GOBIERNO DEL PARAGUAY | PARAGUÁI REKUÁI

DINAC

RESOLUCIÓN Nº 2249/2024

POR LA QUE SE APRUEBA EL MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN EN SU REVISIÓN 03 DE LA DIRECCIÓN NACIONAL DE AERONÁUTICA CIVIL (DINAC).----------

Asunción, 22 de noviembre de 2024

VISTO: El Memorándum MECIP N° 27/2024 de la de la Coordinación MECIP y la providencia de la Subdirección de Planificación (Expdte. N° 227772), y, ----------

CONSIDERANDO: Que, la Coordinación MECIP eleva el proyecto del Manual de Políticas de Seguridad de la Información en su Revisión 03, para aprobación por la Máxima Autoridad Institucional, conforme lo dispone la Resolución N° 1873/2022, que aprueba y establece la frecuencia de revisión del Manual de referencia.----------

Que, las Políticas de Seguridad de la Información, son las directrices de índole técnica y de organización que se llevan adelante respecto de un determinado sistema de computación a fin de proteger y resguardar su funcionamiento y la información en él contenida. Las políticas de seguridad de la información de la DINAC están orientadas a toda la información almacenada, procesada y transmitida en medios electrónicos.----------

Que, la Coordinación General de Tecnología de la Información y Comunicación como área institucional responsable de planificar, diseñar, desarrollar, mantener y mejorar los sistemas tecnológicos de información y comunicación, procedió a la revisión del Manual de Políticas de Seguridad de la Información, y cuyo borrador resultante se socializo a la Alta Dirección Institucional para su tratamiento participativo en sus respectivas dependencias a fin de proponer ajustes y/o cambios al mismo.----------

Que, el comité de Control Interno, en reunión de trabajo de fecha XX de octubre procedió a la revisión final y aprobación del Manual de Políticas de Seguridad de la Información, con la recomendación de proseguir con los trámites para aprobación mediante acto administrativo por la Máxima Autoridad Institucional.--

Que, la Subdirección de Planificación, por providencia eleva a la Presidencia de la DINAC el proyecto aprobado por el Comité de Control Interno para su aprobación por acto administrativo.----------

DIRECCIÓN NACIONAL DE AERONÁUTICA CIVIL DINAC SECRETARÍA GENERAL

Abg. NATALIA ACUÑA
Coordinadora
Gestión de Documentos
Secretaría General - DINAC

POR TANTO: De conformidad con la Ley Nº 73/90 "Carta Orgánica de la DINAC" modificada por la Ley Nº 2199/2003 "Que dispone la Reorganización de los Órganos Colegiados Encargados de la Dirección de Empresas y Entidades del Estado Paraguayo".----------

EL PRESIDENTE DE LA DIRECCIÓN NACIONAL DE AERONÁUTICA CIVIL

RESUELVE

Artículo 1º **Aprobar,** el Manual de Políticas de Seguridad de la Información en su Revisión 03 de la Dirección Nacional de Aeronáutica Civil (DINAC), que se adjunta y forma parte de la presente Resolución.----------

Artículo 2° **Encargar,** a la Coordinación General de Tecnología de Información y Comunicación la difusión y socialización del Manual aprobado por la presente Resolución, a través de capacitaciones, publicaciones y cualquier medio idóneo a todas las dependencias de la Institución, así como a los grupos de intereses internos y externos de la entidad.----------

..//2

Avda. Mcal. López esq. 22 de Setiembre
2do Piso. Teléfono: (021) 212 530
E-mail: sec_gral@dinac.gov.py
Asunción – Paraguay

RESOLUCIÓN Nº 2249 /2024

POR LA QUE SE APRUEBA EL MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN EN SU REVISIÓN 03 DE LA DIRECCIÓN NACIONAL DE AERONÁUTICA CIVIL (DINAC).----------

Artículo 3° **Notificar,** al Coordinación General de Tecnología de Información y Comunicación y a la Subdirección de Planificación----------

Artículo 4° **Abrogar,** la Resolución Nº 1873/2022 de fecha 14 de diciembre 2022, a partir de la presente resolución.----------

Artículo 5° **Comunicar,** a quienes corresponda, publicar en la Página Web de la DINAC, link MECIP, y cumplida archivar.----------

*Fdo. por Don Nelson Mendoza Rolón (***Presidente)**
Abg. Daniel A. Báez Argaña **(Secretario General)**

Es Copia fiel del Original

DIRECCIÓN NACIONAL DE AERONÁUTICA CIVIL DINAC SECRETARÍA GENERAL

Abg. NATALIA ACUÑA
Coordinadora
Gestión de Documentos
Secretaría General - DINAC

Avda. Mcal. López esq. 22 de Setiembre
2do Piso. Teléfono: (021) 212 530
E-mail: sec_gral@dinac.gov.py
Asunción – Paraguay

