B.V.

Solicitante: Monsanto NL B.V.

Representante legal: Miguel Alvarez Arancedo

Patrocinante: Ing. Agr. Miguel Alvarez Arancedo

Fundamentación de novedad:

El nuevo cultivar C6953Z se caracteriza por presentar una altura de planta de 197 cm y una altura de inserción de la espiga de 80 cm. Posee 14 hojas en promedio, son de color verde medio con posición normal respecto al tallo. No presenta macollos, y tiene una espiga por planta. La panoja presenta un N° de 8 ramificaciones primarias con anteras de color amarilla. Los estigmas son de color verde y el porte de la espiga a cosecha es erecta.

Fecha de verificación de estabilidad: 10/10/2006.

Se recibirán las impugnaciones que se presenten dentro de los TREINTA (30) días de aparecido este aviso.

Ing. Agr. RAIMUNDO LAVIGNOLLE, Director de Registro de Variedades, Instituto Nacional de Semillas.

e. 02/09/2013 N° 67184/13 v. 02/09/2013

MINISTERIO DE AGRICULTURA, GANADERIA Y PESCA

INSTITUTO NACIONAL DE SEMILLAS

En cumplimiento del Art. 32 del Decreto N° 2183/91, se comunica a terceros interesados la solicitud de inscripción en el Registro Nacional de la Propiedad de Cultivares, de Maíz (Zea Mays L.) de nombre C7230Z obtenida por Monsanto NL B.V.

Solicitante: Monsanto NL B.V.

Representante legal: Miguel Alvarez Arancedo

Patrocinante: Ing. Agr. Miguel Alvarez Arancedo

Fundamentación de novedad:

El nuevo cultivar C7230Z se caracteriza por presentar una altura de planta de 208 cm y una altura de inserción de la espiga de 94 cm. Posee 16 hojas en promedio, son de color verde medio con posición normal respecto al tallo. No presenta macollos, y tiene una leve tendencia a tener 2 espigas por planta. La panoja presenta anteras de color rosado y un N° de 7 ramificaciones primarias. Los estigmas son de color rosado y el porte de la espiga a cosecha es erecta.

Fecha de verificación de estabilidad: 10/09/2010.

Se recibirán las impugnaciones que se presenten dentro de los TREINTA (30) días de aparecido este aviso.

Ing. Agr. RAIMUNDO LAVIGNOLLE, Director de Registro de Variedades, Instituto Nacional de Semillas.

e. 02/09/2013 N° 67185/13 v. 02/09/2013

MINISTERIO DE AGRICULTURA, GANADERIA Y PESCA

INSTITUTO NACIONAL DE SEMILLAS

En cumplimiento del Art. 32 del Decreto N° 2183/91, se comunica a terceros interesados la solicitud de inscripción en el Registro Nacional de la Propiedad de Cultivares, de Maíz (Zea Mays L.) de nombre C7255Z obtenida por Monsanto NL B.V.

Solicitante: Monsanto NL B.V.

Representante legal: Miguel Alvarez Arancedo

Patrocinante: Ing. Agr. Miguel Alvarez Arancedo

Fundamentación de novedad:

El nuevo cultivar C7255Z se caracteriza por presentar una altura de planta de 200 cm y una altura de inserción de la espiga de 80 cm. Posee 14 hojas en promedio, son de color verde medio con posición normal respecto al tallo. No presenta macollos, y tiene una fuerte tendencia a tener 2 espigas por planta. La panoja presenta un N° de 6 ramificaciones primarias con anteras de color amarillo. Los estigmas son de color verde y el porte de la espiga a cosecha es erecta.

Fecha de verificación de estabilidad: 10/10/2006.

Se recibirán las impugnaciones que se presenten dentro de los TREINTA (30) días de aparecido este aviso.

Ing. Agr. RAIMUNDO LAVIGNOLLE, Director de Registro de Variedades, Instituto Nacional de Semillas.

e. 02/09/2013 N° 67186/13 v. 02/09/2013

MINISTERIO DE AGRICULTURA, GANADERIA Y PESCA

INSTITUTO NACIONAL DE SEMILLAS

En cumplimiento del Art. 32 del Decreto N° 2183/91, se comunica a terceros interesados la solicitud de inscripción en el Registro Nacional de la Propiedad de Cultivares, de Maíz (Zea Mays L.) de nombre HC33 obtenida por Monsanto NL B.V.

Solicitante: Monsanto NL B.V.

Representante legal: Miguel Alvarez Arancedo

Patrocinante: Ing. Agr. Miguel Alvarez Arancedo

Fundamentación de novedad:

El nuevo cultivar HC33 se caracteriza por presentar una altura de planta de 220 cm y una altura de inserción de la espiga de 81 cm. Posee 14 hojas en promedio, son de color verde oscuro con posición normal respecto al tallo. No presenta macollos, y tiene una espiga por planta. La panoja presenta un N° de 12 ramificaciones primarias con anteras de color rosado. Los estigmas son de color verde y el porte de la espiga a cosecha es erecta.

Fecha de verificación de estabilidad: 10/10/2006.

Se recibirán las impugnaciones que se presenten dentro de los TREINTA (30) días de aparecido este aviso.

Ing. Agr. RAIMUNDO LAVIGNOLLE, Director de Registro de Variedades, Instituto Nacional de Semillas.

e. 02/09/2013 N° 67188/13 v. 02/09/2013

MINISTERIO DE AGRICULTURA, GANADERIA Y PESCA

INSTITUTO NACIONAL DE SEMILLAS

En cumplimiento del Art. 32 del Decreto N° 2183/91, se comunica a terceros interesados la solicitud de inscripción en el Registro Nacional de la Propiedad de Cultivares, de Maíz (Zea Mays L.) de nombre C8757Z obtenida por Monsanto NL B.V.

Solicitante: Monsanto NL B.V.

Representante legal: Miguel Alvarez Arancedo

Patrocinante: Ing. Agr. Miguel Alvarez Arancedo

Fundamentación de novedad:

El nuevo cultivar C8757Z se caracteriza por presentar una altura de planta de 163 cm y una altura de inserción de la espiga de 67 cm. Posee 13 hojas en promedio, son de color verde medio con posición normal respecto al tallo. No presenta macollos, y tiene una espiga por planta. La panoja presenta un N° de 4 ramificaciones primarias con anteras de color púrpura. Los estigmas son de color verde y el porte de la espiga a cosecha es erecta.

Fecha de verificación de estabilidad: 15/10/2008.

Se recibirán las impugnaciones que se presenten dentro de los TREINTA (30) días de aparecido este aviso.

Ing. Agr. RAIMUNDO LAVIGNOLLE, Director de Registro de Variedades, Instituto Nacional de Semillas.

e. 02/09/2013 N° 67190/13 v. 02/09/2013

MINISTERIO DE AGRICULTURA, GANADERIA Y PESCA

SECRETARIA DE AGRICULTURA, GANADERIA Y PESCA

Resolución N° 351/2013

Bs. As., 27/8/2013

VISTO el Expediente N° S01:0296629/2009 del Registro del ex - MINISTERIO DE PRODUCCION, y

CONSIDERANDO:

Que por el Decreto N° 2.684 de fecha 27 de diciembre de 2012, se estableció que la SECRETARÍA DE AGRICULTURA, GANADERÍA Y PESCA del MINISTERIO DE AGRICULTURA, GANADERÍA Y PESCA, fije los cupos de exportación para las especies que se mencionan en el Anexo del referido decreto.

Que mediante las Resoluciones Nros. 2 de fecha 3 de enero de 2007, 365 de fecha 31 de mayo de 2007, 399 de fecha 8 de junio de 2007, 347 de fecha 1 de noviembre de 2007, todas del entonces MINISTERIO DE ECONOMÍA Y PRODUCCIÓN; 66 de fecha 28 de diciembre de 2007, 368 de fecha 20 de octubre de 2008, ambas de la ex - SECRETARÍA DE AGRICULTURA, GANADERÍA, PESCA Y ALIMENTOS del entonces MINISTERIO DE ECONOMÍA Y PRODUCCIÓN; 578 de fecha 26 de agosto de 2009 de la citada ex - Secretaría del entonces MINISTERIO DE PRODUCCIÓN; 83 de fecha 2 de marzo de 2010, 308 de fecha 25 de junio de 2010, 581 de fecha 9 de septiembre de 2011 y 713 de fecha 5 de octubre de 2012, todas de la SECRETARÍA DE AGRICULTURA, GANADERÍA Y PESCA del MINISTERIO DE AGRICULTURA, GANADERÍA Y PESCA, se han establecido diversas medidas de manejo y preservación, relacionadas con las exportaciones de pescado de río de la Cuenca Parano-Platense hasta su desembocadura en el Río de la Plata.

Que en virtud del Artículo 3° del citado Decreto N° 2.684/12, se estableció que la SUBSECRETARÍA DE PESCA Y ACUICULTURA de la SECRETARÍA DE AGRICULTURA, GANADERÍA Y PESCA del MINISTERIO DE AGRICULTURA, GANADERÍA Y PESCA, evaluará periódicamente el estado de los recursos involucrados en la presente medida y recomendará el volumen de los cupos de exportación a otorgar y las medidas de manejo que resulten pertinentes, con el objeto de preservar el estado del recurso de la Cuenca Parano-Platense (Ríos de la Plata, Uruguay y Paraná).

Que en ese sentido, la aludida Subsecretaría evaluó la pesquería de la "baja cuenca" del Río Paraná, en forma conjunta con las provincias integrantes de la COMISIÓN DE PESCA CONTINENTAL Y ACUICULTURA (CPCyA) del CONSEJO FEDERAL AGROPECUARIO conforme se desprende del Acta de Reunión N° 3 de dicha Comisión de fecha 22 de noviembre de 2012, glosada a fojas 379/386 del expediente citado en el Visto.

Que a los efectos de contar con una imagen global del estado de los recursos y sus respectivas pesquerías, a nivel de toda la cuenca se están ejecutando en los tramos limítrofes de los ríos Uruguay, Paraná, Paraguay y de la Plata, proyectos de evaluación e investigación de índole pesquero en conjunto con los países vecinos, conforme surge del Acta citada precedentemente.

Que la información considerada surge de los referidos proyectos y en particular de VEINTISEIS (26) campañas de evaluación del recurso pesquero en la "baja cuenca", efectuadas durante el período que se extiende desde fines del año 2005 hasta fines del año 2012.

Que en dichas campañas participaron junto al equipo técnico de la Dirección de Pesca Continental de la Dirección Nacional de Planificación Pesquera de la SUBSECRETARÍA DE PESCA Y ACUICULTURA de la SECRETARÍA DE AGRICULTURA, GANADERÍA Y PESCA del MINISTERIO DE AGRICULTURA, GANADERÍA Y PESCA, equipos de investigadores y técnicos de las Provincias de ENTRE RÍOS, SANTA FE y BUENOS AIRES.

Que entre las conclusiones alcanzadas se coincidió que la situación del recurso sábalo (*Prochilodus platensis*) continuó mejorando en cuanto a abundancia y tallas medias y que además ha sido acompañada por una situación hidrológica favorable para la reproducción y reclutamiento de la especie.

Que de acuerdo al informe técnico efectuado por el equipo técnico de la referida Dirección de Pesca Continental, corresponde fijar un cupo de exportación para las especies fluviales atendiendo un criterio adaptativo y precautorio a los efectos de minimizar la posibilidad de una eventual reducción del stock reproductivo.

Que teniendo en cuenta la calidad de la información disponible, tanto biológica como estadística, respecto de las especies de surubíes (*Pseudoplatystoma spp.*), manguruyúes (*Zungaro spp.*), dorados de río (*Salminus spp.*), armados (*Pterodoras spp.*; *Oxydoras spp.*; *Rhinodoras spp.*; *Anadoras spp.*; *Platydoras spp.*; *Trachidoras spp.*; *Doras spp.*) y manduvies (*Ageneiosus spp.*; *Auchenipterus spp.*), deviene necesario desalentar su exportación, hasta tanto los estudios arrojen resultados que sugieran lo contrario.

Que por ello, la totalidad de los representantes provinciales participantes de la reunión de la COMISIÓN DE PESCA CONTINENTAL Y ACUICULTURA (CPCyA) del CONSEJO FEDERAL AGROPECUARIO, de los días 29 y 30 de marzo de 2012 glosada a fojas 322/331, han coincidido que el cupo de exportación para estas especies debe ser nulo.

Que conforme surge de las Actas CPCyA N° 1 de fecha 26 de marzo de 2013 (a fojas 394/399) y N° 2 de fecha 4 de junio de 2013 (a fojas 406/410) respecto a la situación de patíes (*Luciopimelodus pati*) y bagres de río (*Pimelodus spp.*; *Rhamdia spp.*), con el fin de contemplar y valorar tanto los aspectos biológico-pesqueros como los socio-económicos, pero en virtud de no alentar su captura para exportación, se acordó establecer un cupo total anual menor al valor promedio registrado en los últimos años.

Que como consecuencia de la actividad pesquera dirigida al recurso sábalo (*Prochilodus platensis*) se concretan capturas incidentales de otras especies convivientes, tal es el caso de la tararira (*Hoplias malabaricus spp.*) y la boga (*Leporinus spp.*).

Que desde un punto de vista técnico resulta tolerable una captura incidental que no supere el DIEZ POR CIENTO (10%) del total capturado de la especie blanco.

Que la aludida Comisión considera que se está actuando sobre una base científica y técnica ajustada a preservar el recurso, asegurando su sustentabilidad y la continuidad de la actividad pesquera; correspondiendo mantener el sentido precautorio que fuera adoptado para la determinación de cupos de exportación.

Que conforme surge de la referida Acta CPCyA N° 3/12 el equipo técnico de la citada Dirección de Pesca Continental recomendó para el año 2013 un valor de VEINTE MIL TONELADAS (20.000 t) de captura máxima permisible (CMP) para la especie sábalo, a partir de las cuales la Comisión acordó en sostener los valores del cupo de exportación que se viene otorgando en torno de las QUINCE MIL TONELADAS (15.000 t.) y hasta el DIEZ POR CIENTO (10%) de este valor para las especies acompañantes, tararira y boga.

Que atendiendo a motivos socio-económicos de suma importancia para la administración provincial y sin comprometer los recursos pesqueros, oportunamente se efectuó una asignación anticipada del cupo de exportación de las especies sábalo (*Prochilodus platensis*) y de las especies acompañantes, boga (*Leporinus spp.*) y tararira (*Hoplias malabaricus spp.*) a los establecimientos procesadores de pescado de río, radicados en las Provincias de ENTRE

RÍOS, SANTA FE y BUENOS AIRES, conforme surge del Informe de la referida Dirección de Pesca Continental, de fecha 10 de septiembre de 2012, el que obra glosado a fojas 359/361 de las actuaciones mencionadas en el Visto, la que debe ser descontada del cupo que se establezca en la presente medida.

Que la Dirección General de Asuntos Jurídicos del MINISTERIO DE AGRICULTURA, GANADERÍA Y PESCA ha tomado la intervención que le compete.

Que la presente medida se dicta de conformidad con las facultades emergentes del Decreto N° 2.684 de fecha 27 de diciembre de 2012.

