



Dirección Administrativa

RESOLUCION N° 340-

POR LA CUAL SE APRUEBA LA POLITICA DE SEGURIDAD DE LA INFORMACIÓN DE LA DIRECCIÓN ADMINISTRATIVA.

Asunción, 10 MAY 2013

VISTO: La necesidad de implementar políticas y controles para proteger los activos de la información y establecer el marco de referencia para la regulación de la actividad informática, su correcta administración, buen uso y aprovechamiento de todos los recursos informáticos de la Dirección Administrativa (Exp. SIME N° 7.810/2013), y;

CONSIDERANDO:

Que, uno de los objetivos de la Dirección Administrativa a través del Departamento de Informática es brindar un óptimo servicio de tecnologías de información y telecomunicaciones, a fin de satisfacer las necesidades de las dependencias que conforman la Dirección Superior y la Dirección Administrativa, aplicando la calidad en los servicios para garantizar el uso adecuado de los recursos tecnológicos.

Que, es imprescindible desarrollar políticas que normen las actividades en cuanto al uso, aprovechamiento, y resguardo de los bienes y servicios informáticos de la Dirección Administrativa.

POR TANTO,

**LA DIRECTORA ADMINISTRATIVA
RESUELVE:**

- Art. 1º.-** Aprobar la Política de Seguridad de la Información de la Dirección Administrativa, conforme al Anexo que se adjunta y forma parte de la presente resolución.
- Art. 2º.-** Todas las dependencias que no forman parte de la Dirección Administrativa, deberán firmar un acuerdo de Prestación de Servicios con el Departamento de Informática de la Coordinación de Recursos Administrativos.
- Art. 3º.-** Conformar un Comité de Seguridad Informática.
- Art. 4º.-** Autorizar al Comité a implementar los instrumentos de monitoreo y control necesarios para el cumplimiento del reglamento aprobado por el Artículo 1º de la presente Resolución.
- Art. 5º.-** Comunicar a quienes corresponda y archivar.


C.P. NATALIA PALACIOS
Directora
Dirección Administrativa



Dirección Administrativa

ANEXO DE LA RESOLUCIÓN DA N° 340 /2013

POLITICA DE SEGURIDAD DE LA INFORMACION DE LA D.A.

SUMARIO

1 INTRODUCCIÓN	1
1.1 Objetivo del documento	1
1.2 Definiciones, Acrónimos y Abreviaciones	2
1.3 Antecedentes	2
1.4 Ámbito de aplicación	2
2 PERSONAS	3
2.1 Los funcionarios y la seguridad de la información	3
2.1.1 Códigos de identificación y palabras claves	3
2.1.2 Consideraciones acerca de una contraseña robusta:	3
2.1.3 Categorización de cuentas de usuario	4
2.1.4 De las cuentas de usuario para personas externas a la institución	4
2.1.5 Control de la Información	5
2.1.6 Otros usos	5
3 SOFTWARE	6
3.1 Administración, Operación y Control del Software	6
3.1.1 Administración del Software	6
3.1.2 Adquisición del Software	6
3.1.3 Desarrollo de Software	7
3.1.4 Pruebas de Software	7
3.1.5 Implantación del Software	8
3.1.6 Mantenimiento del Software	8
4 DATOS	9
4.1 Clasificación, almacenamiento y administración de la Información	9
4.1.1 Clasificación de la Información	9
4.1.2 Almacenamiento de la Información	10
4.1.2.1 Almacenamiento Masivo y Respaldo de Información	10
4.1.2.2 Almacenamiento en forma impresa o documentos en papel	10
4.1.3 Administración de la Información	11
4.1.4 Validaciones, controles y manejo de errores	12
5 POLÍTICA DE HARDWARE	12
5.1 Administración, mantenimiento, modernización y adquisición de equipos computacionales y de telecomunicaciones	12
5.1.1 Cambios al Hardware	12
5.1.2 Acceso físico y lógico	13
5.1.3 Respaldo y Continuidad del Negocio	13

Handwritten mark

Handwritten signature: Fernando Saenz
Lic. FERNANDESA SANTIAGO SÁENZ
Coordinadora Interina
Recursos Administrativos - D.A.
Ministerio de Hacienda



Handwritten signature: Lic. Jorge Luis Vega
Dirección Administrativa
Coordinación de Recursos Financieros

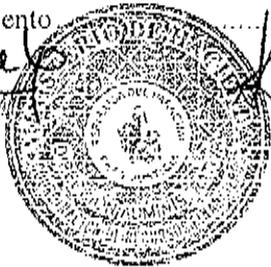


Dirección Administrativa

ANEXO DE LA RESOLUCIÓN DA N° 340 /2013

5.1.4 Otros.....	14
6 POLÍTICA DE INSTALACIONES FÍSICAS.....	14
6.1 Seguridad Física.....	14
6.1.1 Control de acceso físico.....	14
6.1.1.1 Personas.....	14
6.1.1.2 Equipos y Otros Recursos.....	15
6.1.2 Protección física de la información.....	15
6.1.3 Protección contra desastres.....	16
6.1.4 Planes de emergencia, contingencia y recuperación.....	16
7 POLÍTICA DE ADMINISTRACIÓN DE LA SEGURIDAD INFORMÁTICA.....	16
7.1.1 Generalidades.....	16
7.1.2 Funciones de Control.....	17
7.1.3 Comité de Seguridad Informática.....	18
7.1.4 Soporte a Investigaciones.....	18
7.1.5 Elaboración del Mapa de Riesgo.....	18
7.1.6 Plan de Contingencia.....	18
7.1.7 Capacitación y Entrenamiento.....	18

José Luis Saub
 LIC. LOURDES SANTICRUZ SAN JERÓNIMO
 Coordinadora Interim
 Recursos Administrativos - D.A.
 Ministerio de Hacienda



Jorge Luis Vega
 Lic. Jorge Luis Vega
 Dirección Administrativa
 Coordinación de Recursos Financieros

Lucy



Dirección Administrativa

ANEXO DE LA RESOLUCIÓN DA N° 340 /2013

1 INTRODUCCIÓN

La seguridad de la información es la protección de la información de una amplia variedad de amenazas, con el objeto de asegurar la continuidad del negocio, minimizar los riesgos, maximizar el retorno de la inversión y aprovechar las oportunidades que pudieran presentarse.

Conscientes de que la seguridad informática se fundamenta en la existencia de un conjunto de políticas que brinden instrucciones claras y sean el soporte de la alta gerencia y con el objetivo que éstas sean una herramienta para la definición de los estándares y procesos internos de cada entidad, se definen las siguientes políticas:

- Personal
- Datos
- Software
- Hardware
- Instalaciones físicas
- Administración de seguridad

Los activos de información y los equipos informáticos son recursos importantes y vitales de la Institución. Por tal razón, la Dirección Administrativa tiene el deber de preservarlos, utilizarlos y mejorarlos. Esto significa que se deben tomar las acciones apropiadas para asegurar que la información y los sistemas informáticos estén apropiadamente protegidos de muchas clases de amenazas y riesgos tales como fraude, sabotaje, extorsión, violación de la privacidad, intrusos, hackers, interrupción del servicio, accidentes y desastres naturales.

La política es elaborada tomando como base la cultura de la organización y el conocimiento especializado de seguridad de los profesionales involucrados con su aplicación y comprometimiento.