DINAC

DIRECCION NACIONAL DE AERONAUTICA CIVIL

COORDINACIÓN GENERAL DE TECNOLOGÍA DE INFORMACIÓN Y COMUNICACIÓN

"POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN"

DIRECCIÓN NACIONAL DE AERONÁUTICA CIVIL DINAC REPÚBLICA DEL PARAGUAY SECRETARÍA GENERAL

DIRECCIÓN NACIONAL DE AERONÁUTICA CIVIL DINAC REPÚBLICA DEL PARAGUAY PRESIDENCIA

POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

Tabla de contenido

C.P. Fredy A. Garay
Coordinador MECIP
DINAC

C.P. Fredy A. Garay
Coordinador MECIP
DINAC

DIRECCIÓN NACIONAL DE AERONÁUTICA CIVIL DINAC REPÚBLICA DEL PARAGUAY SECRETARÍA GENERAL

DIRECCIÓN NACIONAL DE AERONÁUTICA CIVIL DINAC REPÚBLICA DEL PARAGUAY PRESIDENCIA

C.P. Fredy A. Garay
Coordinador MECIP
DINAC

C.P. Fredy A. Caray
Coordinador MECIP
DINAC

GENERALIDADES

NATURALEZA DE LA DINAC

La Dirección Nacional de Aeronáutica Civil (DINAC) fue creada por Ley N° 73/90, como una entidad autárquica de duración ilimitada, con personería jurídica y patrimonio propio. Tendrá capacidad jurídica, financiera y administrativa; además facultad para planificar, proyectar y dirigir las obras y servicios que tienen por objeto ponerlas en funcionamiento y administrarlas, pudiendo a tales efectos, adquirir derechos y contraer obligaciones..." (Art. 1°, Ley N° 73/90).

MISIÓN

Normar las actividades relacionadas a la aviación civil y prestar servicios para satisfacer a las partes interesadas.

VISIÓN

Ser reconocida por los altos estándares de seguridad y la calidad de los servicios prestados.

C.P. Fredy A. Garay
Coordinador MECIP
DINAC

PARTE I – MARCO DE REFERENCIA

1. - Introducción a las Políticas de Seguridad de la Información

Con los avances en Internet y los desarrollos de la informática y las telecomunicaciones, la Seguridad de la Información, se ha convertido en figura necesaria para la protección, mantenimiento, control de acceso, confidencialidad, integridad y disponibilidad de la información, tanto para su seguridad como para la seguridad en el soporte de las operaciones de las organizaciones.

Las Políticas de Seguridad de la Información son las directrices de índole técnica y de organización que se llevan adelante respecto de un determinado sistema de computación a fin de proteger y resguardar su funcionamiento y la información en él contenida. El principio y final de toda red es el usuario, esto hace que las políticas de seguridad deban, principalmente, enfocarse a los usuarios, indican a las personas cómo actuar frente a los recursos informáticos de la Entidad.

Actualmente la Coordinación General de Tecnología de Información y Comunicación, cuenta con una plataforma tecnológica que almacena, procesa y transmite la información institucional, incluye equipos de cómputo de usuario y servidores que se interconectan por medio de una red de datos, así como servicio de internet y correo electrónico institucional. Siendo la información institucional un activo valioso para la Entidad, se hace necesario no solo la implementación de herramientas de hardware y software de seguridad, sino involucrar al personal para proteger su integridad y confidencialidad.

Los requerimientos de seguridad que involucran las tecnologías de la información, en pocos años han cobrado un gran auge, y más aún con las de carácter globalizador como los son Internet, la visión de nuevos horizontes explorando más allá de las fronteras naturales, situación que ha llevado la aparición de nuevas amenazas en los sistemas computarizados.

De esta manera, las políticas de seguridad de la Información de la DINAC emergen como el instrumento para concienciar a sus miembros acerca de la importancia y sensibilidad de la información y servicios críticos, de la superación de las fallas y de las debilidades, de tal forma que permiten al área cumplir con su misión.

El proponer esta política de seguridad requiere un alto compromiso con la institución, agudeza técnica para establecer fallas y deficiencias, constancia para renovar y actualizar dicha política en función del ambiente dinámico que nos rodea.

2. – Marco Normativo

a) Constitución Nacional
b) Convenio de Aviación Civil (Chicago 1944), ratificado por la República del Paraguay por Decreto-Ley Nº 10.818/45, y sus Anexos.
c) Código Aeronáutico, Ley Nº 1860/02 "Que establece el Código Aeronáutico de la República del Paraguay".
d) Ley Nº 1535/00 "De Administración Financiera del Estado"
e) Ley Nº 73/90 "Que aprueba, con modificaciones, el Decreto-Ley Nº 25/90, que crea la Dirección Nacional de Aeronáutica Civil (DINAC)" y su modificatoria Ley Nº 2.199/03.