Por ello,

EL SECRETARIO
DE AGRICULTURA, GANADERÍA Y PESCA
RESUELVE:

ARTICULO 1° — Fijase hasta el 31 de diciembre de 2013 un cupo de exportación para cada una de las especies que se mencionan en el Anexo que integra el presente acto, según las toneladas allí establecidas.

ARTICULO 2° — El anticipo del cupo de exportación de las especies sábalo (*Prochilodus platensis*), boga (*Leporinus spp.*) y tararira (*Hoplias malabaricus spp.*), percibido por los establecimientos procesadores de pescado de río, deberá computarse como parte integrante del cupo total asignado en la presente medida.

ARTICULO 3° — El cupo de exportación fijado por el Artículo 1° de la presente medida corresponde a pescado entero y fileteado, fresco, refrigerado o congelado; comprendido en las posiciones arancelarias de la NOMENCLATURA COMUN DEL MERCOSUR (N.C.M.) según se detalla en el Anexo que forma parte integrante de la presente resolución.

ARTICULO 4° — La presente Resolución entrará en vigencia a partir del día siguiente al de su publicación en el Boletín Oficial.

ARTICULO 5° — Comuníquese, publíquese, dése a la Dirección Nacional del Registro Oficial y archívese. — Ing. Agr. LORENZO R. BASSO, Secretario de Agricultura, Ganadería y Pesca.

ANEXO

Posición arancelaria	ESPECIES	Cupo en TONELADAS
0304.49.90	Sábalos (<i>Prochilodus spp.</i>)	QUINCE MIL (15.000) entre los de productos de todas las posiciones arancelarias
0304.89.90		
0302.89.31		
0303.89.51		
0305.39.90		
0305.49.90		
0305.59.90		
0305.69.90	Surubíes (<i>Pseudoplatystoma spp.</i>)	CERO (0) entre los productos de todas las posiciones arancelarias
0304.49.90		
0304.89.90		
0302.89.33		
0303.89.53		
0305.39.90		
0305.49.90		
0305.59.90	Tarariras (<i>Hoplias malabaricus</i> y H. cf. <i>lacerdae</i>)	SETECIENTOS CINCUENTA (750) entre los productos de todas las posiciones arancelarias
0304.49.90		
0304.89.90		
0302.89.34		
0303.89.54		
0305.39.90		
0305.49.90		
0305.59.90		
0305.69.90		

0304.49.90	Bogas (Leporinus spp.)	SETECIENTOS CINCUENTA (750) entre los productos de todas las posiciones arancelarias
0304.89.90		
0302.89.35		
0303.89.55		
0305.39.90		
0305.49.90		
0305.59.90		
0305.69.90		
0304.49.90	Manguruyúes (Zungaro spp.)	CERO (0) entre los productos de todas las posiciones arancelarias
0304.89.90		
0302.89.90		
0303.89.90		
0305.39.90		
0305.49.90		
0305.59.90		
0305.69.90		
0304.49.90	Dorados de río (Salminus spp.)	CERO (0) entre los productos de todas las
0304.89.90		

0303.89.90	Bagres de río (Pimelodus spp.; Rhamdia spp.)	VEINTICINCO (25) entre los productos de todas las posiciones arancelarias
0305.39.90		
0305.49.90		
0305.59.90		
0305.69.90		
0304.49.90		
0304.89.90		
0302.89.90		
0303.89.90		
0305.39.90		
0305.49.90		
0305.59.90		
0305.69.90		

e. 02/09/2013 N° 67530/13 v. 02/09/2013

MINISTERIO DE SALUD**Resolución N° 1341/2013**

Bs. As., 27/8/2013

VISTO el expediente N° 2002-18715/12-2 del registro del MINISTERIO DE SALUD, las Leyes 17.132, 23.873, complementarias y modificatorias, el Decreto-Ley 7.595/1963, ratificado por la Ley 16.478 y las Resoluciones Ministeriales N° 1337 de fecha 14 de noviembre de 2001 y N° 1105 de fecha 27 de julio de 2006, y

CONSIDERANDO:

Que es necesario afirmar el rol de Rectoría del MINISTERIO DE SALUD en el desarrollo y calidad de los Recursos Humanos en Salud, teniendo en cuenta también los procesos de integración regional.

Que el ordenamiento racional, la planificación y distribución de los Recursos Humanos en Salud, son un componente central en la política sanitaria de este MINISTERIO.

Que la profesión Bioquímica ha desarrollado diversas modalidades de formación de post grado y esto ha determinado la existencia de numerosas especializaciones en la profesión.

Que es necesario determinar y validar aquellas especializaciones que constituyen especialidades Bioquímicas.

Que por lo tanto resulta pertinente armonizar con las jurisdicciones provinciales cuáles especialidades deberán ser reconocidas en todo el país, con el objeto de estimular su formación en función de las necesidades de la población.

Que el reconocimiento de especialidades es dinámico y requiere de actualizaciones periódicas por la evolución científica y las necesidades de recursos humanos caracterizados.

Que en ese marco, se presentaron para el estudio y consideración de la Comisión Nacional Asesora del Ejercicio de las Profesiones de Grado Universitario en Salud creada por la Resolución Ministerial N° 1105 del 27 de julio de 2006, los formularios correspondientes para el reconocimiento de OCHO (8) especialidades Bioquímicas: la especialidad de BIOQUIMICA CLINICA, con Areas: Química Clínica, Hematología, Citología, Endocrinología, Inmunología, Inmunohematología y Banco de Sangre, Microbiología Clínica, Micología, Bacteriología, Parasitología, Virología, Genética, Hepatología, Toxicología Clínica, Neurobiología, Emergentología, la de TOXICOLOGIA LEGAL Y FORENSE, la de BROMATOLOGIA, la de BIOTECNOLOGIA, la de BIOQUIMICA DEL MEDIO AMBIENTE, la de NUTRICION, la de BIOQUIMICA INDUSTRIAL y la de GESTION DE CALIDAD EN EL LABORATORIO DE BIOQUIMICA CLINICA.

Que dichas especialidades han sido sometidas a consideración de los representantes técnicos de las distintas jurisdicciones provinciales.

Que dicha Comisión Nacional Asesora del Ejercicio de las Profesiones de Grado Universitario en Salud en reunión del 7 de agosto de 2009 resolvió proponer al CONSEJO FEDERAL DE SALUD (COFESA) la aprobación de dichas especialidades.

Que los Ministros presentes en la Reunión Ordinaria del CONSEJO FEDERAL DE SALUD (COFESA) del 4 de septiembre de 2009 aprobaron la incorporación de estas especialidades.

Que por Decreto-Ley 7.595/1963, ratificado por Ley 16.478, se crea en la jurisdicción de la Ciudad Autónoma de Buenos Aires el COLEGIO OFICIAL DE FARMACEUTICOS Y BIOQUIMICOS DE LA CAPITAL FEDERAL, institución que tiene a su cargo el contralor profesional y el gobierno de la matrícula de los Bioquímicos.

Que el Decreto-Ley 7.595/1963, sus normas complementarias y modificatorias, no regulan la especialización de la profesión bioquímica, por lo que los procesos de certificación y registro de las especialidades bioquímicas son de carácter voluntario en el ámbito de aplicación de la normativa mencionada.

Que, sin embargo, cabe destacar la importancia de generar mecanismos de certificación y registro de las especialidades bioquímicas, por ser instancias que favorecen el desarrollo de un sistema de salud transparente, equitativo y de mayor calidad.

0302.89.90		posiciones arancelarias
0303.89.90		
0305.39.90		
0305.49.90		
0305.59.90		
0305.69.90		
0304.49.90	Paties (Luciopimelodus pati)	CIENTO CINCUENTA (150) entre los productos de todas las posiciones arancelarias
0304.89.90		
0302.89.90		
0303.89.90		
0305.39.90		
0305.49.90		
0305.59.90		
0305.69.90		
0304.49.90	Armados (Pterodoras spp.; Oxydoras spp.; Rhinodoras spp.; Anadoras spp.; Platydoras spp.; Trachidoras spp.; Doras spp.)	CERO (0) entre los productos de todas las posiciones arancelarias
0304.89.90		
0302.89.90		
0303.89.90		
0305.39.90		
0305.49.90		
0305.59.90		
0305.69.90		
0305.39.90		
0305.49.90		
0305.59.90		
0305.69.90		

0304.49.90	Manduvies (Ageneiosus spp.; Auchenipterus spp.)	CERO (0) entre los productos de todas las posiciones arancelarias
0304.89.90		
0302.89.90		

Que en virtud de la normativa vigente se considera que el COLEGIO OFICIAL DE FARMACEUTICOS Y BIOQUIMICOS DE LA CAPITAL FEDERAL debe ser el responsable del procedimiento de certificación de las especialidades Bioquímicas en la jurisdicción de la Ciudad Autónoma de Buenos Aires.

Que en ese entendimiento, el MINISTERIO DE SALUD DE LA NACION a través de la DIRECCION NACIONAL DE REGULACION SANITARIA Y CALIDAD EN SERVICIOS DE SALUD Y LA DIRECCION NACIONAL DE REGISTRO, FISCALIZACION Y SANIDAD DE FRONTERAS ha firmado con el COLEGIO OFICIAL DE FARMACEUTICOS Y BIOQUIMICOS DE LA CAPITAL FEDERAL un Acta Acuerdo donde se ratifica que los bioquímicos especialistas que deseen certificarse lo harán en dicho COLEGIO.

Que la DIRECCION NACIONAL DE REGISTRO, FISCALIZACION Y SANIDAD DE FRONTERAS es el organismo competente para entender en todo lo relativo a la inscripción, registro y fiscalización de los profesionales de la salud especialistas, en la jurisdicción nacional y de la Ciudad Autónoma de Buenos Aires.

Que, por consiguiente, el COLEGIO OFICIAL DE FARMACEUTICOS Y BIOQUIMICOS DE LA CAPITAL FEDERAL deberá registrar las certificaciones en la base de datos que esa DIRECCION NACIONAL indique, así como adecuar sus procedimientos a las directivas que esa DIRECCION sugiera.

Que la DIRECCION NACIONAL DE REGULACION SANITARIA Y CALIDAD EN SERVICIOS DE SALUD, la DIRECCION NACIONAL DE REGISTRO, FISCALIZACION Y SANIDAD DE FRONTERAS, la SUBSECRETARIA DE POLITICAS, REGULACION Y FISCALIZACION y la SECRETARIA DE POLITICAS, REGULACION E INSTITUTOS han prestado la debida conformidad.

Que la DIRECCION GENERAL DE ASUNTOS JURIDICOS ha tomado la intervención de su competencia.

Que se actúa conforme a las disposiciones de la "Ley de Ministerios - T.O. 1992", modificada por Ley N° 26.338.

Por ello,

EL MINISTRO
DE SALUD
RESUELVE:

ARTICULO 1° — Apruébese el Listado de Especialidades Bioquímicas que como ANEXO I integra la presente, en el cual se incluyen las especialidades de BIOQUIMICA CLINICA, con Areas: Química Clínica, Hematología, Citología, Endocrinología, Inmunología, Inmunohematología y Banco de Sangre, Microbiología Clínica, Micología, Bacteriología, Parasitología, Virología, Genética, Hepatología, Toxicología Clínica, Neurobiología, Emergentología, la de TOXICOLOGIA LEGAL Y FORENSE, la de BROMATOLOGIA, la de BIOTECNOLOGIA, la de BIOQUIMICA DEL MEDIO AMBIENTE, la de NUTRICION, la de BIOQUIMICA INDUSTRIAL y la de GESTION DE CALIDAD EN EL LABORATORIO DE BIOQUIMICA CLINICA.

ARTICULO 2° — El listado del ANEXO I podrá ser actualizado periódicamente a través del mecanismo instituido por la Resolución Ministerial N° 1105 de fecha 27 de julio de 2006 y con acuerdo del CONSEJO FEDERAL DE SALUD (COFESA).

ARTICULO 3° — Las modalidades y el procedimiento de certificación para las especialidades bioquímicas serán determinadas por el COLEGIO OFICIAL DE FARMACEUTICOS Y BIOQUIMICOS DE LA CAPITAL FEDERAL y deberán tener como requisitos mínimos aquellos que la normativa marca para los médicos y los odontólogos en la Ley 17.132, Ley 23873, su Decreto Reglamentario N° 10 del 3 de enero de 2003 y normas complementarias y modificatorias.

ARTICULO 4° — La certificación de las especialidades bioquímicas en la jurisdicción de la Ciudad Autónoma de Buenos Aires será un proceso voluntario llevado a cabo por el COLEGIO OFICIAL DE FARMACEUTICOS Y BIOQUIMICOS DE LA CAPITAL FEDERAL, siguiendo las modalidades que se aprueban en el artículo 3° de la presente.

ARTICULO 5° — El COLEGIO OFICIAL DE FARMACEUTICOS Y BIOQUIMICOS DE LA CAPITAL FEDERAL registrará las certificaciones de especialidad otorgadas según las instrucciones que le imparta la DIRECCION NACIONAL DE REGISTRO, FISCALIZACION Y SANIDAD DE FRONTERAS.

ARTICULO 6° — Deróguese parcialmente la Resolución Ministerial N° 1337 de fecha 14 de noviembre de 2001 en lo que respecta al Listado de Especialidades Bioquímicas.

ARTICULO 7° — Invítese a los Señores Ministros del CONSEJO FEDERAL DE SALUD (COFESA) a adecuar las normativas jurisdiccionales que permitan la aplicación de la presente resolución en la medida que corresponda.

ARTICULO 8° — Regístrese, comuníquese, publíquese, dése a la DIRECCION NACIONAL DEL BOLETIN OFICIAL y archívese. — Dr. JUAN L. MANZUR, Ministro de Salud.

ANEXO I

ESPECIALIDAD	AREA
BIOQUIMICA CLINICA	QUIMICA CLINICA
	HEMATOLOGIA
	CITOLOGIA
	ENDOCRINOLOGIA
	INMUNOLOGIA
	INMUNOHEMATOLOGIA Y BANCO DE SANGRE
	MICROBIOLOGIA CLINICA
	MICOLOGIA
	BACTERIOLOGIA
	PARASITOLOGIA
	VIROLOGIA
	GENETICA
	HEPATOLOGIA
	TOXICOLOGIA CLINICA
NEUROBIOLOGIA	
EMERGENTOLOGIA	
TOXICOLOGIA LEGAL Y FORENSE	
BROMATOLOGIA	
BIOTECNOLOGIA	

ESPECIALIDAD	AREA
BIOQUIMICA DEL MEDIO AMBIENTE	
NUTRICION	
BIOQUIMICA INDUSTRIAL	
GESTION DE CALIDAD EN EL LABORATORIO	

e. 02/09/2013 N° 67312/13 v. 02/09/2013

MINISTERIO DE INDUSTRIA

SECRETARIA DE LA PEQUEÑA Y MEDIANA EMPRESA Y DESARROLLO REGIONAL

Resolución N° 128/2013

Bs. As., 28/8/2013

VISTO el Expediente N° S01:0165029/2013 del Registro del MINISTERIO DE INDUSTRIA, las Leyes Nros. 24.467 y 25.300 y sus respectivas reglamentaciones, los Decretos Nros. 357 de fecha 21 de febrero de 2002 y sus modificaciones, y 2.550 de fecha 19 de diciembre de 2012, y

CONSIDERANDO:

Que mediante el dictado del Decreto N° 357 de fecha 21 de febrero de 2002 y sus modificaciones fue aprobado y modificado el Organigrama de Aplicación de la Administración Nacional Centralizada.