Es importante considerar que para la modificación de una política de seguridad de la DA se debe:

- Integrar el Comité de Seguridad responsable de definir la política.
- Elaborar el documento final.
- Hacer oficial la política una vez que se tenga definida.
- Publicar y difundir amplia y adecuadamente esta política.

1.1 Objetivo del documento

El objetivo de este documento es determinar las políticas de seguridad de la información, buscando asegurar la capacidad de la Dirección Administrativa (DA) para responder eficazmente ante desastres y otras situaciones de emergencia que pudieren afectar a las dependencias de manera parcial o total.

Proporcionar dirección y apoyo de la DA para la seguridad de la información de acuerdo con los requerimientos del negocio y las leyes y regulaciones correspondientes.

Establecer el marco regulatorio de la seguridad informática, su correcta administración y la optimización del uso y aprovechamiento de todos los recursos informáticos de la DA.

Fernando Sastre
Coordinador General de Recursos Administrativos - D.A.
Ministerio de Hacienda



Fernando Sastre
Dirección Administrativa
Coordinación de Recursos Financieros



Dirección Administrativa

ANEXO DE LA RESOLUCIÓN DA N° 340/2013

1.2 Definiciones, Acrónimos y Abreviaciones

MH	=	Ministerio de Hacienda
DA	=	Dirección Administrativa.
CRA	=	Coordinación de Recursos Administrativos.
UOC	=	Unidad Operativa de Contrataciones
DGIC	=	Dirección General de Informática y Comunicaciones
DI	=	Departamento de Informática.
TI	=	Tecnología de la Información.
SO	=	Sistema Operativo

1.3 Antecedentes

Para la realización de este documento se tomó como punto de partida las políticas de seguridad del Departamento de Informática publicadas en el año 2008.

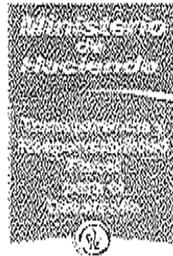
1.4 Ámbito de aplicación

Las políticas de seguridad informática de la DA son de cumplimiento obligatorio para los funcionarios de la Dirección Administrativa y las demás dependencias con quienes se tenga firmado un acuerdo de prestación de servicios. La falta de observancia tendrá como consecuencia, la aplicación de las sanciones previstas en las normas legales vigentes.

Jorge Luis Vega
Coordinador Interimario
Recursos Administrativos
Ministerio de Hacienda



Lic. Jorge Luis Vega
Dirección Administrativa
Coordinación de Recursos Financieros



Dirección Administrativa

ANEXO DE LA RESOLUCIÓN DA N° 340 /2013

2 PERSONAS.

2.1 Los funcionarios y la seguridad de la información.

La responsabilidad por la seguridad de la información no es únicamente del Departamento de Informática, es una obligación de cada funcionario.

Todo funcionario que utilice los equipos informáticos de la DA, deberá observar lo prescrito en estas políticas. Su desconocimiento no exime de las sanciones ocasionadas por el incumplimiento. El Departamento de Informática vigilará su cumplimiento.

Los equipos informáticos de la institución deberán utilizarse en un ambiente seguro, considerándose como tal, aquel en el cual se han implantado las medidas de control apropiadas para proteger el software, el hardware y los datos. Dichas medidas estarán en concordancia con la importancia de los datos y la naturaleza de los riesgos previsibles.

2.1.1 Códigos de identificación y palabras claves

- (a) Las palabras claves o los mecanismos de acceso que les sean otorgados a los funcionarios son responsabilidad exclusiva de cada uno de ellos y no deben ser divulgados a ninguna persona, a menos que exista un requerimiento legal o medie un procedimiento de custodia de claves. De acuerdo con lo anterior, los usuarios no deben obtener palabras claves u otros mecanismos de acceso de otros usuarios que pueda permitirles un acceso indebido.
- (b) La solicitud de una nueva cuenta o el cambio de privilegios debe ser hecha por escrito y debe ser debidamente aprobada por el Jefe del área que lo solicita.
- (c) Los usuarios son responsables de todas las actividades llevadas a cabo con su código de identificación de usuario y sus claves personales.
- (d) Cuando un empleado es despedido o renuncia a la Institución, debe desactivarse su cuenta antes de que deje el cargo.
- (e) No se concederán cuentas a personas que no sean funcionarios de la Institución.

2.1.2 Consideraciones acerca de una contraseña fuerte.

Los sistemas deberán obligar al usuario a utilizar una clave fuerte. Se entiende por clave fuerte a las contraseñas cuyas características las hacen difícil de adivinar, tanto por seres humanos como por algoritmos computacionales. Las propiedades más importantes que debe cumplir una contraseña considerada fuerte son las siguientes:

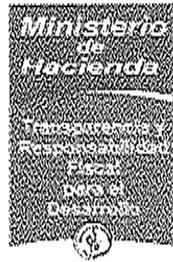
- (a) Debe tener un mínimo de 10 (diez) caracteres.
- (b) No debe ser evidente, como nombres o cumpleaños personales o familiares.
- (c) Debe contener combinación de números, letras (mayúsculas, minúsculas) y símbolos o caracteres especiales.
- (d) No debe encontrarse en un diccionario.
- (e) No debe sugerir aspectos correspondientes a la vida personal o laboral de quien la selecciona.
- (f) Debe permanecer cifrada en archivos seguros y protegidos.

Rodrigo Saiz
COORDINADOR GENERAL
Cuerpo de Asesores
Recursos Administrativos - D.A.
Ministerio de Hacienda



Jorge Luis Vega
Dirección Administrativa
Coordinación de Recursos Financieros

Rod



Dirección Administrativa

ANEXO DE LA RESOLUCIÓN DA N° 340 /2013

- (g) No debe ser visible por pantalla al momento de ser ingresada ni durante la transmisión.
- (h) El concepto a considerar, es que la clave no pueda ser advertida fácilmente.

También se adecuarán a una política de generación y de cambio de contraseñas que mínimamente deberán contemplar:

- (i) La contraseña debe cambiarse obligatoriamente la primera vez que el usuario ingresa al sistema.
- (j) Debe cambiarse obligatoriamente en un período máximo de 90 (noventa) días, debiendo el sistema solicitar automáticamente el cambio de la misma al cumplirse el período.
- (k) La nueva contraseña debe ser distinta a por lo menos, a las últimas 8 (ocho) contraseñas y no se debe permitir el cambio de la misma hasta pasados 3 (tres) días, a menos que sea solicitado al Administrador por el Responsable de Seguridad de la Información o el superior inmediato del usuario.
- (l) Toda vez que el sistema solicite un cambio de contraseña, debe ingresarse la confirmación de la contraseña anterior y de la nueva.
- (m) Las contraseñas para nuevos usuarios deberán configurarse con un valor único para cada usuario y deberá cambiarse luego del primer uso.
- (n) En caso que el Usuario olvide su clave personal, o por decisión de Seguridad de la Información, el Dueño de Datos debe solicitar el cambio de la clave a través de los medios disponibles a tal fin.

2.1.3 Categorización de cuentas de usuario

Todos los sistemas deben contemplar la posibilidad de realizar la categorización de las cuentas de los usuarios o contemplar la interconexión con un software de manejo centralizado de informaciones (Lightweight Directory Access Protocol - LDAP). En estas categorías se deben incluir la definición de los roles, los permisos, las limitaciones, etc. de cada tipo de cuenta. Ejemplos de categorías:

- (a) Usuario privilegiado.
- (b) Usuario genérico.
- (c) Usuario de sistema.
- (d) Usuario de email.