C.P. Fredy A. Garay
Coordinador MECIP
DINAC

f) Resolucion Nº 460/2015 por la quie se aprueba el manual de organización y funciones de la DINAC.
g) Decreto Nº 7052/2017 Plan de Ciberseguridad.
h) Decreto Nº 6234/2016 Estructura TICS GOB.

3. - Objetivo, Alcance y Responsabilidad de las Políticas de Seguridad de la Información

Objetivo

Definir e implementar las políticas de seguridad de la Información que dan las pautas y rigen para la gestión, el uso adecuado y la seguridad de la información de los sistemas informáticos y en general, sobre el ambiente tecnológico de la Dirección Nacional de Aeronáutica Civil, para su interiorización, aplicación y verificación permanente.

Alcance

Las políticas de seguridad de la Información de la DINAC, están orientadas a toda la información almacenada, procesada y transmitida en medios electrónicos, estas políticas deben ser conocidas y cumplidas tanto por funcionarios, por terceros o grupos de interés que utilicen la información generada y por quienes hagan uso de los servicios tecnológicos de la Entidad.

Responsabilidad

Todo el Personal de la Institución sin distinción de rango o jerarquía es responsable por el cumplimiento de las Políticas, Normas, Estándares y Procedimientos vigentes con respecto a la Seguridad de la Información. La violación de las mismas puede acarrear las medidas disciplinarias y sanciones previstas en las normativas vigentes.

Parte II - Políticas Generales

3. - Política: Cultura de la Seguridad de la Información

3.1. Objetivo

Esta Política tiene como objetivo que los Usuarios tomen conciencia de la importancia de la Seguridad de la Información para la Institución.

3.2. Fundamentos

Concientizar a los Usuarios que:

- La información es uno de los recursos más valiosos de la Institución, y por lo tanto la seguridad de la información es responsabilidad diaria de todo el Personal.
- La pérdida de la información podría provocar la pérdida de horas/hombres invertidas en generar dicha información, así como muchas más horas/hombres en tratar de recuperarla.
- La información que se pierde fuera del ambiente de la Institución podría dañar la imagen de la institución y ocasionar serias pérdidas económicas.

3.3. Alcance y Sectores de Aplicación

Personal de la Institución y Terceras Partes asociadas con el mismo.

3.4. Definiciones

C.P. Fredy A. Garay
Coordinador MECIP
DINAC

Usuario: Persona física o jurídica que utiliza uno o varios recursos informáticos de la Institución para el desarrollo de sus tareas específicas.

3.5. Contenido

3.5.1. Concientización de la Seguridad

3.5.1.1.- Todos los Usuarios deben recibir una copia de las Políticas de Seguridad de la Información de la Coordinación General de Tecnología de la Información y Comunicación, tener acceso a las mismas y dejar constancia de su conocimiento.

3.5.1.2.- Todos los Usuarios deben recibir las actualizaciones por las modificaciones de las Políticas de Seguridad de la Información de la Coordinación General de Tecnología de la Información y Comunicación, y deben dejar constancia de su conocimiento y aceptación.

3.5.1.3.- El Encargado de Seguridad de la Información tiene la responsabilidad de concientizar a todos los sectores de la institución sobre la importancia de la Seguridad de la Información para la Institución.

3.5.1.4.- La Concientización de los Usuarios debe incluir como mínimo los siguientes temas:

a. Requerimientos de Identificación de Usuario y Contraseña.
b. Seguridad de las Computadoras Personales, incluyendo protección, reporte y eliminación de virus.
c. Conceptos generales de la Clasificación de la Información.
d. Tratamiento y destrucción de los diferentes tipos de información.
e. Concientización de las técnicas utilizadas por los Hackers.
f. Legalidad del software.
g. Normas de acceso y utilización de Internet.
h. Normas para el uso del Correo Electrónico.
i. Procesos vigentes para el monitoreo de la seguridad de la información.

3.5.1.5.- La Concientización a la Coordinación General de Tecnología de Información y Comunicación y sus miembros debe incluir como mínimo los siguientes temas:

a. Controles y Procedimientos de Seguridad.
b. Cuidado preventivo de los activos tecnológicos de la Institución.
c. Respuesta ante eventuales incidentes o contingencias.
d. Detección y respuesta a situaciones anormales.

3.5.2. Novedades sobre Aspectos de Seguridad

3.5.2.1.- Las novedades de seguridad deben ser publicadas para asegurar que todos los Usuarios que puedan verse afectados por las mismas tengan acceso a esta información.

3.5.2.2.- Las publicaciones de seguridad deben ser comunicadas por medio de documentos escritos, correos electrónicos u otro medio que disponga la Institución.

4. - Política: Personal de la Dirección Nacional de Aeronáutica Civil

4.1. Objetivo

Esta Política establece los lineamientos de seguridad para el personal de la Institución, Proveedores y Visitantes, con el fin de identificar y revocar su acceso cuando finalicen su relación laboral con la Institución.