Que mediante el dictado del Decreto N° 964 de fecha 1 de julio de 2010 le fue asignada a la SECRETARIA DE LA PEQUEÑA Y MEDIANA EMPRESA Y DESARROLLO REGIONAL del MINISTERIO DE INDUSTRIA, competencia para entender en la aplicación de las normas correspondientes a los Títulos I y II de las Leyes Nros. 24.467 y 25.300 y de las disposiciones dictadas en consecuencia, en su carácter de Autoridad de Aplicación.

Que por medio del Decreto N° 748 de fecha 29 de agosto de 2000 se creó el Programa de Estímulo al Crecimiento de las Micro, Pequeñas y Medianas Empresas, el cual fue luego modificado y complementado mediante los Decretos Nros. 871 de fecha 6 de octubre de 2003 y 159 de fecha 24 de febrero de 2005.

Que en el marco de dicha normativa la mencionada Autoridad de Aplicación efectuó diversos llamados a licitación de cupos de crédito con tasa bonificada, adjudicando los mismos a distintas Entidades Financieras, así como también se han suscripto convenios con el objeto de bonificar la tasa de interés de créditos.

Que por su parte, el Decreto N° 353 de fecha 10 de marzo de 2010 en su Artículo 2° aprobó el PLAN DE RENOVACION DE FLOTA DEL TRANSPORTE AUTOMOTOR DE CARGAS, que prevé entre otros beneficios, el otorgamiento de créditos con tasa de interés bonificada por el ESTADO NACIONAL.

Que a los efectos de la implementación de dichos beneficios, y siendo que la SECRETARIA DE LA PEQUEÑA Y MEDIANA EMPRESA Y DESARROLLO REGIONAL del MINISTERIO DE INDUSTRIA es la encargada de gestionar el pago de la bonificación de la tasa de interés resultante de la aplicación del citado Plan, se suscribió un convenio con el BANCO DE LA NACION ARGENTINA, entidad autárquica en el ámbito del MINISTERIO DE ECONOMIA Y FINANZAS PUBLICAS.

Que el Decreto N° 915 de fecha 28 de junio de 2010 aprobó el Programa Nacional para el Desarrollo de Parques Industriales Públicos en el Bicentenario, por medio del cual el ESTADO NACIONAL se comprometió a bonificar parcialmente la tasa nominal anual que establezcan las Entidades Financieras por préstamos a otorgarse en el marco del mencionado Programa, suscribiéndose a los efectos de su implementación, un nuevo convenio con el BANCO DE LA NACION ARGENTINA.

Que por medio del Decreto N° 2.550 de fecha 19 de diciembre de 2012 se creó el nuevo Programa de Estímulo al Crecimiento de las Micro, Pequeñas y Medianas Empresas, con el objeto de mejorar las condiciones de acceso al crédito del sector.

Que si bien por el Artículo 16 del decreto citado en el considerando anterior se dispuso la derogación de los Decretos Nros. 748/00, 871/03 y 159/05, corresponde a esta Autoridad de Aplicación dar cumplimiento con los pagos en concepto de bonificación de tasa de aquellas operaciones que fueron instrumentadas en el marco del Programa creado por los citados decretos.

Que en ese sentido debe entonces procederse al pago en concepto de bonificación de los créditos otorgados por las Entidades Financieras adjudicatarias de cupos de crédito en los llamados a licitación antes mencionados, aquellos otorgados por las distintas Entidades Financieras y Gobiernos Provinciales con quien esta Autoridad de Aplicación ha suscripto convenios de bonificación de tasa, y aquellos instrumentados en el marco del Plan de Renovación de Flota del Transporte Automotor de Cargas y del Programa Nacional para el Desarrollo de Parques Industriales Públicos en el Bicentenario.

Que en el BANCO MERIDIAN S.A., se encontraron diferencias respecto al monto que fuera contabilizado en concepto de pago del mes de julio. Dicha discrepancia surge de la información habida en el archivo obrante en la Coordinación del Régimen de Bonificación de Tasa de Interés. En consecuencia, habiendo realizado la conciliación pertinente, se confirmó la diferencia observada.

Que la Dirección de Legales del Area de Industria, Comercio y de la Pequeña y Mediana Empresa dependiente de la SUBSECRETARIA DE COORDINACION del MINISTERIO DE INDUSTRIA ha tomado la intervención que le compete.

Que la presente medida se dicta en uso de las facultades establecidas por las Leyes Nros. 24.467 y 25.300, y los Decretos Nros. 357/02 y sus modificaciones, y 2.550/12.

Por ello,

EL SECRETARIO
DE LA PEQUEÑA Y MEDIANA EMPRESA Y DESARROLLO REGIONAL
RESUELVE:

ARTICULO 1° — Autorízase el pago por un monto total de PESOS DOS MILLONES TRESCIENTOS CINCUENTA Y CUATRO MIL SETECIENTOS TREINTA Y SEIS CON VEINTIUN CENTAVOS (\$ 2.354.736,21.-), en concepto de pago de bonificación a los créditos otorgados por la utilización de los cupos colocados con vencimiento en el mes de agosto de 2013, cuyo beneficiario es el

BANCO CENTRAL DE LA REPUBLICA ARGENTINA, debiendo éste realizar las acreditaciones en las cuentas corrientes de los distintos bancos operadores de las líneas de financiamiento del Régimen de Bonificación de Tasas, según surge del Anexo I que, con DOS (2) hojas, forma parte integrante de la presente medida.

El gasto que demande el cumplimiento de lo establecido en este artículo será imputado a la Jurisdicción 51 - MINISTERIO DE INDUSTRIA, Programa 24, Actividad 11, Inciso 5, Partida Principal 1, Parcial 9, Subparcial 2020, Fuente de Financiamiento 11.

ARTICULO 2° — Ejecútase el cobro en concepto de conciliación por diferencias en el pago al BANCO MERIDIAN S.A., por un monto total de PESOS CINCO MIL CUATROCIENTOS OCHENTA Y CINCO CON OCHENTA Y UN CENTAVOS (\$ 5.485,81.-), y pónese en conocimiento del BANCO CENTRAL DE LA REPUBLICA ARGENTINA la presente medida, a fin de que arbitre los medios necesarios para debitar de la cuenta corriente que esta Entidad Financiera posee en dicha Entidad, el importe mencionado, conforme lo establecido en el detalle que consta en el Anexo II que con UNA (1) hoja, forma parte integrante de la presente medida.

ARTICULO 3° — El BANCO CENTRAL DE LA REPUBLICA ARGENTINA deberá acreditar los fondos debitados a las Entidades Financieras en la cuenta del Tesoro Nacional N° 330/00, Operaciones a Imputar a las Entidades, conforme se detalla en el Anexo II de la presente medida.

ARTICULO 4° — Dase intervención a la SECRETARIA DE HACIENDA del MINISTERIO DE ECONOMIA Y FINANZAS PUBLICAS.

ARTICULO 5° — Apruébanse los Anexos I, que con DOS (2) hojas, y II que con UNA (1) hoja, forman parte integrante de la presente medida.

ARTICULO 6° — La presente medida entrará en vigencia a partir de la fecha de su publicación en el Boletín Oficial.

ARTICULO 7° — Comuníquese, publíquese, dése a la Dirección Nacional del Registro Oficial y archívese. — Lic. HORACIO G. ROURA, Secretario de la Pequeña y Mediana Empresa y Desarrollo Regional, Ministerio de Industria.

ANEXO I

TOTALES A PAGAR POR BANCO

BANCO	BONIFICACION
BANCO DE LA NACION ARGENTINA.	\$ 883.264,83
BANCO DE GALICIA Y BUENOS AIRES S.A.	\$ 74.094,21
BANCO CREDICOOP COOPERATIVO LTDO.	\$ 366.359,71
BANCO DE LA PROVINCIA DE BUENOS AIRES.	\$ 330.716,19
BANCO SANTANDER RIO S.A.	\$ 25.432,62
BANCO MACRO S.A.	\$ 47.640,99
BANCO DE INVERSION Y COMERCIO EXTERIOR S.A.	\$ 80.982,61
NUEVO BANCO DE SANTA FE S.A.	\$ 31.492,38
BANCO CIUDAD DE BUENOS AIRES.	\$ 3.894,07
HSBC BANK ARGENTINA S.A.	\$ 36.494,02
BBVA BANCO FRANCES S.A.	\$ 52.822,38
INDUSTRIAL AND COMMERCIAL BANK OF CHINA (ARGENTINA) S.A.	\$ 21.188,77
BANCO PROVINCIA DEL NEUQUEN S.A.	\$ 57.481,22
BANCO DE LA PAMPA S.E.M.	\$ 2.038,16
BANCO SUPERVIELLE S.A.	\$ 654,97
NUEVO BANCO DEL CHACO S.A.	\$ 30.657,29
BANCO DE SAN JUAN S.A.	\$ 27.745,40
CITIBANK S.A.	\$ 3.134,65
BANCO PATAGONIA S.A.	\$ 239.009,84
BANCO DE FORMOSA S.A.	\$ 17.494,69
BANCO COMAFI.	\$ 13.587,58
BANCO DE SANTIAGO DEL ESTERO S.A.	\$ 9,40
BANCO HIPOTECARIO S.A.	\$ 53,08
BANCO SANTA CRUZ S.A.	\$ 6.927,91
BANCO TIERRA DEL FUEGO S.A.	\$ 1.559,24
TOTAL	\$ 2.354.736,21

APERTURA BANCO DE LA NACION ARGENTINA

Entidad	Convenio	Total
Banco de la Nación Argentina	Capital de Trabajo, Proyecto de Inversión y Bienes de Capital	\$ 64.537,03
	Convenio Mendoza II	\$ 10.598,94
	FOMICRO	\$ 23.307,95
	FONDER	\$ 128.764,33
	Convenio de Turismo	\$ 11.785,39
	Convenio Línea 400	\$ 416.261,52
	Convenio Línea 400 - Res. 82/12	\$ 133.142,65
	Convenio Santa Cruz	\$ 5.403,85
	Nación Leasing S.A.	\$ 31.087,75
	Programa de Renovación de Flota del Transporte Automotor de Cargas - Decreto N° 353/10	\$ 16.607,52
Programa Nacional para el Desarrollo de Parques Industriales Públicos en el Bicentenario - Decreto N° 915/10	\$ 41.767,90	
TOTAL	\$ 883.264,83	

APERTURA BANCO DE INVERSION Y COMERCIO EXTERIOR S.A.

Entidad	Convenio	Total
Banco de Inversión y Comercio Exterior S.A.	Capital de Trabajo, Proyecto de Inversión y Bienes de Capital	\$ 1.925,16
	Convenio Santa Fe	\$ 182,28
	Convenio Res. 202/12	\$ 78.875,17
TOTAL	\$ 80.982,61	

APERTURA BANCO DE LA PROVINCIA DE BUENOS AIRES

Entidad	Convenio	Total
Banco de la Provincia de Buenos Aires	Capital de Trabajo, Proyecto de Inversión y Bienes de Capital	\$ 298.608,83
	Provincia Leasing S.A.	\$ 32.107,36
TOTAL	\$ 330.716,19	

ANEXO II

TOTAL COBRO POR CONCILIACION

BANCO MERIDIAN S.A.	\$ 5.485,81
---------------------	-------------

e. 02/09/2013 N° 67532/13 v. 02/09/2013

MINISTERIO DE INDUSTRIA

SECRETARIA DE LA PEQUEÑA Y MEDIANA EMPRESA Y DESARROLLO REGIONAL

Resolución N° 129/2013

Bs. As., 28/8/2013

VISTO el Expediente N° S01:0360702/2010 del Registro del MINISTERIO DE INDUSTRIA, lo dispuesto en las Leyes Nros. 24.467 y 25.300 y en los Decretos Nros. 357 de fecha 21 de febrero de 2002 y sus modificaciones, 62 de fecha 10 de diciembre de 2011 y 2.550 de fecha 19 de diciembre de 2012 y las Resoluciones Nros. 40 de fecha 17 de agosto de 2010, 80 de fecha 18 de octubre de 2010 y 150 de fecha 20 julio de 2012 todas de la SECRETARIA DE LA PEQUEÑA Y MEDIANA EMPRESA Y DESARROLLO REGIONAL del MINISTERIO DE INDUSTRIA, y

CONSIDERANDO:

Que mediante el dictado del Decreto N° 357 de fecha 21 de febrero de 2002 y sus modificaciones fue aprobado y modificado el Organigrama de Aplicación de la Administración Nacional Centralizada.

Que mediante el dictado del Decreto N° 964 de fecha 1 de julio de 2010 le fue asignada a la SECRETARIA DE LA PEQUEÑA Y MEDIANA EMPRESA Y DESARROLLO REGIONAL del MINISTERIO DE INDUSTRIA, competencia para entender en la aplicación de las normas correspondientes a los Títulos I y II de las Leyes Nros. 24.467 y 25.300 y de las disposiciones dictadas en consecuencia, en su carácter de Autoridad de Aplicación.

Que por medio del Decreto N° 748 de fecha 29 de agosto de 2000 se creó el Programa de Estímulo al Crecimiento de las Micro, Pequeñas y Medianas Empresas, el cual fue luego modificado y complementado mediante los Decretos Nros. 871 de fecha 6 de octubre de 2003 y 159 de fecha 24 de febrero de 2005.

Que dicha normativa fue abrogada por el Decreto N° 2.550 de fecha 19 de diciembre de 2012, el cual creó el Programa de Estímulo al Crecimiento de las Micro, Pequeñas y Medianas Empresas, con el objeto de mejorar las condiciones de acceso al crédito del sector.

Que de ese modo por medio de la norma citada en el considerando precedente, se dejó sin efecto el anterior Programa de Estímulo al Crecimiento de las Micro, Pequeñas y Medianas Empresas, creándose uno nuevo de características similares aunque con modificaciones tendientes a optimizar el régimen para brindar una mejor y más amplia asistencia al sector.

Que mediante el Decreto N° 915 de fecha 28 de junio de 2010 fue creado el PROGRAMA NACIONAL PARA EL DESARROLLO DE PARQUES INDUSTRIALES PUBLICOS EN EL BICENTENARIO con el objetivo de financiar obras de infraestructura intra y extramuros, facilitar la radicación y desarrollo de las Pequeñas y Medianas Empresas en Parques Industriales Públicos.

Que, asimismo, mediante el decreto mencionado precedentemente fue creado el Registro Nacional de Parques Industriales en el ámbito de la Unidad de Desarrollo Industrial del ex MINISTERIO DE INDUSTRIA Y TURISMO con el fin de contar con un banco de datos estadísticos que permita disponer en tiempo real de la oferta detallada de predios aptos para la radicación industrial en todo el Territorio Nacional, como así también la nómina de las empresas allí instaladas.