2.1.4 De las cuentas de usuario para personas externas a la institución

En el caso de que se requiera dar acceso a personas externas a la institución para realizar algún tipo de mantenimiento se deberá contemplar lo siguiente:

- (a) No está permitido prestar temporalmente la cuenta de un funcionario.
- (b) No está permitido crear una cuenta temporal con los privilegios requeridos para la tarea en cuestión.
- (c) El trabajo deberá ser realizado por un funcionario responsable con el nivel de acceso requerido, el que deberá documentar cada tarea realizada en compañía de la persona externa. Esto a fin de hacer el traspaso del conocimiento (de lo que se hizo) a la Institución.

Rolando Saiz

Comandante en Jefe
Reserva de Armamento - D.A.
Ministerio de Hacienda



Lic. Jorge Luis Vega
Dirección Administrativa
Comandancia de Recursos Financieros



Dirección Administrativa

ANEXO DE LA RESOLUCIÓN DA N° 340 /2013

2.1.5 Control de la Información

- Los usuarios deben informar inmediatamente al Departamento de Informática toda vulnerabilidad encontrada en los sistemas, aparición de virus o programas sospechosos e intentos de intromisión y no deben distribuir este tipo de información interna o externamente.
- Si se detecta la presencia de un virus u otro agente potencialmente peligroso, se debe poner la PC en cuarentena hasta que el problema sea resuelto.
- Los usuarios no deben instalar software en sus computadores o en servidores sin las debidas autorizaciones.
- Los usuarios no deben intentar sobrepasar los controles de los sistemas, examinar los computadores y redes de la entidad en busca de archivos de otros sin su autorización o introducir intencionalmente software diseñado para causar daño o impedir el normal funcionamiento de los sistemas.
- Los usuarios de PCs son responsables de proteger los programas y datos contra pérdida o daño. Para sistemas multiusuario y sistemas de comunicaciones, el Administrador de cada uno de esos sistemas es responsable de hacer copias de respaldo periódicas. Los Jefes de los distintos Departamentos son responsables de definir qué información debe respaldarse, así como la frecuencia del respaldo (por ejemplo: diario, semanal) y el método de respaldo (por ejemplo: incremental, total).
- Los funcionarios no deben suministrar cualquier información de la entidad a ningún ente externo sin las autorizaciones respectivas esto incluye los controles del sistema de información y su respectiva implementación.
- Los funcionarios no deben destruir, copiar o distribuir los archivos de la entidad sin los permisos respectivos.
- Los funcionarios deben guardar en todo momento la privacidad de la información de los clientes internos.
- Todo funcionario que utilice los recursos de los Sistemas, tiene la responsabilidad de velar por la integridad, confidencialidad, disponibilidad y confiabilidad de la información que maneje, especialmente si dicha información ha sido clasificada como crítica.

2.1.6 Otros usos

- Los equipos informáticos de la institución sólo podrán utilizarse para actividades propias del trabajo, no pudiendo ser utilizados para otros fines, tales como: juegos, pasatiempos o trabajos personales.
- Para prevenir demandas legales o la introducción de virus informáticos, se prohíbe estrictamente la instalación de software no autorizado, incluyendo el que haya sido adquirido por el propio usuario. Así mismo, no se permite el uso de ningún tipo de software, a menos que haya sido previamente aprobado por el Departamento de Informática.
- No podrán modificarse el hardware y software desarrollados, proveídos e instalados por el Departamento de Informática.
- No está permitido fumar, comer o beber durante la utilización de un equipo informático.
- Los equipos informáticos deberán evitarse de riesgos del medio ambiente (polvo, agua, incendio, etc.).

51
L. CARLOS SANTACRUZ
Coordinador de Recursos Administrativos
Ministerio de Hacienda



Lic. Jorge Luis Vega
Dirección Administrativa
Caj. Director de Recursos Financieros



Dirección Administrativa

ANEXO DE LA RESOLUCIÓN DA N° 340/2013

- (f) Siempre que estén disponibles, deben utilizarse los filtros de energía eléctrica; en los servidores, deben usarse fuentes de poder ininterrumpibles (UPS).
- (g) Todo medio de almacenamiento a ser utilizado en el equipo informático de la institución, deberá ser previamente verificado por un software antivirus, a los efectos de liberarlos de posibles virus u otros agentes dañinos.
- (h) Los equipos informáticos deberán estar dispuestos de forma apropiada, a los efectos de proteger los datos confidenciales que aparezcan en pantalla a la vista de cualquier persona ajena a la entidad.
- (i) El Departamento de Informática determinará el formato y apariencia del protector y fondo de pantalla.

3 SOFTWARE

3.1 Administración, Operación y Control del Software

Los funcionarios con funciones y responsabilidades para con el software deben seguir los siguientes lineamientos para proteger este activo y la información que a través de él se maneje:

3.1.1 Administración del Software

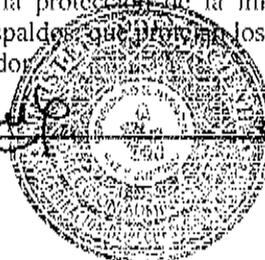
- (a) El Departamento de Informática debe contar en todo momento con un inventario actualizado del software de su propiedad, el comprado a terceros o desarrollado internamente, el adquirido bajo licenciamiento, el entregado y el recibido en comodato. Las licencias se almacenarán bajo los adecuados niveles de seguridad e incluidas en un sistema de administración, efectuando continuos muestreos para garantizar la consistencia de la información allí almacenada.
Igualmente, todo el software y la documentación del mismo que posea la Entidad incluirán avisos de derechos de autor y propiedad intelectual.
- (b) Todas las aplicaciones se clasificarán en una de las siguientes tres categorías: Misión Crítica, Prioritaria y Requerida. Para las de misión crítica y prioritaria deberá permanecer una copia actualizada y su documentación técnica respectiva, como mínimo en un sitio alternativo y seguro de custodia.
- (c) Los ambientes de desarrollo de sistemas, pruebas y producción deben permanecer separados para su adecuada administración, operación, control y seguridad. Los programas que se encuentren en el ambiente de producción de la DA, se modificarán únicamente por personal autorizado, de acuerdo con los procedimientos internos establecidos y en todos los casos se considerarán planes de contingencia y recuperación.

3.1.2 Adquisición del Software

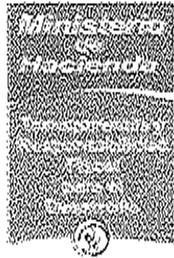
- (a) La Entidad deberá tener una metodología formal para el proceso de adquisición de software de misión crítica o prioritaria a través de terceros que incluya un contrato pro forma con cláusulas básicas para la protección de la información y del software, así como para la documentación y los respaldos que protejan los intereses institucionales frente a las cláusulas entregadas por el vendedor.