4.2. Fundamentos

- Tomar medidas preventivas al contratar, trasladar o finalizar la relación/vínculo

C.P. Fredy A. Garay
Coordinador MECIP
DINAC

laboral con el empleado.

- Establecer controles para informar oportunamente a los Propietarios de Procesos y al Encargado de Seguridad de la Información, los cambios de personal y los requerimientos informáticos correspondientes.

4.3. Alcance y Sectores de Aplicación

Personal de la Dirección Nacional de Aeronáutica Civil y Terceras Partes asociadas con el mismo.

4.4. Definiciones

- Datos: Representa todo tipo de información, que es contenida o procesada por las facilidades de los sistemas de información, las redes, o los medios de almacenamiento de la Institución. Estos datos pueden encontrarse en diferentes formatos: copias impresas, medios magnéticos, etc.

- Proveedor: Para los propósitos de este documento, un proveedor es una persona o Institución que ofrece productos o servicios a la Institución.

4.5. Contenido

4.5.1. Transferencia o Baja de Personal

4.5.1.1.- Los responsables de los sectores conjuntamente con la Coordinación General de Tecnología de Información y Comunicación, deben notificar al Encargado de Seguridad de la Información la desvinculación o traslado de los Usuarios. El Encargado de Seguridad de la Información debe asegurar que el acceso del Usuario sea revocado en forma inmediata.

4.5.1.2.- Los Usuarios desvinculados y terceros que hayan cesado la relación con la Institución, deben entregar todos los objetos, propiedad de la Dirección Nacional de Aeronáutica Civil, tales como tarjetas de identificación, computadoras portátiles, llaves, software, datos, documentación, manuales, etc., a sus respectivos Jefes de Área.

4.5.1.3.- Las suspensiones o despidos de Usuarios deben ser comunicados a la Coordinación General de TIC en forma inmediata para asegurar que los permisos de acceso a la información de la Institución sean debidamente inhabilitados.

4.5.1.4.- Todos los archivos personales de un Usuario desvinculado que permanezca en la red o en el disco rígido de la computadora personal que le fuera asignada, deben ser reasignados a otro Usuario, a menos que el responsable del área especifique lo contrario, en cuyo caso se debe proceder a su eliminación en el plazo estimado según el procedimiento determinado por la Coordinación General de Tecnología de la Información y Comunicación e informando al Encargado de Seguridad de la Información.

4.5.2. Seguridad de Accesos

4.5.2.1.- En los casos de desvinculaciones de Usuarios con acceso a datos altamente Privados/confidencial, el responsable del Área (Gerente o Jefe) juntamente con la Coordinación General de TIC y el Encargado de Seguridad de la Información, deben coordinar la remoción de los derechos de acceso del Usuario.

4.5.2.2.- Cuando un Usuario es dado de baja o transferido, el Responsable del Área debe revisar su documentación y archivos electrónicos, determinar quién es el nuevo propietario de dicha información y decidir los métodos apropiados para utilizar esa información.

5.- Política: Legalidad del Software

C.P. Freddy A. [illegible]
Coordinador MECIP
DINAC

5.1. Objetivo

Establecer los requisitos para proteger la propiedad y regular el uso del Software Corporativo y de Terceros.

5.2. Fundamentos

- Contar con licencias de Software homologadas y aprobadas para prevenir obligaciones legales.
- Asegurar que el software está siendo bien utilizado por el Personal y Terceras Partes.
- Respetar los acuerdos de licencias de software y las normas establecidas al respecto.

5.3. Alcance y Sectores de Aplicación

Personal de la DINAC y Terceras Partes asociadas con el mismo.

5.4. Definiciones

Autorización: Permisos concedidos, asociados con la ID-Usuario o Perfil de un Usuario.

5.5. Contenido

5.5.1. Licencias de Software

5.5.1.1.- Los acuerdos de licencias de software pueden especificar restricciones de uso que deben ser respetadas. Estas restricciones pueden ser: número de copias permitidas a instalar, el número de computadoras sobre las cuales se puede instalar, o el número de usuarios concurrentes permitidos por el software.

5.5.1.2.- El uso o copia del software adquirido para ser utilizado en otra computadora que no sea para la cual ha sido licenciado, está estrictamente prohibido. El incumplimiento de esta Política puede tener consecuencias legales para el Usuario y/o la Institución.

5.5.1.3.- No está permitido instalar, utilizar o ejecutar productos o software de diagnóstico de la seguridad. Si la ejecución responde a necesidades de trabajo se debe obtener la autorización previa del Encargado de Seguridad de la Información. Cualquier uso no autorizado de estos programas será considerado como una violación severa de las Políticas de Seguridad de la Institución.