Que mediante la Resolución N° 40 de fecha 17 de agosto de 2010 del MINISTERIO DE INDUSTRIA fue reglamentado el Programa antes mencionado a efectos de instrumentar su operatoria y optimizar su funcionamiento.

Que a su vez, mediante la Resolución N° 80 de fecha 18 de octubre de 2010 de la SECRETARIA DE LA PEQUEÑA Y MEDIANA EMPRESA Y DESARROLLO REGIONAL del MINISTERIO DE INDUSTRIA, fue aprobado el modelo de Convenio de Bonificación de Tasas entre la SECRETARIA DE LA PEQUEÑA Y MEDIANA EMPRESA Y DESARROLLO REGIONAL del MINISTERIO DE INDUSTRIA y el BANCO DE LA NACION ARGENTINA, entidad autárquica en el ámbito del MINISTERIO DE ECONOMIA Y FINANZAS PUBLICAS.

Que dicho Convenio fue suscripto por la SECRETARIA DE LA PEQUEÑA Y MEDIANA EMPRESA Y DESARROLLO REGIONAL y el BANCO DE LA NACION ARGENTINA con fecha 29 de octubre de 2010.

Que por medio del citado Convenio la SECRETARIA DE LA PEQUEÑA Y MEDIANA EMPRESA Y DESARROLLO REGIONAL se comprometió a bonificar los préstamos que el BANCO DE LA NACION ARGENTINA otorgue a las Micro, Pequeñas y Medianas Empresas que resultaren elegibles en el marco del PROGRAMA NACIONAL PARA EL DESARROLLO DE PARQUES INDUSTRIALES PUBLICOS EN EL BICENTENARIO.

Que mediante la Resolución N° 150 de fecha 20 de julio de 2012 de la SECRETARIA DE LA PEQUEÑA Y MEDIANA EMPRESA Y DESARROLLO REGIONAL del MINISTERIO DE INDUSTRIA fue aprobado el modelo de Addenda al Convenio de Bonificación de Tasas antes mencionado, prorrogando su vigencia hasta el día 31 de diciembre de 2012, o hasta agotar el cupo, lo que ocurriera primero.

Que tal como reflejan las constancias de este expediente, ambas partes en dicho Convenio consideran oportuno y conveniente modificar la vigencia del citado Convenio prorrogado por la Addenda mencionada, a fin de darle un mejor cumplimiento a sus objetivos.

Que mediante la Nota DIR/N° 1875 de fecha 28 de diciembre de 2012 el BANCO DE LA NACION ARGENTINA ha informado la modificación de la tasa de la Línea de Financiamiento de Inversiones de Actividades Productivas para la Micro, Pequeña y Mediana Empresa - Reglamentación N° 400 - Condiciones Especiales Programa Nacional para el Desarrollo de Parques Industriales Públicos con Tasa Bonificada por la SECRETARIA DE LA PEQUEÑA Y MEDIANA EMPRESA Y DESARROLLO REGIONAL.

Que en virtud de lo expuesto y atento a las modificaciones instauradas por el nuevo marco reglamentario aprobado por el Decreto N° 2550/12, se ha considerado pertinente promover la adecuación del Convenio antes mencionado de modo de lograr una mejora en las condiciones del financiamiento y continuar apoyando el desarrollo del empresariado nacional, ampliando los montos y la bonificación de tasa asumida por la SECRETARIA DE LA PEQUEÑA Y MEDIANA EMPRESA Y DESARROLLO REGIONAL.

Que en virtud de todo lo expuesto y a los fines de llevar a cabo las modificaciones propuestas resulta procedente promover la suscripción de una nueva Addenda al Convenio suscripto.

Que la Dirección de Legales del Area de Industria, Comercio y de la Pequeña y Mediana Empresa dependiente de la SUBSECRETARIA DE COORDINACION del MINISTERIO DE INDUSTRIA ha tomado la intervención que le compete.

Que la presente medida se dicta en uso de las facultades establecidas por las Leyes Nros. 24.467 y 25.300, y los Decretos Nros. 357/02 y sus modificaciones, 62 de fecha 10 de diciembre de 2011 y 2.550/12.

Por ello,

EL SECRETARIO
DE LA PEQUEÑA Y MEDIANA EMPRESA Y DESARROLLO REGIONAL
RESUELVE:

ARTICULO 1° — Apruébase el modelo de Addenda al Convenio suscripto con fecha 29 de octubre de 2010, modificado por la Addenda aprobada por la Resolución N° 150 de fecha 20 de julio de 2012 de la SECRETARIA DE LA PEQUEÑA Y MEDIANA EMPRESA Y DESARROLLO REGIONAL del MINISTERIO DE INDUSTRIA, entre la SECRETARIA DE LA PEQUEÑA Y MEDIANA EMPRESA Y DESARROLLO REGIONAL del MINISTERIO DE INDUSTRIA y el BANCO DE LA NACION ARGENTINA, entidad autárquica en el ámbito del MINISTERIO DE ECONOMIA Y FINANZAS PUBLICAS, que como Anexo con QUINCE (15) hojas en SEIS (6) cláusulas y Anexo I, forma parte integrante de la presente medida.

ARTICULO 2° — Comuníquese, publíquese, dése a la Dirección Nacional del Registro Oficial y archívese. — Lic. HORACIO G. ROURA, Secretario de la Pequeña y Mediana Empresa y Desarrollo Regional, Ministerio de Industria.

ANEXO

MODELO DE ADDENDA AL CONVENIO CELEBRADO ENTRE LA SECRETARIA DE LA PEQUEÑA Y MEDIANA EMPRESA Y DESARROLLO REGIONAL DEL MINISTERIO DE INDUSTRIA Y EL BANCO DE LA NACION ARGENTINA, ENTIDAD AUTARQUICA EN EL AMBITO DEL MINISTERIO DE ECONOMIA Y FINANZAS PUBLICAS.

En la Ciudad Autónoma de Buenos Aires, a los días del mes de de 2013, entre la SECRETARIA DE LA PEQUEÑA Y MEDIANA EMPRESA Y DESARROLLO REGIONAL del MINISTERIO DE INDUSTRIA, en adelante LA SECRETARIA, con domicilio en la Avenida Julio Argentino Roca N° 651, Piso 2° de la Ciudad Autónoma de Buenos Aires, representada por el señor Secretario Licenciado en Economía Don Horacio Gustavo ROURA (M.I. N° 12.946.611), y el BANCO DE LA NACION ARGENTINA, entidad autárquica en el ámbito del MINISTERIO DE ECONOMIA Y FINANZAS PUBLICAS, en adelante EL BANCO, con domicilio en la calle Bartolomé Mitre N° 326, de la Ciudad Autónoma de Buenos Aires, representado en este acto por el señor Presidente Don Juan Carlos FABREGA (M.I. N° 5.523.631) por la otra parte, en conjunto LAS PARTES, y

CONSIDERANDO:

Que con fecha 29 de octubre de 2010, LAS PARTES suscribieron un Convenio, en adelante EL CONVENIO, por medio del cual LA SECRETARIA se comprometió a bonificar los préstamos que EL BANCO otorgara a las Micro, Pequeñas y Medianas Empresas, y EL BANCO se obligó a otorgar préstamos bajo la normativa "Línea de Financiamiento de Inversiones de Actividades Productivas para la Micro, Pequeña y Mediana Empresa - Reglamentación N° 400 - Condiciones Especiales Programa Nacional para el Desarrollo de Parques Industriales Públicos con Tasa Bonificada por la SECRETARIA DE LA PEQUEÑA Y MEDIANA EMPRESA Y DESARROLLO REGIONAL", todo ello de acuerdo con el reglamento aprobado por la Resolución N° 80 de fecha 18 de octubre de 2010 de LA SECRETARIA.

Que con fecha 27 de agosto de 2012 LAS PARTES suscribieron una Addenda al CONVENIO extendiendo su vigencia hasta el día 31 de diciembre de 2012.

Que LAS PARTES han considerado apropiado modificar nuevamente la vigencia del CONVENIO con el objetivo de extender y optimizar el alcance temporal del apoyo financiero brindado al sector en cuestión.

Que por su parte, EL BANCO ha modificado, con fecha 28 de diciembre de 2012, la tasa de dicha Línea de Financiamiento de Inversiones de Actividades Productivas para la Micro, Pequeña y Mediana Empresa - Reglamentación N° 400.

Que por medio del Decreto N° 2.550 de fecha 19 de diciembre de 2012 se creó el Programa de Estímulo al Crecimiento de las Micro, Pequeñas y Medianas Empresas, y se abrogó el anterior Decreto N° 748 de fecha 29 de agosto de 2000, mejorándose de ese modo las condiciones de acceso al crédito del sector de las Micro, Pequeñas y Medianas Empresas.

Que en virtud de ello LAS PARTES han promovido la adecuación del CONVENIO antes mencionado a fin de dotar a las Micro, Pequeñas y Medianas Empresas con mejores alternativas de financiamiento para su expansión productiva.

Que por todo lo expuesto, LAS PARTES han considerado apropiado plasmar estas modificaciones en el texto del CONVENIO mediante la suscripción de una Addenda.

En virtud de lo antedicho, LAS PARTES acuerdan modificar EL CONVENIO celebrado con fecha 29 de octubre de 2010, modificado por la Addenda suscripta en fecha 27 de agosto de 2012, de acuerdo con los términos que siguen:

CLAUSULA PRIMERA: Sustitúyese la Cláusula Segunda del CONVENIO celebrado con fecha 29 de octubre de 2010 por la siguiente:

"CLAUSULA SEGUNDA: EL BANCO se compromete al otorgamiento de préstamos, mientras se mantengan las actuales condiciones del mercado financiero y sujeto a su capacidad prestable, bajo la normativa "Línea de Financiamiento de Inversiones de Actividades Productivas para la Micro, Pequeña y Mediana Empresa - Reglamentación N° 400 - Condiciones Especiales Programa Nacional para el Desarrollo de Parques Industriales Públicos con Tasa Bonificada por la SECRETARIA DE LA PEQUEÑA Y MEDIANA EMPRESA Y DESARROLLO REGIONAL", que como Anexo I, con NUEVE (9) hojas forma parte integrante del presente CONVENIO, en adelante, LA LINEA.

La bonificación asumida por parte de LA SECRETARIA en el marco del presente CONVENIO será aplicable sobre un total de préstamos a otorgarse a favor de las Micro, Pequeñas y Medianas Empresas por hasta la suma total de PESOS TRESCIENTOS MILLONES (\$ 300.000.000)".

CLAUSULA SEGUNDA: LAS PARTES acuerdan sustituir el Anexo I del CONVENIO celebrado con fecha 29 de octubre de 2010, por el Anexo I que forma parte integrante de la presente Addenda.

CLAUSULA TERCERA: Sustitúyese la Cláusula Tercera del CONVENIO celebrado con fecha 29 de octubre de 2010, por la siguiente:

"CLAUSULA TERCERA: LA SECRETARIA toma a su cargo la bonificación de los préstamos que otorgue EL BANCO en el marco de LA LINEA en la medida que tengan como destino inversiones, incluidas la adquisición de bienes de capital, instalación y puesta en marcha de los bienes financiados tanto para la radicación de empresas en Parques Industriales Públicos como para empresas ya radicadas en tales parques. Este destino comprende supuestos tales como construcción edilicia, instalaciones, maquinaria y equipos, y tecnología.

No podrán ser financiadas operaciones destinadas a:

1. Gastos de evolución ni capital de trabajo.
2. Gastos por tareas específicas para mudanza y/o traslado de equipos existentes.

Asimismo, y conforme lo establecido en el Artículo 34 de la Ley N° 25.300, quedan excluidas del presente CONVENIO las operaciones crediticias destinadas a refinanciar pasivos en mora o que correspondan a créditos otorgados con tasas bonificadas por otros regímenes, cualesquiera sean estos, sea que correspondan al ámbito nacional, provincial o municipal.

El monto del crédito a otorgar no podrá superar la suma de PESOS CINCO MILLONES (\$ 5.000.000).

El plazo de amortización de los créditos a bonificar por LA SECRETARIA no podrá superar los SESENTA (60) meses.

Para el caso de desembolsos múltiples, el plazo mencionado en el párrafo precedente, se considerará desde la consolidación del crédito".

CLAUSULA CUARTA: Sustitúyese la Cláusula Cuarta del CONVENIO celebrado con fecha 29 de octubre de 2010, por la siguiente:

"CLAUSULA CUARTA: La tasa de interés de los créditos a otorgar en el marco de LA LINEA, será fija durante los primeros CINCO (5) años del crédito.

La tasa nominal anual a aplicar será la de la Reglamentación N° 400 según destino, manteniendo las bonificaciones del BANCO por zonas geográficas.

LA SECRETARIA, en el marco del presente CONVENIO, bonificará SEIS (6) puntos porcentuales anuales de la tasa de interés de los créditos que EL BANCO otorgue en el marco de LA LINEA conforme lo establecido en los párrafos precedentes.

En todos los casos, la bonificación a cargo de LA SECRETARIA se restará de la tasa de interés que correspondería abonar a las empresas beneficiarias conforme LA LINEA".

CLAUSULA QUINTA: Sustitúyese la Cláusula Quinta del CONVENIO celebrado con fecha 29 de octubre de 2010, por la siguiente:

"CLAUSULA QUINTA: El presente Convenio de Bonificación de Tasas tendrá vigencia a partir de la fecha de su suscripción y hasta el día 31 de diciembre de 2015 inclusive, hasta el vencimiento de LA LINEA (Reglamentación N° 400), o hasta agotar el cupo de crédito establecido en el último párrafo de la Cláusula Segunda, lo que ocurra primero.

En cualquier caso, se mantendrán las obligaciones comprometidas por LA SECRETARIA, respecto de aquellas operaciones financieras otorgadas durante la vigencia del presente Convenio hasta la fecha correspondiente a la cancelación de la última cuota de los créditos otorgados incluidos en el PROGRAMA NACIONAL PARA EL DESARROLLO DE PARQUES INDUSTRIALES PUBLICOS EN EL BICENTENARIO".

CLAUSULA SEXTA: LAS PARTES manifiestan que las operaciones acordadas así como aquellas con declaración de elegibilidad emitida entre el día 1 de enero de 2013 y la fecha de suscripción de la presente Addenda, quedan alcanzadas por EL CONVENIO y sujetas, en todos sus términos, a las cláusulas del mismo. Asimismo, aquellas operaciones que cuenten con declaración de elegibilidad dictada con anterioridad a la fecha de finalización de la vigencia del CONVENIO, también quedarán alcanzadas por los términos y condiciones del mismo.

En prueba de conformidad se firman DOS (2) ejemplares de un mismo tenor y a un solo efecto en la Ciudad Autónoma de Buenos Aires a los días del mes de de 2013.