Jorge Luis Vega

6
Lic. Jorge Luis Vega
Dirección Administrativa
Coordinación de Recursos Financieros



Lic. Jorge Luis Vega
Dirección Administrativa
Coordinación de Recursos Financieros



MINISTERIO
DE HACIENDA
PRESIDENCIA
DE LA REPÚBLICA
"PARAGUAY"



Dirección Administrativa

ANEXO DE LA RESOLUCIÓN DA N° 340 /2013

- (b) El software contará con acceso controlado que permita al propietario del recurso restringir el acceso al mismo; el software protegerá los objetos para que los procesos y/o los usuarios no los puedan acceder sin los debidos permisos; cada usuario se identificará por medio de un único código de identificación de usuario y clave, antes de que se le permita el acceso al sistema; el software auditará los eventos en el sistema relacionados con la seguridad. Para cumplir con éstas premisas, será necesario que el software incluya el plan de cuentas de acceso, el plan de auditoría y el de cierre de puertas traseras.
- (c) Cuando se adquiriera una licencia de uso de software, a través de un proveedor o la contratación de software a la medida, el vendedor depositará en custodia en una empresa especializada una copia del software adquirido y su documentación técnica respectiva y sus correspondientes actualizaciones. Igualmente dejará una autorización por escrito para que la Entidad los pueda retirar, cuando por motivos de fuerza mayor el vendedor deje de existir en el mercado.
- (d) Para disminuir los riesgos sobre la información administrada en las aplicaciones adquiridas a través de terceros o las desarrolladas en casa, el documento de especificaciones incluirá un capítulo relativo a la seguridad informática.

3.1.3 Desarrollo de Software

- (a) El departamento deberá tener una metodología formal para el desarrollo de software de los sistemas de información de misión crítica y prioritaria, desarrollos rápidos del mismo y las actividades de mantenimiento, las cuales cumplirán con las políticas, normas, procedimientos, controles y otras convenciones estándares aplicables en el desarrollo de sistemas. Los controles desarrollados internamente deberán ser como mínimo los exigidos en adquisición de software que incluyan el plan de cuentas, el plan de auditoría y el cierre de puertas traseras. Adicionalmente, toda solicitud de modificación al software deberá contar con estudios de factibilidad y de viabilidad al igual que las autorizaciones respectivas dentro de la Entidad.
- (b) Con el propósito de garantizar integridad y confidencialidad de la información que administrará el software desarrollado y antes del paso a pruebas, se deberán ejecutar las pruebas intrínsecas al desarrollo y a la documentación técnica respectiva. Para todo desarrollo de software se deberán utilizar herramientas definidas por la DA, de las cuales se tengan certeza que su comportamiento es seguro y confiable. Solamente las funciones descritas en el documento aprobado de especificaciones de la solución tecnológica, podrán ser desarrolladas.
- (c) Los programadores de software no deberán conocer las claves utilizadas en ambientes de producción.
- (d) Los desarrollos y/o modificaciones hechos a los sistemas de aplicación no deberán trasladarse al ambiente de producción si no se cuenta primero con la documentación de entrenamiento, operación y de seguridad adecuados.

3.1.4 Pruebas de Software

- 1) Un equipo especializado deberá realizar las pruebas en representación de los usuarios finales. El área de desarrollo de sistemas deberá entregar el software desarrollado con códigos fuentes al área responsable de ejecutar las pruebas, el cual deberá ser revisado para encontrar códigos

Jorge Luis Vega
Jefe de Área
Recursos Administrativos - DA
Ministerio de Hacienda



Jorge Luis Vega
Dc. Jorge Luis Vega
Dirección Administrativa
Coordinación de Recursos Financieros



MINISTERIO
DE HACIENDA
PRESIDENCIA
DE LA REPÚBLICA
DEL PARAGUAY



Dirección Administrativa

ANEXO DE LA RESOLUCIÓN DA N° 340 /2013

- mal intencionado y debilidades de seguridad utilizando preferiblemente herramientas automáticas, para luego ser compilado e iniciar las pruebas correspondientes.
- 2) Los tipos de pruebas mínimas a realizar deberán ser previamente establecidas por el Departamento de Informática. Para garantizar la integridad de la información en producción éstas deberán ser debidamente planeadas, ejecutadas, documentados y controlados sus resultados, con el fin de garantizar la integridad de la información en producción. Además, el ambiente de pruebas deberá ser lo más idéntico, en su configuración, al ambiente real de producción.
 - 3) Las pruebas sobre el software desarrollado tanto interna como externamente deberán contemplar aspectos funcionales, de seguridad y técnicos. Adicionalmente, se incluirá una revisión exhaustiva a la documentación mínima requerida, así como la revisión de los procesos de retorno a la versión anterior. En caso que se requirieran las claves de producción, para ejecutar pruebas, su inserción y mantenimiento se deberá efectuar de manera segura. El departamento de Informática deberá poseer un cronograma para la ejecución de las pruebas con el fin de cumplir con los compromisos institucionales acordados, éste se podrá ver afectado en su calendarización por eventos en que se tengan que atender desarrollos rápidos únicamente por exigencias de entes de control externos y/o de la DA.
 - 4) Eliminar todas las cuentas, usuarios y/o archivos temporales y de prueba creados durante esta etapa.

3.1.5 Implantación del Software

- (a) Para implementar software mediará una autorización por escrito del responsable para tal fin. Las características que son innecesarias en el ambiente informático de la DA se identificarán y desactivarán en el momento de la instalación del software.
- (b) Antes de implementar el software en producción se verificará que se haya realizado: La divulgación y entrega de la documentación, la capacitación al personal involucrado, su licenciamiento y los ajustes de parámetros en el ambiente de producción. Se deberá tener un cronograma de puesta en producción con el fin de minimizar el impacto del mismo.
- (c) Los módulos ejecutables nunca deberán ser trasladados directamente de las librerías de pruebas a las librerías de producción sin que previamente sean compilados por el área asignada para tal efecto, que en ningún momento deberá ser el área de desarrollo de sistemas informáticos.
- (d) Los programas en el ambiente de producción de la DA, serán modificados únicamente por personal autorizado y cuando se requiera por fuerza mayor de acuerdo con las normas institucionales establecidas.
- (e) Los clientes, compañías comerciales y otros terceros, deberán firmar previamente un acuerdo que declare que ellos no desensamblarán, modificarán, ni usarán indebidamente los programas entregados que fueron desarrollados por la Entidad.

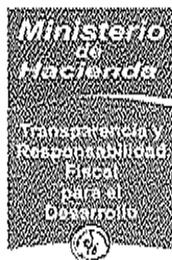
3.1.6 Mantenimiento del Software

- (a) El área de desarrollo de sistemas no hará cambios al software de producción sin las debidas autorizaciones por escrito y sin cumplir con los procedimientos establecidos por la Entidad. A

Jorge Luis Vega
Lic. Jorge Luis Vega
Dirección Administrativa
Coordinación de Recursos Financieros



Lic. Jorge Luis Vega
Dirección Administrativa
Coordinación de Recursos Financieros



Dirección Administrativa

ANEXO DE LA RESOLUCIÓN DA N° 340 /2013

su vez, la Entidad contará con un procedimiento de control de cambios que garantice que sólo se realicen las modificaciones autorizadas.

- (b) La documentación de todos los cambios hechos al software en la Entidad, se preparará simultáneamente con el proceso de cambio. Se deberá considerar, además, que cuando un tercero efectúe ajuste al software de la Entidad, éste deberá firmar un acuerdo de no-divulgación y utilización no autorizada del mismo.
- (c) Para cada mantenimiento, a la versión del software de misión crítica y prioritaria de la Entidad, se actualizará el depositado en custodia en el sitio alerno y el respaldado en la institución. Este software y su documentación se verificarán y certificará su actualización.
- (d) Las actualizaciones de software requerido de la Entidad deberán cumplir con los procedimientos de licenciamiento respectivo.