5.5.1.4.- El Encargado de Seguridad de la Información debe realizar revisiones periódicas sobre la utilización de las computadoras personales, computadoras portátiles y servidores de la Institución, para asegurar que éstas cumplen con los acuerdos de licencias. Todo software que no respete las normas de la Institución debe ser removido inmediatamente.

5.5.2. Derechos de Autor de Software

5.5.2.1.- Todos los Usuarios de los sistemas de información de la Institución deben cumplir estrictamente con las leyes de derecho de autor (Copyright), así como también las restricciones detalladas por el fabricante.

5.5.3. Instalación y Uso de Programas y Utilitarios de Libre Utilización en la Institución.

5.5.3.1.- La Coordinación General de Tecnología de Información y Comunicación debe aprobar todos los programas y utilitarios de libre utilización para ser incorporados como recursos informáticos de la Institución e informar al Encargado de Seguridad de la Información sobre dicha aprobación.

5.5.3.2.- Los Usuarios no están autorizados a instalar programas o utilitarios en las PC´s propiedad de la Institución. Esta atribución es única de la Coordinación General de Tecnología de Información y Comunicación, cualquier excepción debe ser aprobada por el Encargado de

C.P. Ing. A. Gara
Coordinador MECIP
DINAC

Seguridad de la Información.

5.5.3.3. – Los Usuarios no están autorizados a compartir recursos de las PC's propiedad de la Institución. Esta atribución es única de la Coordinación General de Tecnología de Información y Comunicación, cualquier excepción debe ser aprobada por el Encargado de Seguridad de la Información.

5.5.3.4.- Todos los programas y utilitarios deben estar licenciados y cumplir estrictamente con las leyes derecho de autor (Copyright), así como también con las restricciones detalladas por el fabricante.

5.5.4. Propiedad del Software

5.5.4.1.- El software desarrollado por personal de la Institución es propiedad de la Dirección Nacional de Aeronáutica Civil. Esta norma previene cualquier disputa posterior acerca de la propiedad del software. Esta norma debe ser aplicada a las Terceras Partes que hayan desarrollado el software o aplicaciones para uso de la Dirección Nacional de Aeronáutica Civil.

5.5.4.2.- El software o aplicaciones desarrolladas interna o externamente para uso de la Institución, debe ser registrado a nombre de la Dirección Nacional de Aeronáutica Civil. En caso de que la Coordinación General de Tecnología de Información y Comunicación lo considere necesario, el Asesor Legal debe intervenir en el convenio escrito entre las partes, donde se acuerde la registración del derecho de propiedad intelectual.

6.- Política: Informe de Incidente

6.1. Objetivo
Definir lineamientos para actuar ante Incidentes de Seguridad, a fin de garantizar su solución y evitar que se repitan.

6.2. Fundamentos
Asegurar que el Personal de la Institución:

- Confeccione oportunamente un informe de incidentes ante una potencial o real violación de la seguridad que afecte a los recursos de información de la Institución.
- Se involucre en la solución de los Incidentes de Seguridad.

6.3. Alcance y Sectores de Aplicación
Esta Política se aplica a todo el Personal de la Institución y Terceros relacionados con el mismo.

6.4. Contenido

6.4.1. Informe sobre las Violaciones de Seguridad

6.4.1.1.- El conocimiento de cualquier mal funcionamiento de Software/hardware de la Institución, aparente o comprobado, que pueda comprometer la Integridad o Confidencialidad de la Información de la Dirección Nacional de Aeronáutica Civil, debe ser inmediatamente reportado al Encargado de Seguridad de la Información.

6.4.1.2.- El conocimiento de cualquier problema o violación de la seguridad de los sistemas informáticos, así como de puntos vulnerables del mismo, debe ser inmediatamente reportado al Encargado de Seguridad de la Información.

6.4.1.3.- No se debe comunicar información sobre violaciones de seguridad a otros Usuarios y a Terceros.

6.4.1.4.- Todo Usuario que en forma deliberada actúe en contraposición a lo dispuesto en la

C.P. Fredy A. Garay
Coordinador MECI
DINAC

presente norma puede recibir sanciones disciplinarias de acuerdo con la gravedad del hecho.

6.4.1.5.- El informe de incidentes debe incluir la detección de actividades maliciosas, u otro proceder que afecten al funcionamiento o correcto uso de los recursos de información.

6.4.2.- Manejo de Incidente de Seguridad

6.4.2.1.- El Encargado de Seguridad de la Información es responsable de conducir las investigaciones relacionadas con cualquier incidente, intento y/o violación de la seguridad determinando la severidad del incidente.

6.4.2.2.- Los Incidentes de Seguridad deben ser corregidos por acciones determinadas por el Encargado de Seguridad de la Información y la Coordinación General de TIC.

6.4.2.3.- El Encargado de Seguridad de la Información debe registrar en detalle el curso de acción seguido para la solución de los Incidentes de Seguridad.