ANEXO I AL CONVENIO

"LINEA DE FINANCIAMIENTO DE INVERSIONES DE ACTIVIDADES PRODUCTIVAS PARA LA MICRO, PEQUEÑA Y MEDIANA EMPRESA - REGLAMENTACION N° 400 - CONDICIONES ESPECIALES PROGRAMA NACIONAL PARA EL DESARROLLO DE PARQUES INDUSTRIALES PUBLICOS CON TASA BONIFICADA POR LA SECRETARIA DE LA PEQUEÑA Y MEDIANA EMPRESA Y DESARROLLO REGIONAL".

USUARIOS

Micro, Pequeñas y Medianas Empresas (MiPyMEs), según lo establecido en la Resolución N° 24 de fecha 15 de febrero de 2001 de la ex SECRETARIA DE LA PEQUEÑA Y MEDIANA EMPRESA del ex MINISTERIO DE ECONOMIA, sus modificatorias y complementarias o las que en el futuro la reemplacen ("Reglamentación N° 281 del Banco"), bajo cualquier forma societaria o unipersonal, quedando exceptuadas las cooperativas, de los sectores Industria y Servicios, cuya producción, de bienes y/o servicios, esté destinada al mercado interno o a la exportación, y que obtengan una constancia de elegibilidad de la empresa emitida por la SECRETARIA DE LA PEQUEÑA Y MEDIANA EMPRESA Y DESARROLLO REGIONAL del MINISTERIO DE INDUSTRIA.

DESTINOS

Inversiones, incluidas la adquisición de bienes de capital nacional o de origen extranjero en el caso que no existan sustitutos de producción nacional. Para dicha certificación el BANCO DE LA NACION ARGENTINA entidad autárquica en el ámbito del MINISTERIO DE ECONOMIA Y FINANZAS PUBLICAS, en adelante EL BANCO continuará utilizando el mismo mecanismo que utiliza en

la actualidad, también se financiará instalación y puesta en marcha de los bienes financiados, para la radicación de empresas en Parques Industriales Públicos y para empresas ya radicadas en tales parques. Este destino comprende supuestos tales como construcción edilicia, instalaciones, maquinaria y equipos, y tecnología.

En aquellos casos de préstamos destinados a inversiones para riego (proyectos integrales, adquisición de equipos, sistematización, etcétera), el solicitante deberá aportar un informe técnico de desarrollo hídrico del lugar donde se prevé la inversión, debiendo resultar del mismo que este aspecto no constituya una limitante para el objeto propuesto. (Ver Otras Condiciones - punto 4).

No serán financiados:

1.- Gastos de evolución ni capital de trabajo.

2.- Gastos por tareas específicas para mudanza y/o traslado de equipos existentes. Quedan excluidas las operaciones crediticias destinadas a refinanciar pasivos en mora o aquellas que contemplen créditos otorgados con tasas bonificadas por otros regímenes, cualesquiera sean éstos, tanto los pertenecientes al ámbito nacional, provincial o municipal.

MODALIDAD

En Pesos.

MONTO

Hasta PESOS CINCO MILLONES (\$ 5.000.000).

No rigen las limitaciones para acceder a bonificaciones de tasas fijadas en otras líneas y/o condiciones especiales, en las que la SECRETARIA DE LA PEQUEÑA Y MEDIANA EMPRESA Y DESARROLLO REGIONAL otorgue este beneficio.

El monto máximo del crédito no podrá superar los PESOS CINCO MILLONES (\$ 5.000.000.-) a través de estas "Condiciones Especiales". En caso de necesitar el usuario mayor financiamiento, el excedente deberá canalizarlo por otra línea de crédito.

PROPORCION DEL APOYO

Hasta el CIENTO POR CIENTO (100%) del valor de compra o tasación, de ambos el menor, incluido el Impuesto al Valor Agregado (I.V.A.), sin superar el monto máximo establecido precedentemente.

PLAZO

El plazo total de los créditos a bonificar no podrá exceder los SESENTA (60) meses. Debe tenerse presente que, como norma general, el plazo de las operaciones deberá ser inferior a la vida útil estimada de los bienes que se financien, y debe surgir de la capacidad de pago de la empresa.

DESEMBOLSOS

Cuando la inversión lo justifique se podrá aceptar un máximo de hasta TRES (3) desembolsos, incluido anticipo, conforme el avance de obra o proyecto, a determinar por EL BANCO.

El plazo máximo entre el primer y último desembolso no podrá exceder los SEIS (6) meses, ni la fecha máxima para contabilizar operaciones.

El plazo máximo se computará a partir del primer desembolso.

REGIMEN DE AMORTIZACION

En todos los casos se liquidará mediante el sistema alemán. La periodicidad del pago de las amortizaciones de capital se pactarán preferentemente en cuotas mensuales. Sólo en casos de excepción fundamentada podrán admitirse amortizaciones trimestrales.

El pago de intereses se producirá con una periodicidad igual o menor que la convenida para la amortización del capital, a solo juicio de la instancia crediticia.

PERIODO DE GRACIA

Hasta ONCE (11) meses, contados a partir del primer desembolso, incluidos en el plazo de la operación. El vencimiento de la primera cuota de amortización tendrá lugar al mes o trimestre posterior a la fecha de finalización del período de gracia no debiendo superar, dicho vencimiento, el término de UN (1) año.

En ningún caso habrá período de gracia para el pago de intereses.

En casos de desembolsos múltiples, los intereses que devengan cada uno de ellos deberán ser cancelados con una periodicidad igual o menor que la pactada (mensual o trimestral). A la fecha del último desembolso los intereses anteriormente mencionados deberán estar cancelados.

INTERES

1. Regirá la tasa según destino y región:

1.1. La tasa de interés de los créditos a otorgar en el marco de LA LINEA, será fija durante los primeros CINCO (5) años del crédito.

1.2. La tasa nominal anual a aplicar será la de la Reglamentación N° 400 según destino, manteniendo las bonificaciones del BANCO por zonas geográficas.

2. Bonificación a cargo de la SECRETARIA DE LA PEQUEÑA Y MEDIANA EMPRESA Y DESARROLLO REGIONAL:

2.1 Adicionalmente a las reducciones de la tasa que eventualmente aplique EL BANCO, la citada Secretaría tomará a su cargo la siguiente bonificación de tasa:

Para todos los beneficiarios rige una bonificación de SEIS (6) puntos porcentuales anuales en la tasa de interés de LA LINEA.

2.2. Se producirá el cese inmediato de la bonificación de la tasa de interés de cada préstamo cuando:

2.2.1. Se produzca el incumplimiento, por parte del usuario, del pago de la cuota del crédito otorgado por EL BANCO. En caso de que esta situación se regularice dentro del término máximo de NOVENTA (90) días, la SECRETARIA DE LA PEQUEÑA Y MEDIANA EMPRESA Y DESARROLLO REGIONAL bonificará los importes como si la mora no hubiera ocurrido.

2.2.2. Concurso o quiebra del usuario.

2.2.3. Inicio de acciones judiciales o extrajudiciales exigidas o no como requisito necesario para la tramitación de las primeras, de cobro al tomador del préstamo.

2.2.4. Cancelación anticipada del préstamo.

2.2.5. Refinanciación del préstamo.

3. En caso de mora o en los casos previstos en "Interés - Punto 2.2.2", "Interés - Punto 2.2.3" e "Interés - Punto 2.2.5", EL BANCO aplicará sobre las cuotas impagas y desde el último vencimiento abonado, la tasa activa de cartera general para operaciones en Pesos, más los punitivos correspondientes.

Todo beneficiario que atienda una cuota con atraso, deberá abonar por el período de atraso los intereses correspondientes calculados con la tasa de cartera general, más punitivos.

4. No cursarán por LA LINEA operaciones que correspondan a créditos con tasas bonificadas por otros regímenes, cualquiera sean éstos, y su ámbito (nacional, provincial o municipal).

GARANTIAS

A satisfacción del BANCO, aplicándose lo dispuesto en la "Normas Específicas sobre Garantías - Reglamentación N° 246".

SEGUROS

1. Cobertura de vida: Si el titular es una persona física, es requisito para acceder a estos préstamos que el mismo disponga de seguro de vida a favor del BANCO por el saldo de la deuda, que cubra las eventuales incobrabilidades por fallecimiento del mismo.

2. Sobre bienes en garantía: en la forma de práctica.

COMISION POR CONSTITUCION Y CONTROL DE GARANTIAS

Se establece según los siguientes valores fijos que se aplicarán sobre los saldos deudores, en forma adelantada y por período semestral, a saber:

Saldo Deudor	Comisión
Hasta \$ 100.000	\$ 500
\$ 100.001 - 300.000	\$ 1.600
\$ 300.001 - 500.000	\$ 3.200
\$ 500.001 - 700.000	\$ 4.200
\$ 700.001 - 900.000	\$ 5.600
\$ 900.001 - 1.100.000	\$ 6.650
\$ 1.100.001 - 1.400.000	\$ 8.750
\$ 1.400.001 - 1.500.000	\$ 10.850

Esta comisión absorbe los gastos por tasaciones, valuaciones y control de las garantías, excluyéndose honorarios y gastos relacionados con la creación del derecho real de la garantía.

No se percibirá esta comisión cuando se trate de operaciones avaladas por GARANTIZAR S.G.R.

COMISION DE ADMINISTRACION DE PRESTAMOS (REGLAMENTACION N° 10):

No se percibirá.

OTRAS CONDICIONES

1. En la instrumentación de las operaciones, los beneficiarios deberán aceptar que:

1.1. La bonificación de la tasa de interés que se determina en esta operatoria sólo tendrá efectos si la SECRETARIA DE LA PEQUEÑA Y MEDIANA EMPRESA Y DESARROLLO REGIONAL afronta los pagos correspondientes. En caso contrario los beneficiarios deberán soportar la tasa de interés sin bonificación.

1.2. Tanto EL BANCO como la SECRETARIA DE LA PEQUEÑA Y MEDIANA EMPRESA Y DESARROLLO REGIONAL tienen amplias facultades para verificar la correcta y efectiva aplicación de los fondos al destino previsto en EL PROGRAMA.

2. En la instrumentación de las operaciones, se deberá consignar que la tasa de interés está bonificada por la SECRETARIA DE LA PEQUEÑA Y MEDIANA EMPRESA Y DESARROLLO REGIONAL.

3. En todos los casos los solicitantes deberán tramitar ante la SUBSECRETARIA DE PROMOCION AL FINANCIAMIENTO DE LA PEQUEÑA Y MEDIANA EMPRESA, una constancia de elegibilidad que los habilite para tramitar sus créditos en EL BANCO. Una vez recibida la notificación de dicha Subsecretaría, EL BANCO procederá a su evaluación y a determinar si su riesgo es asumible.

Los aspectos no contemplados en el presente Reglamento serán considerados puntualmente para cada caso mediante elevación al Directorio de EL BANCO.

4. El informe requerido en el punto Destino para inversiones para riego deberá ser elaborado por un geólogo ó profesional con incumbencia en el tema (cualquiera de ellos habilitados) y especificará entre otros conceptos: profundidad de la napa, capacidad hídrica y calidad de la misma, ó de la fuente de agua de que se trata. Asimismo, se requiere del profesional interviniente un informe acerca de la existencia de regulaciones provinciales ó de otra índole para el uso de la fuente de agua de que se trate y de existir, su cumplimiento.

PLAZO MAXIMO PARA DESEMBOLSAR OPERACIONES

Hasta el vencimiento de LA LINEA (Reglamentación N° 400), hasta el día 31 de diciembre de 2015, o hasta agotar el cupo máximo asignado para esta operatoria, lo que ocurra primero.

ENDEUDAMIENTO DE LOS USUARIOS

Rigen las normas "Administración del Crédito".

LIMITES DE CARTERA

Serán solicitados en la forma de práctica, indicando el presente destino.

e. 02/09/2013 N° 67533/13 v. 02/09/2013

MINISTERIO DEL INTERIOR Y TRANSPORTE**DIRECCION NACIONAL ELECTORAL****SUBDIRECCION NACIONAL ELECTORAL****Disposición N° 245/2013**

Bs. As., 28/8/2013

VISTO el Expediente N° S02:0107888/2013 del registro de este Ministerio, la Ley N° 26.571 y el Decreto N° 760 de 17 de junio de 2013, y

CONSIDERANDO:

Que las normas precitadas establecen que la DIRECCION NACIONAL ELECTORAL dará a conocer el listado preliminar de servicios de comunicación audiovisual confeccionado por la AUTORIDAD FEDERAL DE SERVICIOS DE COMUNICACION AUDIOVISUAL (AFSCA), el cual se pondrá en conocimiento de las agrupaciones políticas a los efectos de que verifiquen la integridad del mismo y formulen las observaciones que estimen pertinentes.

Que, asimismo, se establece que la DIRECCION NACIONAL ELECTORAL, realizará un sorteo público de asignación de espacios de publicidad electoral en los servicios de comunicación audiovisual.

Que resulta conveniente fijar las fechas y hacer público el cronograma correspondiente a estas actividades.

Que el presente acto se dicta en virtud de las atribuciones conferidas por los artículos 2°, 4°, 15 y 37 del Decreto N° 760 del 17 de junio de 2013.

Por ello,

EL SUBDIRECTOR NACIONAL ELECTORAL
DISPONE:

ARTICULO 1° — Fijase como fecha para el sorteo de asignación de espacios para publicidad electoral, el día 13 de septiembre de 2013, a las 12:00 horas, en el "Salón Presidente" del MINISTERIO DEL INTERIOR Y TRANSPORTE sito en la calle 25 de Mayo N° 145, piso 2°, de la Ciudad Autónoma de Buenos Aires.

ARTICULO 2° — Invítese, a los apoderados de las Agrupaciones Políticas a presenciar el sorteo.

ARTICULO 3° — La Dirección de Campañas Electorales de la DIRECCION NACIONAL ELECTORAL arbitrará los medios para la notificación de los resultados del sorteo a los servicios de

comunicación audiovisual y a las agrupaciones políticas, sin perjuicio de lo establecido en el tercer párrafo del artículo 15 del Decreto N° 760 del 17 de junio de 2013.

ARTICULO 4° — Apruébese el cronograma que como Anexo I, forma parte integrante de la presente.

ARTICULO 5° — Hágase saber la presente medida a la AUTORIDAD FEDERAL DE SERVICIOS DE COMUNICACION AUDIOVISUAL (AFSCA), a la UNIDAD DE AUDITORIA INTERNA de la Jurisdicción y a la SINDICATURA GENERAL DE LA NACION e invítese a sus titulares a presenciar el sorteo dispuesto en el artículo 1°.

ARTICULO 6° — Comuníquese, publíquese, dése a la DIRECCION NACIONAL DEL REGISTRO OFICIAL y archívese. — Lic. ESTEBAN DI SIBIO, Subdirector Nacional Electoral, Dirección Nacional Electoral, Ministerio del Interior y Transporte.