4 DATOS

4.1 Clasificación, almacenamiento y administración de la Información

Los funcionarios de la entidad son responsables de la información que manejan y deberán seguir los siguientes lineamientos para protegerla y evitar pérdidas, accesos no autorizados y utilización indebida de la misma.

4.1.1 Clasificación de la Información

- (a) Todos los datos de propiedad de la entidad se deben clasificar dentro de las siguientes categorías para los datos sensibles: SECRETO, CONFIDENCIAL, PRIVADO, y para los datos no sensibles la categoría es PÚBLICO. Para identificar la naturaleza de la información y las personas autorizadas para accederla se deben utilizar prefijos como indicadores generales tales como: "CRA", "CRF", "CRII", "GAB", "DA", etc. Toda información secreta, confidencial y privada debe etiquetarse (marcarse) según las normas de la Entidad y todos los datos que se divulguen por cualquier medio deben mostrar la clasificación de sensibilidad de la información.
- (b) Cuando se consolida información con varias clasificaciones de sensibilidad, los controles usados deben proteger la información más sensible y se debe clasificar con el máximo nivel de restricción que contenga la misma.
- (c) La información que se clasifica dentro de las categorías de sensibilidad debe identificarse con la marca correspondiente y se debe indicar la fecha en que deja de ser sensible, esto aplica para la información que se reclasifica tanto en un nivel inferior como en un nivel superior de sensibilidad.
- (d) La responsabilidad para definir la clasificación de la información debe ser tanto del dueño de la información como del área encargada de la seguridad informática en la organización; adicionalmente, deben tener una programación para realizar mantenimiento a la clasificación de sensibilidad de la información.
- (e) Para la eliminación de la información debe seguir procedimientos seguros y debidamente aprobados por el Departamento de Informática y por el responsable de los datos en la entidad.

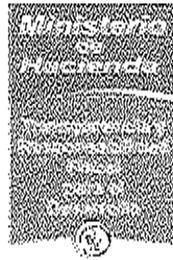
[Handwritten mark]

Jorge Luis Vega



9 LIC. JORGE LUIS VEGA
Coordinador Técnico
Recursos Financieros
Ministerio de Hacienda

Lic. Jorge Luis Vega
Dirección Administrativa
Coordinación de Recursos Financieros



MINISTERIO
DE HACIENDA
PRESIDENCIA
DE LA REPÚBLICA
DEL PARAGUAY



Dirección Administrativa

ANEXO DE LA RESOLUCIÓN DA N° 340 /2013

4.1.2 Almacenamiento de la Información

4.1.2.1 Almacenamiento Masivo y Respaldo de Información

- Toda información secreta debe estar cifrada, ya sea que se encuentre al interior de la entidad o externamente, en cualquier medio de almacenamiento, transporte o transmisión.
- Toda información sensible debe tener un proceso periódico de respaldo, tener asignado un periodo de retención determinado, la fecha de la última modificación y la fecha en que deja de ser sensible o se degrada; sin embargo, la información no se debe guardar indefinidamente por lo cual se debe determinar un periodo máximo de retención para el caso en que no se haya especificado este tiempo.
- La información clasificada como sensible (secreta, confidencial o privada) debe tener un respaldo, además debe tener copias recientes completas en sitio externo a la entidad o en un lugar lejano de donde reside la información origen; en caso que no se tengan copias de la información crítica no se deben llevar a cabo procesos de restauración puesto que se corre el riesgo de perder la única copia que se tenga.
- Todos los medios físicos donde la información de valor, sensitiva y critica sea almacenada por periodos mayores de seis (6) meses, no deben estar sujetos a una rápida degradación o deterioro.
- Los respaldos de información de valor o sensible debe tener un proceso periódico de validación con el fin de garantizar que no ha sufrido ningún deterioro y que se podrá utilizar en el momento en que se necesite.
- Toda la información contable, de impuestos, y de tipo legal debe ser conservada de acuerdo con las normas de ley vigentes.

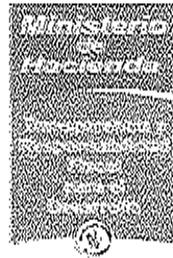
4.1.2.2 Almacenamiento en forma impresa o documentos en papel

- La remisión de información sensible tanto por correo interno como externo debe cumplir con los procedimientos establecidos de manera que se realice en forma segura.
- Para todos los mensajes remitidos en formato libre de texto que contengan información sensible para el negocio debe numerarse cada línea y los documentos oficiales de la entidad que se realicen a mano deben ser escritos con tinta.
- La información sensible que aparece en los recibos generados por computador y entregados a los clientes deben ser truncados.
- Todas las copias de documentos secretos deben ser numeradas individualmente con un número secuencial para que las personas responsables puedan localizar rápidamente los documentos e identificar algún faltante de la misma.
- Cuando se utilicen medios de transmisión como el fax, se deben seguir los procedimientos establecidos de tal manera que se asegure la confidencialidad e integridad de la información.

Handwritten signature
LIC. JORGE DANIEL VEGA
Coordinador de Recursos
Financieros
Ministerio de Hacienda



Handwritten signature
Lic. Jorge Luis Vega
Dirección Administrativa
Coordinación de Recursos Financieros



MINISTERIO
DE HACIENDA
PRESIDENCIA
DE REPÚBLICA
DEL PARAGUAY



Dirección Administrativa

ANEXO DE LA RESOLUCIÓN DA N° 340 /2013

4.1.3 Administración de la Información

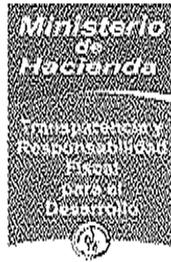
1. Cualquier tipo de información interna de la entidad no debe ser vendida, transferida o intercambiada con terceros para ningún propósito diferente al de la entidad y se debe cumplir con los procedimientos de autorización internos para los casos en que se requiera.
2. Todos los derechos de propiedad intelectual de los productos desarrollados o modificados por los empleados de la institución, durante el tiempo que dure su relación laboral, son de propiedad exclusiva del Departamento de Informática.
3. Los datos y programas de la entidad deben ser modificados únicamente por personal autorizado de acuerdo con los procedimientos establecidos, al igual que el acceso a bodegas de información debe restringirse únicamente a personal autorizado.
4. Cuando la información sensible no se está utilizando se debe guardar en los sitios destinados para esto, los cuales deben contar con las debidas medidas de seguridad que garanticen su confidencialidad e integridad.
5. En cualquier momento, el propietario de la información con la participación del responsable de la seguridad informática y de datos puede reclasificar el nivel de sensibilidad inicialmente aplicado a la información.
6. El acceso a la información secreta se debe otorgar únicamente a personas específicas.
7. Toda divulgación de información secreta, confidencial o privada a terceras personas debe estar acompañada por un contrato que describa explícitamente qué información es restringida y cómo puede o no ser usada.
8. Toda la información de la organización debe contemplar las características de Integridad, Confidencialidad, Disponibilidad, Auditabilidad, Efectividad, Eficiencia, Cumplimiento y Confiabilidad.
9. Todo software que comprometa la seguridad del sistema se custodiará y administrará únicamente por personal autorizado.
10. La realización de copias adicionales de información sensible debe cumplir con los procedimientos de seguridad establecidos para tal fin.
11. La información de la entidad no debe ser divulgada sin contar con los permisos correspondientes, además, ningún empleado, contratista o consultor debe tomarla cuando se retire de la entidad.
12. Todos los medios de almacenamiento utilizados en el proceso de construcción, asignación, distribución o cifrado de claves se deben someter a un proceso de eliminación (zeroization) inmediatamente después de ser usados.
13. Toda la información histórica almacenada debe contar con los medios, procesos y programas capaces de manipularla sin inconvenientes, esto teniendo en cuenta la reestructuración que sufren las aplicaciones y los datos a través del tiempo.
14. Los usuarios deberán utilizar un sistema robusto de contraseñas que no tenga relación obvia con el usuario, sus familiares, el grupo de trabajo u otras asociaciones parecidas.
15. El usuario deberá configurar el protector de pantalla para que se active, como máximo, al cabo de cinco minutos de inactividad y que requiera una contraseña al reasumir la actividad, siempre y cuando esto no haya sido configurado por los técnicos del Dpto. de Informática de la DA.
16. Activar el protector de pantalla automáticamente, cada vez que se ausente de su oficina.