6.4.2.4.- Cuando haya evidencia de que la Institución ha sido víctima de un delito informático, debe ser llevada a cabo una investigación que provea información suficiente para prevenir futuros incidentes y, de corresponder, establecer las medidas disciplinarias correspondientes.

6.4.2.5.- Para los incidentes o amenazas, se deben tomar acciones que aseguren que la integridad de que la evidencia es mantenida y que puede ser aplicada una acción legal.

7. - Política: Excepciones

7.1. Objetivo

Establecer los lineamientos que el personal de la Institución debe seguir para identificar cualquier excepción a las Políticas y Normas de Seguridad de la información con el fin de procurar la efectiva continuidad de las actividades del negocio.

7.2. Fundamentos

- Contemplar la posibilidad de que ciertas actividades de la Institución puedan entrar en conflicto con las Políticas de Seguridad de la Dirección Nacional de Aeronáutica Civil.
- Proveer de flexibilidad a las actividades de la Institución.
- Establecer criterios para cumplir con los casos de excepción.

7.3. Alcance y Sectores de Aplicación

Esta Política se aplica a todo el Personal de la Institución y Terceros asociados con el mismo.

7.5. Contenido

7.5.1. Procedimientos de Solicitud de Excepciones

7.5.1.1.- Las solicitudes de excepciones deben ser documentadas y justificadas en forma escrita, y contar con las aprobaciones necesarias para que se consideren válidas.

7.5.1.2.- Las excepciones deben ser aprobadas como mínimo por el Encargado de Seguridad de la Información.

7.5.1.3.- Las excepciones aprobadas deben contar con un plazo de validez. En la fecha de vencimiento deben ser nuevamente evaluadas y en caso de persistir la necesidad de excepción, aprobadas por un nuevo plazo.

7.5.1.4.- En caso que las excepciones evadan los controles existentes, se deben implementar y realizar nuevos controles para minimizar los riesgos o compensar los controles existentes. Esta situación debe ser incluida en la documentación de las excepciones, detallando los controles existentes reemplazados y los compensaotrios implementados.

C.P. Fredy A. Garay
Coordinador MECIP
DINAC

7.5.1.5.- El Encargado de Seguridad de la Información debe ser informado de todas las situaciones en que los controles internos de seguridad sean violados.

Parte III - Políticas de Seguridad de la Información

8. - Política: Uso de Red y Computadoras

8.1. Objetivo

Esta Política establece los lineamientos para el uso adecuado de los recursos informáticos y de telecomunicaciones; a la información almacenada o transmitida por computadoras, redes o cualquier otro dispositivo de comunicación, como el uso y la protección física de dichos dispositivos.

8.2. Fundamentos

- Normar el uso adecuado y la protección de los recursos y de la información de la Institución.
- Determinar la responsabilidad y obligación de cada Usuario para asegurar que todos los recursos informáticos y de comunicaciones sean protegidos del uso no autorizado.

8.3. Alcance y Sectores de Aplicación

Todo el Personal de la Dirección Nacional de Aeronáutica Civil y Terceras Partes relacionadas con el mismo.

8.4. Definiciones

- Firewall: Hardware/Software utilizado para proteger la Red de la Institución.
- Plataforma: Cada uno de los distintos ambientes tecnológicos que pertenecen a la Institución.

8.5. Contenido

8.5.1. Programas Antivirus

8.5.1.1.- Todos los Servidores, Computadoras Personales y Computadoras Portátiles deben tener instaladas y activadas versiones actualizadas de programas/sistemas de protección contra software malicioso.

8.5.1.2.- Se deben establecer mecanismos automáticos y/o manuales de actualización periódica de las versiones de los programas/sistemas de protección contra software malicioso que se utilizan. En la adquisición de programas antivirus debe ser previsto tanto el mantenimiento como la actualización de dicho software.

8.5.1.3.- El software antivirus debe verificar las Computadoras Personales en el momento del encendido y permanecer residente durante la sesión de trabajo. El disco rígido debe ser completamente verificado, como mínimo, una vez por semana o según se defina en el procedimiento respectivo.

8.5.1.4.- Todo soporte de almacenamiento externo debe ser verificado antes de ser utilizado (Ej. Pen Drive, CD´s, etc.).

8.5.1.5.- El Usuario debe conocer el procedimiento de utilización de recursos de TI para:

a. No debe abrir directamente los archivos ejecutables recibidos por Correo Electrónico o bajados de Internet, sino que debe elegir la opción "Archivo / Guardar" que permitirá la detección de posibles virus.

C.P. Fredy A. Garay
Coordinador MECIP
DINAC

b. Debe tener en cuenta que las extensiones de los archivos ejecutables (exe, com, bat, dll, etc.), aunque no contengan virus, cuando han sido bajados de Internet o de otros sitios que no son confiables, pueden provocar daños a las computadoras o introducir vulnerabilidades en los sistemas.