ANEXO I

29/08/2013	PUBLICACION DEL LISTADO PRELIMINAR DE SERVICIOS DE COMUNICACION AUDIOVISUAL
07/09/2013	FIN PLAZO PARA REALIZAR OBSERVACIONES AL LISTADO PRELIMINAR
12/09/2013	FIN PLAZO PARA RESOLVER OBSERVACIONES Y PUBLICAR EL LISTADO DEFINITIVO DE SERVICIOS DE COMUNICACION AUDIOVISUAL
13/09/2013	REALIZACION DEL SORTEO PUBLICO DE ASIGNACION DE ESPACIOS
13/09/2013	PUBLICACION DEL RESULTADO DEL SORTEO
13/09/2013	COMUNICACION DEL RESULTADO DEL SORTEO

e. 02/09/2013 N° 67378/13 v. 02/09/2013

MINISTERIO DEL INTERIOR Y TRANSPORTE**DIRECCION NACIONAL ELECTORAL****SUBDIRECCION NACIONAL ELECTORAL****Disposición N° 246/2013**

Bs. As., 28/8/2013

VISTO el Expediente N° S02:0107854/2013 del registro de este Ministerio y el artículo 4° del Decreto N° 760 del 17 de junio de 2013, y

CONSIDERANDO:

Que la norma citada en el Visto encomienda a la Dirección de Campañas Electorales de esta DIRECCION NACIONAL ELECTORAL, la confección de un listado preliminar de servicios de comunicación audiovisual en condiciones de emitir anuncios de publicidad electoral.

Que corresponde poner en conocimiento de las agrupaciones políticas, y/o los titulares de los servicios de comunicación audiovisual y de la Justicia Nacional Electoral el referido listado preliminar a los efectos que los primeros formulen observaciones al mismo respecto de la omisión, incorporación o exclusión de servicios que no aparecieran hasta los DIEZ (10) días siguientes al de la publicación.

Que, consecuentemente, corresponde comunicar que la información pertinente está disponible en la página web de esta DIRECCION NACIONAL ELECTORAL, y la forma de efectuar las observaciones a que hace referencia el Decreto N° 760 del 17 de junio de 2013.

Que ha tomado la intervención que le compete la DIRECCION GENERAL DE ASUNTOS JURIDICOS de este Ministerio.

Que la presente se funda en las atribuciones conferidas por los artículos 4° y 37 del Decreto N° 760 del 17 de Junio de 2013.

Por ello,

EL SUBDIRECTOR NACIONAL ELECTORAL
DISPONE:

ARTICULO 1° — Publicar el listado preliminar de señales de alcance nacional y de servicios de comunicación audiovisual de cada distrito en el sitio web www.elecciones.gob.ar.

ARTICULO 2° — Instruir a la Dirección de Campañas Electorales para que remita a la Secretaría de Actuación Judicial de la Excm. CAMARA NACIONAL ELECTORAL copia certificada de los listados preliminares a que hace referencia el artículo precedente, en forma impresa y en soporte electrónico.

ARTICULO 3° — Las agrupaciones políticas y/o los titulares de los servicios de comunicación audiovisual podrán efectuar observaciones a los listados por correo electrónico a dce@mininterior.gov.ar o por vía postal a Dirección de Campañas Electorales, 25 de Mayo 101, piso 3°, oficina N° 338, Ciudad Autónoma de Buenos Aires, hasta el día 7 de septiembre del corriente año inclusive, para lo cual se habilita este último administrativamente.

ARTICULO 4° — Las observaciones consisten en la comunicación al citado organismo de la omisión, incorporación o exclusión de servicios y deberán indicar distrito, razón social, tipo de servicio, frecuencia y toda información que permita su identificación. Las observaciones deberán ser suscriptas por los apoderados de las agrupaciones políticas y/o los titulares de los servicios de comunicación audiovisual.

ARTICULO 5° — Comuníquese, publíquese, dése a la DIRECCION NACIONAL DEL REGISTRO OFICIAL y archívese. — Lic. ESTEBAN DI SIBIO, Subdirector Nacional Electoral, Dirección Nacional Electoral, Ministerio del Interior y Transporte.

e. 02/09/2013 N° 67379/13 v. 02/09/2013

Separatas de Legislación

LEY DE CONTRATO DE TRABAJO

- Ley 20.744
- Texto Actualizado
- Normas Modificatorias y Complementarias



\$43

BOLETIN OFICIAL
DE LA REPUBLICA ARGENTINA

www.boletinoficial.gob.ar 0810-345-BORA (2672) atencionalcliente@boletinoficial.gob.ar

Ventas / Ciudad Autónoma de Buenos Aires

Sede Central: Suipacha 767 (09:30 a 16:00 hs.) Tel.: (011) 5218-8400 // **Delegación Tribunales:** Libertad 469 (8:30 a 14:30 hs.) Tel.: (011) 4379-1979 // **Delegación Colegio Público de Abogados:** Av. Corrientes 1441. Entrepiso (10:00 a 15:45 hs.) Tel.: (011) 4379-8700 (int. 236) // **Delegación Consejo Profesional de Ciencias Económicas:** Viamonte 1549. Planta Baja (12:00 a 17:00 hs.) Tel.: (011) 5382-9535.

AVISOS OFICIALES

Anteriores



MINISTERIO DE SALUD

DIRECCION NACIONAL DE REGISTRO, FISCALIZACION Y SANIDAD DE FRONTERAS

MINISTERIO DE SALUD, conforme a lo dispuesto por el artículo 49 de la Ley N° 17.565 y atento a la imposibilidad de ubicarlo, por el presente se cita al Sr. Gastón Javier Sarubbi, DNI 23.102.432, para que en el plazo de DIEZ (10) días a contar del quinto de esta publicación, comparezca ante el DEPARTAMENTO DE FALTAS SANITARIAS de la DIRECCION DE SUMARIOS del MINISTERIO DE SALUD sito en la Av. 9 de Julio 1925, Piso 3, CAPITAL FEDERAL en el horario de 09:30 a 17:30 a los efectos de tomar vista del Expediente N° 12002-15468-07-8 para posteriormente formular descargo y ofrecer la prueba que haga al derecho de su defensa por la presunta infracción a la Ley 17.565 en que habría incurrido bajo APERCIBIMIENTO, en caso de incomparecencia, de juzgarlo en rebeldía. — Dr. MARIO A. ROSENFELD, Dirección Nacional de Registro, Fiscalización y Sanidad de Fronteras.

e. 29/08/2013 N° 66280/13 v. 02/09/2013

MINISTERIO DE SALUD

DIRECCION NACIONAL DE REGISTRO, FISCALIZACION Y SANIDAD DE FRONTERAS

MINISTERIO DE SALUD. Conforme lo dispuesto por el art. 131 párrafo 2 de la Ley 17.132 y atento a la imposibilidad de ubicarlo, por el presente se cita al odontólogo Richard Nilton Gonzales Balderas para que en el plazo de DIEZ (10) días a contar del quinto de esta publicación, comparezca ante el DEPARTAMENTO DE FALTAS SANITARIAS de la DIRECCION DE SUMARIOS del MINISTERIO DE SALUD sito en la Av. 9 de Julio 1925, Piso 3, CAPITAL FEDERAL en el horario de 09:30 a 17:30 a los efectos de tomar vista del Expediente N° 12002-10961-08-6 para posteriormente formular descargo y ofrecer la prueba que haga al derecho de su defensa por la presunta infracción a los arts. 29 inc. 3 de la Ley 17.132 y art. 35 del Decreto Reglamentario 6216/67 en que habría incurrido bajo APERCIBIMIENTO, en caso de incomparecencia, de juzgarlo en rebeldía. — Dr. MARIO A. ROSENFELD, Dirección Nacional de Registro, Fiscalización y Sanidad de Fronteras.

e. 29/08/2013 N° 66281/13 v. 02/09/2013

MINISTERIO DE DESARROLLO SOCIAL

INSTITUTO NACIONAL DE ASOCIATIVISMO Y ECONOMIA SOCIAL

El INSTITUTO NACIONAL DE ASOCIATIVISMO Y ECONOMIA SOCIAL notifica que por Resoluciones N°s.: 2.613; 2.614; 2.615; 2.616; 2.617; 2.618; 2.619/13-INAES, ha resuelto CANCELAR la matrícula correspondiente a las siguientes mutuales: ASOCIACION MUTUAL PARTENON DE SERVICIOS PARA LA VIVIENDA (m. 1.731); ASOCIACION MUTUAL DE LOS VENDEDORES DE DIARIOS Y REVISTAS DE CAPITAL FEDERAL (m. 637); ASOCIACION MUTUAL DE LOS TRABAJADORES DE LAS AGENCIAS HIPICAS (m. 786); MUTUAL ARGENTINA DE PRESTACIONES Y SERVICIOS (m. 1.671); UNION ARGENTINA DE KICK BOXING ASOCIACION MUTUAL (m. 2.351); ASOCIACION MUTUAL "SAN EXPEDITO" (m. 2.671); ASOCIACION MUTUAL "NUEVA SOCIEDAD" (m. 2.076). Las entidades citadas precedentemente tienen el domicilio legal en la Ciudad Autónoma de Buenos Aires. Y por Resolución N° 2.620/13-INAES, a la MUTUAL AMPLIACION 23 DE ABRIL (m. 669), con domicilio legal en la Provincia de Córdoba. Contra la medida dispuesta son oponible los siguientes Recursos: REVISION (Art. 22, inc. a) —10 días— y Art. 22, incs. b), c) y d) —30 días— Ley N° 19.549). RECONSIDERACION (Art. 84, Dto. N° 1.759/72 - t.o. 1.991, —10 días—). JERARQUICO (Art. 89, Dto. N° 1.759/72 - t.o. 1.991, —15 días—. Y ACLARATORIA (Art. 102, Dto. N° 1.759/72 - t.o. 1.991, —5 días—). Asimismo, en razón de la distancia, se le concede un plazo ampliatorio de CUATRO (4) días a la entidad ubicada en la Provincia de Córdoba. Quedan debidamente notificadas (Art. 42, Dto. N° 1.759/72 (t.o. 1.991). — OSVALDO A. MANSILLA, Coordinador Financiero Contable, INAES.

e. 29/08/2013 N° 66364/13 v. 02/09/2013

CONVENCIONES COLECTIVAS DE TRABAJO



MINISTERIO DE TRABAJO, EMPLEO Y SEGURIDAD SOCIAL

DIRECCION NACIONAL DE RELACIONES DEL TRABAJO

Disposición N° 576/2013

Registro N° 774/2013

Bs. As., 1/8/2013

VISTO el Expediente N° 96.108/13 del Registro del MINISTERIO DE TRABAJO, EMPLEO Y SEGURIDAD SOCIAL, la Ley N° 14.250 (t.o. 2004), la Ley N° 20.744 (t.o. 1976) y sus modificatorias, y

CONSIDERANDO:

Que a fojas 44/45 del Expediente de referencia, obra el Acuerdo celebrado ante esta Autoridad de Aplicación entre el SINDICATO DEL PERSONAL JERARQUICO Y PROFESIONAL DEL PETRO-

LEO Y GAS PRIVADO DE NEUQUEN Y RIO NEGRO y la empresa CHEVRON ARGENTINA SOCIEDAD DE RESPONSABILIDAD LIMITADA, conforme a lo establecido en la Ley N° 14.250 (t.o. 2004).

Que mediante dicho acuerdo, las partes convienen reajustar la remuneración de ciertos trabajadores en el marco del Convenio Colectivo de Trabajo N° 637/11, conforme surge de las planillas y detalles que surgen agregadas a fojas 26/35 de autos.

Que en el mismo sentido, establecen reajustar las remuneraciones de otros tres trabajadores allí enunciados, en base a las sumas estipuladas en el presente.

Que corresponde hacer saber a las partes que en el caso de proceder al dictado de un acto administrativo por parte de esta Autoridad, será de registración del presente como acuerdo marco de carácter colectivo y sin perjuicio de los derechos individuales de los trabajadores involucrados.

Que los agentes negociales ratifican el contenido y firmas insertas en el acuerdo traído a estudio, acreditando su personería y facultades para negociar colectivamente con las constancias obrantes en autos.

Que asimismo se acreditan los recaudos formales establecidos por la Ley N° 14.250 (t.o. 2004).

Que por lo expuesto, corresponde dictar el pertinente acto administrativo, de conformidad con los antecedentes mencionados.

Que las facultades de la suscripta para dictar la presente surgen de lo dispuesto por el Decreto N° 738/12.

Por ello,

LA DIRECTORA NACIONAL
DE RELACIONES DEL TRABAJO
DISPONE:

ARTICULO 1° — Declárese registrado el Acuerdo celebrado entre el SINDICATO DEL PERSONAL JERARQUICO Y PROFESIONAL DEL PETROLEO Y GAS PRIVADO DE NEUQUEN Y RIO NEGRO y la empresa CHEVRON ARGENTINA SOCIEDAD DE RESPONSABILIDAD LIMITADA, obrante a fojas 44/45 del Expediente N° 96.108/13.

ARTICULO 2° — Regístrese la presente Disposición por medio de la Dirección General de Registro, Gestión y Archivo Documental dependiente de la SUBSECRETARIA DE COORDINACION. Cumplido, pase a la Dirección de Negociación Colectiva, a fin que el Departamento Coordinación registre el Acuerdo de fojas 44/45 del Expediente N° 96.108/13.

ARTICULO 3° — Remítase copia debidamente autenticada de la presente Disposición al Departamento Biblioteca para su difusión.

ARTICULO 4° — Notifíquese a las partes signatarias. Cumplido, procedase a la guarda del presente legajo.

ARTICULO 5° — Hágase saber que en el supuesto que este MINISTERIO DE TRABAJO, EMPLEO Y SEGURIDAD SOCIAL no efectúe la publicación gratuita del Acuerdo y de esta Disposición, las partes deberán proceder de acuerdo a lo establecido en el Artículo 5° de la Ley N° 14.250 (t.o. 2004).

ARTICULO 6° — Comuníquese, publíquese, dése a la Dirección Nacional del Registro Oficial y archívese. — Dra. SILVIA SQUIRE DE PUIG MORENO, Directora Nacional de Relaciones del Trabajo, Ministerio de Trabajo, Empleo y Seguridad Social.

Expediente N° 96.108/13

Buenos Aires, 5 de agosto de 2013

De conformidad con lo ordenado en la DISPOSICION DNRT N° 576/13, se ha tomado razón del acuerdo obrante a fojas 44/45 del expediente de referencia, quedando registrado bajo el número 774/13. — VALERIA A. VALETTI, Registro de Convenios Colectivos, Departamento Coordinación — D.N.R.T.

Expediente N° 96.108/13

En la Ciudad Autónoma de Buenos Aires a los 13 días del mes de junio de dos mil trece a las 13 horas, comparecen en el MINISTERIO DE TRABAJO, EMPLEO Y SEGURIDAD SOCIAL - ante mí Dr. MAURICIO J. RIAFRECHA VILLAFANE, Analista Superior de Relaciones Laborales; el Sr. IGNACIO URBIETA por la firma CHEVRON ARGENTINA S.R.L. por una parte y, por la otra, lo hacen el Sr. MANUEL AREVALO, OMAR SOTO y RUBEN MALUENDA, asistidos por el Dr. JUAN PABLO CAPON FILAS por el SINDICATO DE PERSONAL JERARQUICO Y PROFESIONAL DEL PETROLEO Y GAS PRIVADO DE RIO NEGRO, NEUQUEN Y LA PAMPA, quienes asisten al presente acto.