[Handwritten signature]

José Luis Saenz
Dpto. de Informática
Coordinación de Recursos
Recursos Administrativos
Ministerio de Hacienda



Jorge Luis Vega
Dirección Administrativa
Coordinación de Recursos Financieros



Dirección Administrativa

ANEXO DE LA RESOLUCIÓN DA N° 340/2013

4.1.4 Validaciones, controles y manejo de errores

- (a) Para reducir la probabilidad de ingreso erróneo de datos de alta sensibilidad, todos los procedimientos de ingreso de información deben contener controles de validación.
- (b) Se deben tener procedimientos de control y validaciones para las transacciones rechazadas o pendientes de procesar, además de tiempos determinados para dar la solución y tomar las medidas correctivas.
- (c) Todas las transacciones que ingresen a un sistema de producción computarizado, deben ser sujetos a un chequeo razonable, chequeos de edición y/o validaciones de control.
- (d) Todos los errores cometidos por los funcionarios de la entidad y que son detectados por los clientes internos deben cumplir con un proceso de investigación de acuerdo con los procedimientos y tiempos establecidos.

5 POLÍTICA DE HARDWARE

5.1 Administración, mantenimiento, modernización y adquisición de equipos computacionales y de telecomunicaciones

La administración, mantenimiento, modernización y adquisición de equipos computacionales y de telecomunicaciones debe adoptar los siguientes criterios para proteger la integridad técnica de la institución.

5.1.1 Cambios al Hardware

- (a) Los equipos de cómputo de la entidad no deben ser alterados ni mejorados (cambios de procesador, adición de memoria o tarjetas) sin el consentimiento, evaluación técnica y autorización del Departamento de Informática.
- (b) Los funcionarios deben reportar a los entes pertinentes de la entidad y al Departamento de Informática, sobre daños o pérdida del equipo que tengan a su cuidado y sea propiedad de la entidad. La intervención directa para reparar el equipo está expresamente prohibida. El Departamento de Informática debe proporcionar personal interno o externo para la solución del problema reportado.
- (c) Cualquier falla en los equipos informáticos o en la red local, deberá ser reportada inmediatamente por el usuario que la detecte, al Departamento de Informática.
- (d) Los equipos informáticos deben ser protegidos de los riesgos de robo, destrucción o mala utilización por el usuario responsable de los mismos.
- (e) La pérdida o robo de cualquier componente de hardware o software deberá ser reportado inmediatamente al Departamento de Informática.
- (f) Todos los equipos de la entidad deben estar registrados en un inventario que incluya la información de sus características, configuración y ubicación.
- (g) Para todas las adquisiciones de hardware se deberán seguir los canales de compra, estándares y procedimientos definidos por el Departamento de Informática, el que será el único responsable de ampliar, reducir o consolidar los pedidos realizados por los clientes internos.
- (h) Para todos los equipos y sistemas de comunicación utilizados en procesos de producción en la entidad, se debe aplicar un procedimiento formal de control de cambios que garantice que solo se realicen los cambios autorizados. Este procedimiento de control de cambios debe

12 | *Jorge Luis Vega*
LIC. JORGE LUIS VEGA
Carrera de Ingeniería de Sistemas
Recursos Administrativos - D.A.
Ministerio de Hacienda



Jorge Luis Vega
Lic. Jorge Luis Vega
Dirección Administrativa
Comando en Jefe Recursos Financieros



Dirección Administrativa

ANEXO DE LA RESOLUCIÓN DA N° 340 /2013

incluir la documentación del proceso con las respectivas propuestas revisadas, la aprobación de las áreas correspondientes y la manera como el cambio fue realizado.

- (i) Todos los productos de hardware deben ser registrados por proveedor y contar con el respectivo contrato de mantenimiento.
- (j) Los equipos de informáticos (PC, servidores, cableado, etc.) no deben quitarse, moverse o reubicarse sin la aprobación previa del Departamento de Informática y el administrador, jefe o coordinador del área involucrada.

5.1.2 Acceso físico y lógico

Antes de conectarlos a la red interna todos los servidores de Intranet de la entidad deben ser autorizados por el área responsable del hardware.

Todos los equipos multiusuarios (servidores y equipos de comunicaciones) deben estar ubicadas en lugares asegurados para prevenir alteraciones y usos no autorizados.

Las bibliotecas de cintas magnéticas, discos y documentos se deben ubicar en áreas restringidas dentro del centro de cómputo y en sitios alternos con acceso únicamente a personas autorizadas.

Se prohíbe la utilización de hardware o software que permita la conexión externa desde y hacia la red de datos de la DA. En caso de requerirse, todas las conexiones con los sistemas y redes de la entidad serán dirigidas a través de dispositivos probados y aprobados por el Departamento de Informática y deberán contar con mecanismos que soporten la infraestructura de autenticación y autorización de usuarios de la DA.

Los equipos de computación de la entidad que pueden ser accedidos por terceros a través de diversos canales - como líneas conmutadas, redes de valor agregado, Internet y otros-, deben ser protegidos por mecanismos de control aprobados por el área de seguridad informática y de datos.

Las direcciones internas, configuraciones e información relacionada con el diseño de los sistemas de comunicación y cómputo de la entidad deben ser restringidas.

Todas las líneas conmutadas que permitan el acceso a la red de comunicaciones o sistemas multiusuario deben pasar a través de un punto de control adicional (firewall) antes de ingresar a la red de datos de la DA.

5.1.3 Respaldo y Continuidad del Negocio

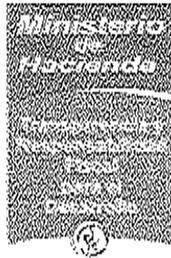
- (a) La administración debe proveer, mantener y dar entrenamiento sobre los sistemas de protección necesarios para asegurar la continuidad del servicio en los sistemas de computación críticos, tales como sistemas de detección y eliminación de fuego, sistemas de potencia eléctrica suplementarios y sistemas de aire acondicionado, entre otros.
- (b) Los microcomputadores y estaciones de trabajo se deben equipar con unidades suplementarias de energía eléctrica (UPS), filtros eléctricos, supresores de picos de corriente y, en lo posible, eliminadores de corriente estática.
- (c) Los sistemas de computación de comunicaciones deben en lo posible estar geográficamente dispersos.