8.5.1.6.- El Usuario no está autorizado a eliminar un virus presente en su computadora utilizando un programa antivirus que no sea el aprobado por el Encargado de Seguridad de la Información o la Coordinación General de TIC.

8.5.2. Correo Electrónico

8.5.2.1.- Los mensajes de Correo Electrónico deben ser considerados como documentos formales. Cuando se redactan los Correos Electrónicos, los Usuarios deben respetar lineamientos éticos y buenas costumbres en el uso del lenguaje.

8.5.2.2.- Los sistemas de Correo Electrónico de la Institución no deben ser utilizado para:

a. Enviar cadenas de mensajes.
b. Enviar mensajes de seguridad, que no fueron originados por el Encargado de Seguridad de la Información y la Coordinación General de Tecnología de Información y Comunicación.
c. Relacionarse con actividades ilegales, no éticas o inapropiadas.
d. Relacionarse con los propósitos ajenos de la Institución.

8.5.2.3.- No deben ser enviados Correos Electrónicos de la Institución con Información Privada a destinatarios externos.

8.5.2.4.- La Información del Correo Electrónico de la Institución no es considerada privada para la Dirección Nacional de Aeronáutica Civil.

8.5.2.5.- Los Sistemas de Correo Electrónico deben brindar la facilidad de mitigar que un Usuario reciba correos de un remitente que puede poner en peligro los recursos de la Institución, o que contenga material no autorizado.

8.5.2.6.- Los Usuarios no deben utilizar el Correo Electrónico de otra persona.

8.5.2.7.- La utilización de Casillas de Correo Genéricas deben cumplir con los procedimientos de solicitud de excepciones.

8.5.2.8.- Los envíos y recepción de correo electrónico deberán ser autenticados por usuario y contraseña.

8.5.2.9.- La institución establecerá las restricciones o límites en cuanto a almacenamiento de correo electrónico por usuario.

8.5.3.- Gestión de Usuarios

8.5.3.1.- Los accesos a los sistemas de información serán otorgados mediante normativas vigentes que respalden sus funciones. El usuario debe firmar una declaración que lo ponga en conocimiento de la actividad que desarrolle sobre los recursos informáticos de la Institución. Al funcionario de la institución le será asignado un identificador informático o código de usuario y clave de acceso, mediante solicitud que respalde el otorgamiento del acceso o autorización expresa del superior inmediato.

8.5.4. Valores Predeterminados de los Sistemas

8.5.4.1. Para evitar posibles incidencias de seguridad, los valores predeterminados, o parámetros, de los sistemas deben ser revisados antes de su instalación en la Coordinación General de Tecnología de Información y Comunicación. Aquellos valores que puedan

C.P. Fredy A. Garay
Coordinador MECIP
DINAC

comprometer potencialmente la seguridad deben ser modificados, antes de ser implementados en producción.

8.5.4.2.- El Encargado de Seguridad de la Información debe verificar que los valores predeterminados, o parámetros relacionados con la seguridad, hayan sido configurados de acuerdo con los estándares de seguridad de la Plataforma.

8.5.4.3.- Las Contraseñas de acceso predeterminadas otorgadas por proveedores de software y/o hardware deben ser cambiadas antes de que el sistema comience a ser utilizado en producción.

8.5.4.4.- El Encargado de Seguridad de la Información debe asegurar que se implementen todas las mejoras relacionadas con la vulnerabilidad en la seguridad de la Plataformas tecnológicas de la Institución.

8.5.5. Encriptación

8.5.5.1.- Todos los datos de la Institución deben ser encriptados cuando son transmitidos por conexiones sensibles. Para este fin deben ser utilizados vínculos de comunicaciones encriptados por hardware o por software de encriptación aprobados por la Coordinación General de Tecnología de Información y Comunicación.

8.5.5.2.- Las Terceras Partes que deban conectarse a las computadoras o redes de la Institución, deben cumplir con los requerimientos de encriptación establecidos por la Dirección Nacional de Aeronáutica Civil para este tipo de conexiones.

8.5.5.3.- Las conexiones a Internet realizadas por la Institución deben utilizar un protocolo de comunicación encriptado cuando sean informaciones sensibles que se establecerán en los procedimientos.

8.5.6. Destrucción de la Información en Medios Electrónicos

8.5.6.1.- Toda información almacenada, en dispositivos ópticos y/o electrónicos de uso temporal, deberán ser conservados correctamente, especificando los datos contenidos en dicho dispositivo, para posteriormente ser eliminada del dispositivo de uso transitorio o temporal.

8.5.6.2.- Todos los equipos que pasen por un proceso de baja patrimonial, serán pasibles de borrado de la información contenida, antes de su transferencia final.