Declarado abierto el acto por el funcionario actuante, luego de un intercambio de opiniones, las partes llegan al siguiente acuerdo, solicitando a la autoridad administrativa su homologación:

I.- Las partes acuerdan reajustar la remuneración de los trabajadores por aplicación del art. 63 del CCT 637/2011, a partir del mes de julio de 2013, por los montos que resultan de las planillas agregadas por la representación empleadora en la audiencia del 30 de mayo de 2013.

Asimismo, las partes acuerdan reajustar de idéntica forma, las remuneraciones de los señores Aladino Vejar, Martín Spadafora, y Esteban Ojeda, por las sumas de \$ 26.400 mensuales para cada uno de éstos.

II. La representación empresaria y la parte sindical acuerdan el pago de un retroactivo, en un solo pago, pagadero hasta el cuarto día hábil de agosto de 2013, a los trabajadores que resultan de las planillas agregadas por la representación empleadora en la audiencia del 30 de mayo de 2013, por el valor indicado en dichas planillas con más el reajuste correspondiente al mes de junio de 2013 y pagar asimismo en idéntica forma el retroactivo que correspondiere a los trabajadores Aladino Vejar, Martín Spadafora y Esteban Ojeda.

III.- A los efectos de instrumentar el pago del retroactivo, las partes y los empleadores contratistas de Chevron S.R.L. suscribirán los acuerdos correspondientes con la conformidad expresa de cada trabajador, ante la Subsecretaría de Trabajo de la Provincia del Neuquén.

No siendo para más, se da por finalizado el acto previa lectura y ratificación por ante mí que certifico firman los comparecientes.

MINISTERIO DE TRABAJO, EMPLEO Y SEGURIDAD SOCIAL**DIRECCION NACIONAL DE RELACIONES DEL TRABAJO****Disposición N° 597/2013****Registro N° 783/2013**

Bs. As., 5/8/2013

VISTO el Expediente N° 1.570.391/13 del Registro del MINISTERIO DE TRABAJO, EMPLEO Y SEGURIDAD SOCIAL, la Ley N° 14.250 (t.o. 2004), la Ley N° 20.744 (t.o. 1976) y sus modificatorias, y

CONSIDERANDO:

Que a fojas 2/5 del Expediente N° 1.570.391/13 obra el Acuerdo celebrado por la UNION FERROVIARIA, por la parte sindical, y FERROSUR ROCA SOCIEDAD ANONIMA, por la parte empresarial, conforme a lo dispuesto en la Ley de Negociación Colectiva N° 14.250 (t.o. 2004).

Que bajo dicho acuerdo las precitadas partes incorporan dentro del ámbito del Convenio Colectivo de Trabajo de Empresa N° 710/05 "E" el puesto denominado "Operador de Plantas", conforme surge de los términos y contenido del texto.

Que el ámbito de aplicación del presente acuerdo se corresponde con la actividad principal de la parte empleadora signataria y la representatividad de la entidad sindical firmante, emergente de su personería gremial.

Que una vez dictado el presente acto administrativo homologando el acuerdo alcanzado, se procederá a remitir estas actuaciones a la Dirección Nacional de Regulaciones del Trabajo, a fin de evaluar la procedencia de efectuar el pertinente Proyecto de Base Promedio y Tope Indemnizatorio, de conformidad a lo establecido en el Artículo 245 de la Ley N° 20.744 (t.o. 1976) y sus modificatorias.

Que asimismo se acreditan los recaudos formales exigidos por la Ley N° 14.250 (t.o. 2004).

Que la Asesoría Legal de la Dirección Nacional de Relaciones del Trabajo de este Ministerio tomó la intervención que le compete.

Que de la lectura de las cláusulas pactadas, no surge contradicción con la normativa laboral vigente.

Que las partes acreditan la representación que invocan ante esta Cartera de Estado y ratifican en todos sus términos el mentado acuerdo.

Que por lo expuesto, corresponde dictar el pertinente acto administrativo de homologación, de conformidad con los antecedentes mencionados.

Que las facultades de la suscripta para resolver en las presentes actuaciones, surgen de las atribuciones otorgadas por el Decreto N° 738/12.

Por ello,

LA DIRECTORA NACIONAL
DE RELACIONES DEL TRABAJO
DISPONE:

ARTICULO 1° — Declárase homologado el Acuerdo celebrado por la UNION FERROVIARIA, por la parte sindical, y FERROSUR ROCA SOCIEDAD ANONIMA, por la parte empresarial, obrante a fojas 2/5 del Expediente N° 1.570.391/13, conforme a lo dispuesto en la Ley de Negociación Colectiva N° 14.250 (t.o. 2004).

ARTICULO 2° — Regístrese la presente Disposición por medio de la Dirección General de Registro, Gestión y Archivo Documental dependiente de la SUBSECRETARIA DE COORDINACION. Cumplido, pase a la Dirección de Negociación Colectiva a fin de que el Departamento Coordinación registre el Acuerdo obrante a fojas 2/5 del Expediente N° 1.570.391/13.

ARTICULO 3° — Remítase copia debidamente autenticada al Departamento Biblioteca para su difusión.

ARTICULO 4° — Notifíquese a las partes signatarias. Posteriormente pase a la Dirección Nacional de Regulaciones del Trabajo, a fin de evaluar la procedencia de efectuar el Proyecto de Base Promedio y Tope Indemnizatorio, de las escalas salariales que por este acto se homologan y de conformidad a lo establecido en el Artículo 245 de la Ley N° 20.744 (t.o. 1976) y sus modificatorias. Finalmente procédase a la guarda del presente legajo conjuntamente con el Convenio Colectivo de Trabajo de Empresa N° 710/05 "E".

ARTICULO 5° — Hágase saber que en el supuesto que este MINISTERIO DE TRABAJO, EMPLEO Y SEGURIDAD SOCIAL no efectúe la publicación de carácter gratuito del Acuerdo homologado y de esta Disposición, las partes deberán proceder de acuerdo a lo establecido en el Artículo 5 de la Ley N° 14.250 (t.o. 2004).

ARTICULO 6° — Comuníquese, publíquese, dése a la Dirección Nacional del Registro Oficial y archívese. — Dra. SILVIA SQUIRE DE PUIG MORENO, Directora Nacional de Relaciones del Trabajo, Ministerio de Trabajo, Empleo y Seguridad Social.

Expediente N° 1.570.391/13

Buenos Aires, 07 de Agosto de 2013

De conformidad con lo ordenado en la DISPOSICION DNRT N° 597/13, se ha tomado razón del acuerdo obrante a fojas 2/5 del expediente de referencia, quedando registrado bajo el número 783/13. — VALERIA A. VALETTI, Registro de Convenios Colectivos, Departamento Coordinación - D.N.R.T.

En la Ciudad Autónoma de Buenos Aires, a los trece días del mes de junio de 2013, se reúnen, por una parte la UNION FERROVIARIA, con domicilio en Avenida Independencia 2880, de esta ciudad, en adelante, indistintamente "UF" o "el Gremio", representada por los señores Néstor País en su función de Secretario de Administración y Germán Grandi como Delegado del Personal, con el asesoramiento letrado del Dr. José Gutiérrez; y por la otra la empresa FERROSUR ROCA S.A., representada por el señor Rubén O. Carboni, con domicilio en Reconquista 1088, 5° piso de esta ciudad, con el asesoramiento letrado del Dr. Carlos A. Sánchez Obertello, en adelante, indistintamente, "LA EMPRESA" o "FERROSUR" o "FSR", y en conjunto, en adelante, "LAS PARTES", las

que luego de haber mantenido una serie de reuniones al respecto, convienen celebrar el presente acuerdo, manifestando previamente:

- Que en función de las características de las tareas prestadas por los trabajadores representados por UF en distintas instalaciones del cliente "Loma Negra" ubicadas en los subpatios planta Loma Negra y planta L'Amali, del Partido de Olavarría, Provincia de Buenos Aires, con fecha 3 de junio de 2010, LAS PARTES celebraron un acuerdo (en adelante, "EL ACUERDO"), a cuyo contenido se remiten.

- Que a lo largo del tiempo transcurrido desde la celebración de EL ACUERDO hasta la fecha, se han ido produciendo modificaciones en las modalidades de las tareas prestadas por los trabajadores involucrados.

- Que en virtud de esos cambios en la prestación de las tareas, LAS PARTES consideran necesario y conveniente, junto con su correspondiente descripción, fusionarlas en un único nuevo puesto a crearse al que habrá de asignársele la pertinente Categoría Laboral.

- Que el puesto que se crea y la Categoría que se le asigna corresponde incorporarlos dentro del marco del convenio colectivo de trabajo de empresa actualmente vigente (CCT "E" 710/05, en adelante CCT), dentro de la Sección Tráfico (Transporte).

- Que esa Categoría corresponderá sólo a los trabajadores alcanzados por EL ACUERDO que efectivamente presten las tareas con las modalidades que corresponden al nuevo puesto.

- Que paralelamente corresponde asignarle una denominación o título al puesto que se crea por el presente.

- Que las tareas son prestadas en la actualidad, en forma indistinta, en los subpatios planta Loma Negra y planta L'Amali, ubicados en el Partido de Olavarría, Provincia de Buenos Aires.

- Que las tareas prestadas por los trabajadores que se desempeñan en el puesto que se crea, se caracterizan por su diversidad.

- Que al día de la fecha los trabajadores alcanzados por EL ACUERDO, que ocuparán el puesto que se crea, tienen diferentes categorías laborales en el CCT, inferiores a la Categoría que se crea.

- Que a esos trabajadores se les reconoció un adicional denominado "Adicional Multifunción", según lo estipulado oportunamente en EL ACUERDO.

- Que el presente convenio sustituye y reemplaza a EL ACUERDO.

- Que en función y como consecuencia de lo antedicho, el adicional "Multifunción" en planta Loma Negra y planta L'Amali pierde virtualidad.

En virtud de lo manifestado precedentemente, lo que forma parte del presente acuerdo, LAS PARTES convienen:

CLAUSULA PRIMERA: Dentro del ámbito del CCT "E" 710/05 se incorpora el puesto denominado "Operador de Plantas" al que se le asigna la Categoría Laboral o Nivel "E1" que se crea por el presente, dentro de la Sección Tráfico (Transporte).

CLAUSULA SEGUNDA: La Descripción de Tareas que corresponde al "Operador de Plantas" es la que se consigna en el Anexo I y que forma parte del presente convenio. Las tareas detalladas lo son a título enunciativo, quedando asimismo incluidas dentro de las tareas a realizar, las accesorias y conexas a las mismas, y todas aquellas que, apreciadas bajo el principio de la buena fe, sean propias del puesto.

CLAUSULA TERCERA: Las tareas correspondientes al "Operador de Plantas" son las prestadas en la actualidad, en forma indistinta, en los subpatios planta Loma Negra y planta L'Amali, ubicado en el Partido de Olavarría, Provincia de Buenos Aires.

CLAUSULA CUARTA: Se conviene que la nueva Categoría que se crea por la cláusula precedente:

a) tendrá un salario básico de \$ 7.694,00 (pesos siete mil seiscientos noventa y cuatro);

b) sólo le corresponderá a los trabajadores alcanzados por EL ACUERDO que efectivamente presten las tareas de "Operador de Plantas" descriptas en el Anexo I.

CLAUSULA QUINTA: A partir de su entrada en vigencia, el presente convenio sustituye y reemplaza a EL ACUERDO. En virtud de ello los trabajadores alcanzados por EL ACUERDO que pasarán a desempeñarse como "Operador de Plantas" dejarán de percibir el adicional "Trabajos en Loma Negra" que venían percibiendo.

CLAUSULA SEXTA: Se deja expresa constancia que, a los efectos del cumplimiento de las tareas como "Operador de Plantas", LA EMPRESA estará facultada, en forma indistinta, a asignar a los trabajadores en los subpatios planta Loma Negra y planta L'Amali, ubicados en el Partido de Olavarría, Provincia de Buenos Aires.

CLAUSULA SEPTIMA: El presente acuerdo entrará en vigencia a partir del 1° de julio de 2013, sujeto a la homologación previa del Ministerio de Trabajo, Empleo y Seguridad Social. En caso que la homologación se produjera con posterioridad a la citada fecha, la entrada en vigencia se diferirá al primer día del mes inmediatamente posterior a la de la homologación por el Ministerio de Trabajo, Empleo y Seguridad Social.

CLAUSULA OCTAVA: El pedido de homologación, en forma indistinta, podrá ser requerido por cualquiera de LAS PARTES.

En prueba de conformidad se firman cinco ejemplares de un mismo tenor y a un solo efecto en el lugar y fecha indicados en el encabezamiento.

ANEXO I

Acuerdo UNION FERROVIA-FERROSUR ROCA S.A. - Junio 13, 2013,

Operador de Plantas - Categoría Laboral "E1"- Sección Tráfico (Transporte)

Descripción de tareas

- Coordinar tareas operativas con personal de FSR (Patio Olavarría y CAC) y Planta LN /Lamali.

- Diariamente y en el momento que se le requiera brindar información sobre estado y situación de vagones dentro de planta.

- Efectuar apertura y cierre de vagones.
- Realizar carga y descarga de vagones utilizando las herramientas necesarias para la operación.
- Operación sistemas informáticos de carga y descarga de vagones, correspondientes registros y partes del turno.
- Confeccionar cartas de Porte en forma manual si así lo requiera la planta y otras tareas administrativas si fuera necesario.
- Registro de incidentes y condiciones peligrosas.
- Realizar revisión de trenes, vagones y etiquetado de vagones.
- Formación de trenes en un todo de acuerdo con el R.O.
- Realizar orden y limpieza de los sectores de trabajo e instalaciones donde opera FSR conforme a la metodología 5S.
- Operaciones de manejo de todo tipo de cambios de vías, enganche, desenganche y acoplamiento de vagones.
- Colocar calzas a los vagones.
- Confección del libro de abordó.
- Limpieza y lubricación de cambios del sector.
- Pesaje de vagones.
- Precintado de vagones.
- Utilización como soporte de vibradores de vagones y llave criquet.
- Realizar tareas de eslingado de vagones.
- Realizar limpieza/acondicionamiento interior de vagones si fuera necesario.
- Verificar el buen estado de los pallets, bolsas, etc. del producto y tipo de vagón que se carga e informar cualquier anomalía.

MINISTERIO DE TRABAJO, EMPLEO Y SEGURIDAD SOCIAL

DIRECCION NACIONAL DE RELACIONES DEL TRABAJO

Disposición N° 605/2013

Registros N° 809/2013 y N° 810/2013

Bs. As., 7/8/2013

VISTO el Expediente N° 1.556.012/13 del registro del MINISTERIO DE TRABAJO, EMPLEO Y SEGURIDAD SOCIAL, la Ley N° 14.250 (t.o. 2004), la Ley N° 20.744 (t.o. 1976) y sus modificatorias, y

CONSIDERANDO:

Que a fojas 2, 3/4 y 5/6 del Expediente N° 1.570.338/13, agregado como foja 56 al principal, obran los Acuerdos y Anexo celebrados entre la FEDERACION TRABAJADORES DE INDUSTRIAS DE LA ALIMENTACION, por la parte gremial y la FEDERACION DE INDUSTRIAS DE PRODUCTOS ALIMENTICIOS Y AFINES, por el sector empresarial, conforme a lo establecido en la Ley N° 14.250 (t.o. 2004).