José Carlos Salas



Dic. Jorge Luis Vega

Dirección Administrativa
Coordinación de Recursos Financieros



Dirección Administrativa

ANEXO DE LA RESOLUCIÓN DA N° 340/2013

- (d) El diseño de la red de comunicaciones debe estar de tal forma que se evite tener un punto crítico de falla, como un centro único de conmutación que cause la caída de todos los servicios.
- (e) Los backups de los sistemas de computación y redes deben ser almacenados en una zona de fuego diferente de donde reside la información original. Las zonas de fuego varían de edificio a edificio y son definidas por el área de seguridad de la entidad.
- (f) A todo equipo de cómputo, comunicaciones y demás equipos de soporte debe realizarse un mantenimiento preventivo periódico, de tal forma que el riesgo a fallas se mantenga en una probabilidad de ocurrencia baja.
- (g) Los planes de contingencia y recuperación de equipos deben ser probados regularmente con el fin de asegurar que el plan sea relevante, efectivo, práctico y factible de realizar. Cada prueba debe documentarse y sus resultados y las acciones de corrección deben comunicarse a la alta dirección.

5.1.4 Otros

- 1. Todos los procesos relacionados con el cifrado de datos deben ser soportados preferiblemente por módulos de hardware. Este sistema minimiza la amenaza de ingeniería inversa del software y una revelación de la(s) clave(s).
- 2. Ningún equipo portátil de computación de la Institución (laptop, notebook, palmtop, etc.) debe registrarse como equipaje de viaje. Estos deben llevarse como equipaje de mano.
- 3. Los equipos portátiles de computación que contengan información sensible deben utilizar software de cifrado para proteger la información.
- 4. Todo equipo de cómputo y de comunicaciones de la entidad debe tener un número (lógico y físico) de identificación permanente grabado en el equipo, además, los inventarios físicos se deben realizar en forma periódica, regular y eficientemente.
- 5. Todo equipo portátil debe tener Declaración de Responsabilidad, la cual incluya instrucciones de manejo de información y acato de normas internas y de seguridad para el caso de robo o pérdida.

6 POLÍTICA DE INSTALACIONES FÍSICAS

6.1 Seguridad Física

Todos los funcionarios de la entidad deberán seguir los siguientes lineamientos de seguridad física con el fin de salvaguardar los recursos técnicos y humanos de la entidad.

6.1.1 Control de acceso físico

La entidad debe contar con los mecanismos de control de acceso tales como puertas de seguridad, sistemas de control con tarjetas inteligentes y sistema de alarmas, en las dependencias que la entidad considere críticas.

6.1.1.1 Personas

- (a) Los visitantes deben permanecer escoltados y portar un distintivo o escarapela claramente visible, y las personas que laboran para la entidad que requieran ingresar a áreas críticas

Jorge Luis Vega
LICENCIADO EN ADMINISTRACIÓN
Coordinador de Recursos
Recursos Administrativos - D.A.
Ministerio de Hacienda



Jorge Luis Vega
Dirección Administrativa
Coordinación de Recursos Financieros



Dirección Administrativa

ANEXO DE LA RESOLUCIÓN DA N° 310 /2013

también deben permanecer escoltados. Además, tanto los visitantes como los empleados mencionados únicamente deben tener acceso a la información y recursos necesarios para el desarrollo de sus actividades.

- (b) En el evento que los funcionarios dejen de tener vínculos laborales con la entidad todos sus códigos de acceso deben ser cambiados o desactivados. Además, en caso de pérdida de la escarapela o tarjeta de acceso también deben desactivarse dichos códigos.
- (c) Se debe mantener el registro de acceso del personal autorizado y de ingresos con el objeto de facilitar procesos de investigación.
- (d) Como mecanismo de prevención todos los empleados y visitantes no deben comer, fumar o beber en el centro de cómputo o instalaciones con equipos tecnológicos, al hacerlo estarían exponiendo los equipos a daños eléctricos como a riesgos de contaminación sobre los dispositivos de almacenamiento.
- (e) Las reuniones de trabajo donde se discute y maneja información sensible, se deben realizar en salas cerradas para que personas ajenas a ella no tengan acceso.
- (f) Todos los sistemas de control de acceso deben ser monitoreados permanentemente.

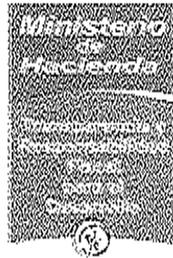
6.1.1.2 Equipos y Otros Recursos

- (a) Toda sede y equipo informático, ya sean propios o de terceros, que procesen información para la entidad o posean un vínculo especial con la misma, debe cumplir con todas las normas de seguridad física que se emitan, con el fin de evitar el acceso a personas no autorizadas a las áreas restringidas donde se procese o mantenga información secreta, confidencial y privada, y asegurar la protección de los recursos de la plataforma tecnológica y su información.
- (b) Los equipos de cómputo no deben moverse o reubicarse sin la aprobación previa del Departamento de Informática y el Administrador del Departamento involucrado.
- (c) Todos los equipos propiedad de la entidad como máquinas de escribir, teléfonos celulares, equipos portátiles, módems y equipos relacionados con sistemas de información NO podrán retirarse de las instalaciones físicas de la entidad por ningún personal, a menos que éste cuente con una autorización por escrito del Departamento de Informática y del Responsable de la dependencia.
- (d) Todo maletín, caja o bolso debe ser revisado por personal de seguridad tanto al momento de acceder a las instalaciones como al momento de salir de ellas en búsqueda de equipos y/o accesorios tecnológicos a fin de evitar el ingreso de equipos prohibidos o el retiro de equipos de la institución sin autorización.
- (e) No se debe proveer información sobre la ubicación del centro de cómputo, como mecanismo de seguridad.

6.1.2 Protección física de la información

- (a) Todas las personas que laboren para la entidad y/o aquellas designadas por las entidades para trabajar en actividades particulares (consultores y contratistas) son responsables del adecuado uso de la información suministrada para tal fin por lo cual se debe velar por su integridad, confidencialidad, disponibilidad y accesibilidad. Toda información secreta, confidencial y privada debe estar provista de la seguridad necesaria por quien la maneja para evitar el uso indebido por parte de personal no autorizado.





Dirección Administrativa

ANEXO DE LA RESOLUCIÓN DA N° 340 /2013

- (b) Al terminal la jornada laboral, los escritorios y áreas de trabajo deben quedar desprovistos de documentos sensibles que puedan comprometer los intereses de la entidad. Estos deben quedar bajo llave en archivadores, cajas fuertes o demás medios de almacenamiento físico seguros.
- (c) Las áreas donde se maneja información confidencial o crítica deben contar con cámaras que registren las actividades realizadas por los funcionarios.

6.1.3 Protección contra desastres

Dado que cualquier tipo de desastre natural o accidental ocasionado por el hombre (cortos circuitos, vandalismo, fuego, fugas químicas, movimiento de material nuclear, y otras amenazas etc.) puede afectar el nivel de servicio y la imagen de la entidad, se debe prever que los equipos de procesamiento y comunicaciones se encuentren localizados en áreas aseguradas y debidamente protegidas contra inundaciones, robos, interferencias electromagnéticas, fuego, humo y demás amenazas que puedan interferir con el buen uso de los equipos y la continuidad del servicio.

6.1.4 Planes de emergencia, contingencia y recuperación

- (a) Es responsabilidad de la administración de la Entidad el preparar, actualizar periódicamente y regularmente probar los planes de Contingencias, Emergencias y Recuperación previendo la continuidad de los procesos críticos para el negocio en el evento de presentarse una interrupción o degradación del servicio.
- (b) La Administración debe establecer, mantener y probar periódicamente el sistema de comunicación que permita a los usuarios de la plataforma tecnológica notificar posibles intromisiones a los sistemas de seguridad, estos incluyen posibles infecciones por virus, intromisión de hackers, divulgación de información no autorizada y debilidades del sistema de seguridad.
- (c) El plan de Contingencia y de Recuperación debe permanecer documentado y actualizado de manera tal que sea de conocimiento general y fácilmente aplicable en el evento de la presencia de un desastre. Permitiendo que los recursos previstos se encuentren disponibles y aseguren la continuidad de los procesos de negocio, en un tiempo razonable para cada caso y contemplando como mínimo los riesgos más probables de ocurrencia que afecten su continuidad.
- (d) El mantenimiento del plan de Contingencias y Recuperación general debe incluir entre otros un proceso estándar que integre los planes de contingencia para computadoras y comunicaciones, así como también el inventario de hardware, software existente y los procesos que correrán manualmente por un periodo de tiempo.

7 POLÍTICA DE ADMINISTRACIÓN DE LA SEGURIDAD INFORMÁTICA

Funciones y responsabilidades del Departamento Informática

7.1.1 Generalidades

- (a) El Departamento de Informática debe definir, implementar, controlar y mantener las políticas, normas, estándares, procedimientos, funciones y responsabilidades necesarias para preservar

16

José Luis Vega
Lic. Jorge Luis Vega
Dirección Administrativa
Coordinación de Recursos Financieros



Lic. Jorge Luis Vega
Dirección Administrativa
Coordinación de Recursos Financieros



Dirección Administrativa

ANEXO DE LA RESOLUCIÓN DA N° 340 /2013

- y proteger la confidencialidad, disponibilidad e integridad de la información de la Entidad donde ésta resida (aplicaciones, bases de datos, sistemas operativos, redes, backups y medios).
- (b) El área de Seguridad Informática, es la encargada de establecer, mantener y administrar una arquitectura de seguridad para la entidad y facilitar la incorporación de prácticas de seguridad de la información en todas las dependencias.
 - (c) El área de Seguridad Informática debe estar ubicada organizacionalmente de manera que tenga autonomía e independencia frente a las demás áreas de tecnología tales como: soporte, diseño y desarrollo, entre otras.
 - (d) Representar a la DA ante organizaciones externas sobre temas relacionados a las tecnologías de la información y a la seguridad de la información.
 - (e) Promover que los planes estratégicos y de operaciones de la DA estén alineados con las estrategias de seguridad del Ministerio de Hacienda.
 - (f) El área de seguridad debe velar porque las excepciones a las políticas de seguridad estén autorizadas únicamente por la Dirección Administrativa, de las cuales se debe dejar constancia de los riesgos que en forma consciente se están asumiendo y el período de vigencia de la excepción.

7.1.2 Funciones de Control

- (a) Establecer e implementar un plan de Seguridad que permita controlar el entorno lógico y físico de la información estratégica de la entidad, teniendo en cuenta los criterios de confidencialidad, integridad, auditabilidad, disponibilidad, autenticidad y no repudiación de la información.
- (b) Participar activamente en los proyectos informáticos de la entidad para proveerlos de las seguridades adecuadas, gerenciando los de Seguridad Informática.
- (c) Definir las directrices básicas de Seguridad Informática para la descripción de los diferentes requerimientos en la adquisición de tecnología (hardware y software) en la Entidad, y velar porque se realicen las pruebas de seguridad a los Sistemas de Información.
- (d) Participar activamente en el equipo de trabajo de análisis, implementación y mantenimiento de los perfiles de usuario que interactúan con los Sistemas Operativos, Bases de Datos y Aplicaciones, y velar porque en producción únicamente estén los autorizados y vigentes.
- (e) Contar con mecanismos de monitoreo con el fin de detectar oportunamente procedimientos inseguros para los Sistemas Operacionales, Aplicativos, Datos y Redes.
- (f) Desarrollar métodos y técnicas para monitorear efectivamente los sistemas de seguridad de la información y reportar periódicamente su efectividad a la Alta Dirección.
- (g) Direccionar, recomendar y aconsejar a todos los usuarios de los sistemas de información de la Dirección Superior en cuanto a la seguridad de la información.
- (h) Interactuar con los organismos de control interno y externo, apoyándolos en su gestión administrativa y de ejecución.
- (i) Asegurar que la organización cuente con ambientes independientes de Desarrollo, Pruebas, Producción y Capacitación.
- (j) Garantizar que todos los mantenimientos a los sistemas de misión crítica y prioritaria estén autorizados, probados e implementados de acuerdo con los requerimientos de los usuarios

17

Jorge Luis Vega
Lic. JORGE LUIS VEGA
Responsable Administrativo
Ministerio de Hacienda



Jorge Luis Vega
Dirección Administrativa
Coordinación de Recursos Financieros



Dirección Administrativa

ANEXO DE LA RESOLUCIÓN DA N° 340 2013

previamente validados por un grupo especializado y que no comprometan la seguridad informática de la organización. Además, que los sistemas de información queden correctamente documentados y se de la capacitación necesaria a los usuarios finales.

- (k) El Departamento de Informática, es responsable por la revisión continua de las Políticas de Seguridad de la información por lo menos una vez al año.

7.1.3 Comité de Seguridad Informática

- (a) El comité de Seguridad Informática será conformado por los representantes de los principales usuarios informáticos, aprobado por Resolución DA y liderado por el Departamento de Informática, donde se sustentará el plan de Seguridad Informática a ejecutar en la Entidad, desarrollado por el área informática, analizando la administración de problemas de seguridad y se definan las estrategias a implementar que permitan controlar el entorno lógico y físico de la información estratégica de la Entidad.

7.1.4 Soporte a Investigaciones

- (b) Realizar el Soporte de las investigaciones sobre violaciones a la seguridad de los sistemas en apoyo al área de Seguridad no Tecnológica (Física) y presentar los informes respectivos a la Dirección de la Organización.
- (c) Investigar, documentar e informar a los propietarios de la información los incidentes de seguridad tanto lógica como física.
- (d) Realizar seguimiento a las acciones disciplinarias y legales asociadas con los incidentes de seguridad investigados.

7.1.5 Elaboración del Mapa de Riesgo

- Efectuar estudios de análisis de riesgos en Seguridad Informática para identificar oportunamente los eventos o situaciones de fallos en los accesos o en el manejo de la información presentados en la Entidad, estableciendo planes de acción que incluyan controles para contrarrestarlos y reducir el riesgo a un nivel aceptable.

7.1.6 Plan de Contingencia

- (a) Preparar, implementar y mantener el Plan de Emergencia, Contingencia y de Recuperación de desastres y continuidad del negocio relacionados con tecnología informática.
- (b) Liderar el proceso de pruebas que se debe ejecutar periódicamente a los Planes de Emergencia, Contingencia y de Recuperación.

7.1.7 Capacitación y Entrenamiento

- (a) Establecer y apoyar a las áreas encargadas en la ejecución de un plan de Capacitación continuo que permita actualizar a los funcionarios en aspectos de seguridad informática fortaleciendo la cultura sobre el tema.
- (b) Dar un entrenamiento adecuado a los usuarios, estudios, y usuarios dueños de la información en cuanto a los requerimientos de responsabilidad sobre la seguridad de la información.

Jorge Luis Vega



Jac. Jorge Luis Vega
Dirección Administrativa
Coordinación de Recursos Financieros

18 | *Jorge Luis Vega*
Coordinación de Recursos Financieros
Ministerio de Hacienda