Que a través de los textos convencionales alcanzados, se establece una recomposición salarial y una contribución solidaria y empresaria, dentro de las condiciones allí especificadas.

Que los presentes resultarán de aplicación para el personal comprendido en el Convenio Colectivo de Trabajo N° 244/94.

Que los actores intervinientes en autos se encuentran legitimados para negociar colectivamente, conforme surge de los antecedentes acompañados.

Que los agentes negociales han ratificado el contenido y firmas allí insertas, acreditando la personería y facultades para negociar colectivamente invocadas, con las constancias obrantes en autos.

Que el ámbito de aplicación de los presentes se circunscribe a la correspondencia entre la representatividad que ostenta el sector empleador firmante y la entidad sindical signataria, emergente de su personería gremial.

Que de la lectura de las cláusulas pactadas, no surge contradicción con la normativa laboral vigente.

Que la Asesoría Técnico Legal de esta Dirección Nacional de Relaciones del Trabajo de este Ministerio ha tomado la intervención que le compete.

Que asimismo se acreditan los recaudos formales establecidos por la Ley N° 14.250 (t.o. 2004).

Que se encuentra cumplido el procedimiento negociado previsto en la Ley N° 23.546.

Que en virtud de lo expuesto, correspondería dictar el acto administrativo de homologación de conformidad con los antecedentes mencionados.

Que por último, corresponde que una vez dictado el acto administrativo homologatorio de los Acuerdos de referencia, se remitan estas actuaciones a la Dirección Nacional de Regulaciones del Trabajo, a fin de evaluar la procedencia de elaborar el cálculo del tope previsto por el artículo 245 de la Ley N° 20.744 (t.o. 1976) y sus modificatorias.

Que las facultades de la suscripta para resolver en las presentes actuaciones, surgen de las atribuciones otorgadas por el Decreto N° 738/12.

Por ello,

LA DIRECTORA NACIONAL
DE RELACIONES DEL TRABAJO
DISPONE:

ARTICULO 1° — Decláranse homologados el Acuerdo y Anexo celebrados entre la FEDERACION TRABAJADORES DE INDUSTRIAS DE LA ALIMENTACION y la FEDERACION DE INDUSTRIAS DE PRODUCTOS ALIMENTICIOS Y AFINES, que lucen a fojas 2 y 5/6 del Expediente N° 1.570.338/13, agregado como foja 56 al principal, conforme a lo dispuesto en la Ley de Negociación Colectiva N° 14.250 (t.o. 2004).

ARTICULO 2° — Declárase homologado el Acuerdo celebrado entre la FEDERACION TRABAJADORES DE INDUSTRIAS DE LA ALIMENTACION y la FEDERACION DE INDUSTRIAS DE PRODUCTOS ALIMENTICIOS Y AFINES, que luce a fojas 3/4 del Expediente N° 1.570.338/13, agregado como foja 56 al principal, conforme a lo dispuesto en la Ley de Negociación Colectiva N° 14.250 (t.o. 2004).

ARTICULO 3° — Regístrese la presente Disposición por la Dirección General de Registro, Gestión y Archivo Documental dependiente de la SUBSECRETARIA DE COORDINACION. Cumplido, pase a la Dirección de Negociación Colectiva a fin de que el Departamento Coordinación registre los Acuerdos y Anexo obrantes a fojas 2, 3/4 y 5/6 del Expediente N° 1.570.338/13.

ARTICULO 4° — Remítase copia debidamente autenticada al Departamento Biblioteca para su difusión.

ARTICULO 5° — Notifíquese a las partes signatarias. Posteriormente, pase a la Dirección Nacional de Regulaciones del Trabajo, a fin de evaluar la procedencia de elaborar el Proyecto de Base Promedio y Tope Indemnizatorio, de acuerdo a lo establecido en el Artículo 245 de la Ley N° 20.744 (t.o. 1976) y sus modificatorias. Finalmente, procédase a la guarda del presente legajo conjuntamente con el Convenio Colectivo de Trabajo N° 244/94.

ARTICULO 6° — Hágase saber que en el supuesto de que este MINISTERIO DE TRABAJO, EMPLEO Y SEGURIDAD SOCIAL no efectúe la publicación de carácter gratuito de los Acuerdos y Anexo homologados y de esta Disposición, las partes deberán proceder de acuerdo a lo establecido en el Artículo 5 de la Ley N° 14.250 (t.o. 2004).

ARTICULO 7° — Comuníquese, publíquese, dése a la Dirección Nacional del Registro Oficial y archívese. — Dra. SILVIA SQUIRE DE PUIG MORENO, Directora Nacional de Relaciones del Trabajo, Ministerio de Trabajo, Empleo y Seguridad Social.

Expediente N° 1.556.012/13

Buenos Aires, 12 de agosto de 2013

De conformidad con lo ordenado en la DISPOSICION DNRT N° 605/13, se ha tomado razón del acuerdo obrante a fojas 2 y 5/6 del expediente 1.570.338/13, agregado como fojas 56 al expediente principal, y el acuerdo de fojas 3/4 del expediente 1.570.338/13, agregado como fojas 56 al expediente de referencia, quedando registrados bajo los números 809/13 y 810/13. — VALERIA A. VALETTI, Registro de Convenios Colectivos, Departamento Coordinación - D.N.R.T.

ANEXO A

PLANILLA DE RETRIBUCION BASICAS 2013/2014

ELABORACION, ENVASAMIENTO Y VARIOS	Mayo/Julio de 2013	Agosto/Diciembre de 2013	Enero/Abril de 2014
OPERARIO	28,67	30,39	30,39
OPERARIO GENERAL	29,80	31,58	31,58
OPERARIO CALIFICADO	30,88	32,73	32,73
MEDIO OFICIAL	32,29	34,23	34,23
OFICIAL	35,22	37,32	37,32
OFICIAL GENERAL	37,32	39,55	39,55
OFICIAL CALIFICADO	39,06	41,40	41,40
MANTENIMIENTO			
OPERARIO CALIFICADO	30,88	32,73	32,73
MEDIO OFICIAL GENERAL	37,32	39,55	39,55
OFICIAL DE OFICIOS VARIOS	38,21	40,49	40,49
OFICIAL DE OFICIOS GENERALES	40,84	43,28	43,28
OFICIAL CALIFICADO	42,94	45,51	45,51
ADMINISTRACION			
CATEGORIA I	5.739,58	6.082,98	6.082,98
CATEGORIA II	6.067,48	6.430,50	6.430,50
CATEGORIA III	6.631,36	7.028,11	7.028,11
CATEGORIA IV	7.223,43	7.655,60	7.655,60
CATEGORIA V	7.578,70	8.032,12	8.032,12
CATEGORIA VI	8.259,60	8.753,76	8.753,76
2DO. JEFE DE SECCION	9.562,16	10.134,26	10.134,26
PERSONAL OBRERO MENSUALIZADO			
CELADORES, CUIDADORES Y CAMARERAS COMEDOR	5.684,92	6.025,04	6.025,04
ENCARGADAS, AYUDANTE DE COCINA COMEDOR PERSONAL	5.794,22	6.140,88	6.140,88
PORTEROS Y SERENOS	6.012,85	6.372,59	6.372,59
AYUDANTE REPARTIDOR	5.794,22	6.140,88	6.140,88
COCINERO COMEDOR PERSONAL	6.122,15	6.488,43	6.488,43
CHOFER Y CHOFER REPARTIDOR	6.286,12	6.662,21	6.662,21
SECADORES DE ARROZ - MAQUINISTAS Y ESTIBADORES, MAS EL SUPLEMENTO BOLSA DE:			
MANEJAR CAMION CON ACOPLADO			
POR CADA BULTO DE 50 KG			
POR CADA BULTO DE 51 A 60 KG			
ALMUERZO O CENA (ART. 14)			

ASIGNACION EXTRAORDINARIA NO REMUNERATIVA DE \$ 450, A SER ABONADA EN DOS PAGOS: EL PRIMERO CON LA SEGUNDA QUINCENA DE SEPTIEMBRE 2013 (\$ 225) Y EL SEGUNDO CON LA SEGUNDA QUINCENA DE NOVIEMBRE 2013 (\$ 225).

Expediente.: 1.556.012/13

Expediente N° 1.556.012/13

ACUERDO:

En la Ciudad Autónoma de Buenos Aires, a los catorce días del mes de junio del año dos mil trece, por una parte FEDERACION TRABAJADORES DE INDUSTRIAS DE LA ALIMENTACION (FTIA), representada por los señores Héctor Morcillo, José Varela y Silvia Villareal, patrocinado por el Dr. Adolfo MATARRESE; y por la otra parte la FEDERACION DE INDUSTRIAS DE PRODUCTOS ALIMENTICIOS Y AFINES (FIPAA) representada por el Sr. Marcelo CERETTI en su carácter de Secretario de la Entidad, con la asistencia letrada del Dr. Eduardo VIÑALES, las partes manifiestan que han arribado a un acuerdo para todo el personal comprendido en el CCT N° 244/94 el que se expresa de la siguiente manera:

La parte sindical en manifiesta (FTIA): que el APOORTE SOLIDARIO: De conformidad con las facultades legales y estatutarias y el mandato de la representación negociadora sindical conferido por los cuerpos orgánicos y los fundamentos aportados a la Comisión Negociadora, la Federación establece que los trabajadores comprendidos en el convenio colectivo 244/94 o el que lo reemplace, de conformidad a lo preceptuado en el art. 9° de la ley 14.250 (t.o.) aporten solidariamente a cada entidad sindical de primer grado adherida a la Federación Trabajadores de Industrias de la Alimentación, durante el plazo de un año a partir del mes de Mayo de 2013, una suma equivalente al 2% sobre las remuneraciones mensuales que los mismos perciban.

Este aporte de los trabajadores beneficiarios, entre otros destinos, estará destinado a cubrir gastos ya realizados y a realizar en la concertación de las convenciones colectivas de diferentes niveles. Asimismo coadyudará, entre otros objetivos, al desarrollo de la capacitación, acción social, a la formación profesional de equipos pluri-disciplinarios, sindicales y técnicos, que posibilite el desarrollo de la negociación colectiva favorable a mejores condiciones para todos los trabajadores beneficiarios y al desenvolvimiento económico y financiero de servicios y prestaciones que determine la asociación sindical que posibiliten una mayor y mejor calidad de vida del trabajador y su grupo familiar. La parte empleadora, teniendo presente lo expresado precedentemente en el párrafo primero, relativo a facultades y mandato de la representación sindical, manifiesta que sujeto a homologación ministerial, acuerda en cumplimiento de la normativa vigente en actuar como agente de retención del aporte, el que se depositará en la cuenta habilitada de cada sindicato de primer grado, afiliado a la F.T.I.A., que corresponda al establecimiento respectivo, dentro de los 15 días posteriores al mes que se devenguen.

Los trabajadores afiliados a los sindicatos de primer grado compensarán el aporte solidario, hasta su concurrencia, con la cuota sindical que deban abonar a la respectiva asociación sindical.

La parte empresaria ratifica la vigencia de la contribución empresaria prevista en el inc. B) del anexo V, del convenio celebrado el 16 de setiembre de 2003, homologado por resolución N° 188/03 de la D.N.R.L. Dicha contribución se incrementará a la suma de \$ 14 (pesos catorce) mensuales por cada trabajador comprendido en el CCT N° 244/94, manteniéndose todas las condiciones allí establecidas, a partir del mes de mayo de 2013 inclusive.

ACUERDO:

En la Ciudad Autónoma de Buenos Aires, a los catorce días del mes de junio del año dos mil trece, por una parte FEDERACION TRABAJADORES DE INDUSTRIAS DE LA ALIMENTACION, representada por los señores Héctor Morcillo, José Varela, Silvia Villareal, patrocinado por el Dr. Adolfo MATARRESE; y por la otra parte la FEDERACION DE INDUSTRIAS DE PRODUCTOS ALIMENTICIOS Y AFINES (FIPAA) representada por el Sr. Marcelo CERETTI en su carácter de Secretario de la Entidad, con la asistencia letrada del Dr. Eduardo VIÑALES, las partes manifiestan que han arribado a un acuerdo respecto a las nuevas remuneraciones para todo el personal comprendido en el CCT N° 244/94 el que se expresa de la siguiente manera:

PRIMERA:

Se pacta un incremento a partir del mes de mayo de 2013, correspondiendo a partir de dicha fecha las retribuciones que surgen de la columna que se identifica como "Mayo/Julio de 2013" en la planilla que se adjunta como anexo A.

SEGUNDA:

Se pacta un incremento a partir del mes de Agosto de 2013, correspondiendo a partir de dicha fecha las retribuciones que surgen de la columna que se identifica como "Agosto/Diciembre de 2013" en la planilla que se adjunta como anexo A.

TERCERA:

Las retribuciones básicas de cada una de las categorías establecidas en el presente acuerdo, incluyen y absorben hasta su concurrencia los aumentos otorgados a cuenta de paritarias, o futuros aumentos, a partir del mes de Febrero del año 2013.

CUARTA: Se pacta además, una asignación no remunerativa extraordinaria, de \$ 450 (pesos cuatrocientos cincuenta), la que se abonará en 2 pagos, por una suma de \$ 225 (pesos doscientos veinticinco), cada una, la primera de ellas junto con las retribuciones correspondientes a la segunda quincena del mes de Setiembre de 2013 y la segunda junto con el pago de las retribuciones correspondientes a la primera quincena del mes de noviembre de 2013.

QUINTA: El retroactivo del incremento pactado en la cláusula primera se podrá abonar hasta el momento del pago de la segunda quincena del mes de junio de 2013.

SEXTA: Las PARTES entienden que el compromiso económico asumido es sustentable en la medida en que se mantenga el respeto de los derechos mutuos, el clima de colaboración y de armonía laboral, la normalidad de los procesos productivos y la paz social, para la consecución de los objetivos de producción, comercialización y calidad, que sostengan económicamente la actividad y el bienestar de los trabajadores. El compromiso de paz social asumido en esta instancia se extiende durante la vigencia del presente acuerdo y las partes lo consideran esencial para viabilizar los incrementos pactados. En tal entendimiento las partes se obligan a resolver los diferendos, sin vulnerar derechos y sin afectar, salvo incumplimiento, la producción, por causas o circunstancias vinculadas con los aspectos alcanzados en el presente acuerdo resultando un compromiso esencial para las partes.

SEPTIMA: El período de vigencia es desde el 1/5/13 hasta el 30/4/14. Se adjunta planilla con las escalas salariales básicas del presente acuerdo, la misma figura como "ANEXO A".

OCTAVA: Las partes de común acuerdo ratifican y solicitan la homologación del presente acuerdo.



BOLETIN OFICIAL DE LA REPUBLICA ARGENTINA

*Agregando valor para estar
más cerca de sus necesidades...*



0810-345-BORA (2672)

**CENTRO DE ATENCIÓN
AL CLIENTE**

www.boletinoficial.gob.ar