8.5.7. Almacenamiento de Información

8.5.7.1.- La información confidencial almacenada en medios electrónicos debe ser protegida de daños accidentales o maliciosos y de accesos no autorizados. El Encargado de Seguridad de la Información debe definir los procedimientos de seguridad física para estos casos.

8.5.7.2.- La información considerada Pública, puede ser almacenada en cualquier sistema computarizado de la Institución.

8.5.7.3.- El almacenamiento de la información confidencial debe ser asegurada mediante los siguientes procedimientos:

a. El acceso al recinto donde reside la información debe ser restringido y controlado. El recinto debe mantenerse cerrado mientras se encuentre desocupado. Solo el personal autorizado debe contar con acceso al recinto. El Personal de Limpieza y cualquier otro individuo no autorizado debe ser escoltado al ingresar al recinto.
b. La información debe ser almacenada utilizando un método aprobado por el Encargado de Seguridad de la Información.

8.5.7.4.-Toda vez que se transfiere datos de producción a una Computadora Personal,

C.P. Fredy A. Garay
Coordinador MECIP
DINAC

a. El Usuario debe contar con la aprobación del Encargado de Seguridad de la Información y personal de la Coordinación General de Tecnología de Información y Comunicación.
b. El Encargado de Seguridad de la Información debe asegurarse que la Computadora Personal de destino cuenta con los esquemas de seguridad adecuados.

8.5.8. Uso de Internet y Correo Externo

8.5.8.1.- Los casos especiales de conectividad a Internet debe ser otorgada mediante una autorización de la Coordinación General de Tecnología de Información y Comunicación para propósitos relacionados con el negocio.

8.5.8.2.- El Encargado de Seguridad de la Información y la Coordinación General de Tecnología de Información y Comunicación son responsable de evaluar los riesgos de seguridad y aprobar toda información que sea gestionada en los servidores.

8.5.8.3.- Toda información confidencial o sensible, enviada a través de Internet debe ser encriptada, caso contrario puede ser accedida, alterada y/o publicada por cualquier individuo.

8.5.8.4.- La Coordinación General de Tecnología de Información y Comunicación es el responsable de trasladar la información aprobada al Servidor de Internet, y de aprobar e implementar todos los cambios sobre los Servidores de Correo.

8.5.8.5.- Los procedimientos de control de cambios de la Institución deben ser respetados.

8.5.8.6.- Los accesos a los Servidores de Datos y/o Aplicaciones a través de Internet no deben ser implementados en caso que los riesgos de seguridad excedan los beneficios de otorgar tales accesos. Cuando una norma legal requiera que una información sea publicada o dada a conocer por medio de Internet, el Encargado de Seguridad de la Información determinará las medidas apropiadas a implementar para asegurar el cumplimiento de dicha norma legal.

8.5.8.7.- La administración del proceso de otorgar autorizaciones de acceso a los Clientes/Usuarios para acceder desde la Red Pública (Internet) a los Servidores de la Institución debe ser realizada por la Coordinación General de Tecnología de Información y Comunicación.

8.5.8.8.- Las Contraseñas utilizadas para identificar a Usuarios y/o Clientes que acceden a servidores de la Institución desde la Red Pública (Internet) deben cumplir con los requisitos establecidos en las Políticas de Seguridad de la Dirección Nacional de Aeronáutica Civil.

8.5.8.9.- Los Usuarios autorizados para acceder a Internet, deben utilizar como medio de comunicación el software y el hardware de salida provisto por la Institución.

8.5.8.10.- La conexión a Redes Públicas como Internet para casos de equipos externos debe ser realizada desde un Firewall que controle que la totalidad del tráfico entrante y saliente a la Red Interna es el autorizado.

8.5.8.11.- El Sistema Operativo del Firewall debe estar configurado de modo que no se puedan eludir los controles establecidos. Esta configuración periódicamente o al producirse cambios sobre los sistemas relacionados con Internet.

8.5.8.12.- El uso de Internet debe ser verificado periódicamente. Si existe alguna razón para creer que la seguridad está siendo violada, el Encargado de Seguridad de la Información puede revisar el contenido de las comunicaciones de Internet.

8.5.8.13.- Los Usuarios deben tomar conocimiento que el acceso a Internet está siendo registrado y verificado.

8.5.8.14.- Está prohibida la utilización de cookies u otros medios no autorizados para capturar sin su consentimiento, información de las personas que visitan las páginas o servidores de Internet

C.P. Frady A. Garay
Coordinador MECIP
DINAC

de la Institución.

8.5.9. Actividades No Relacionadas con el Negocio

8.5.9.1.- No se autoriza el uso de recursos informáticos de la Institución a los Usuarios para actividades no relacionadas con el ramo.

8.5.9.2.- El Correo Electrónico e Internet no pueden ser utilizados para otra actividad que no esté relacionada con las actividades de la Institución.

8.5.9.3.- El acceso a los sitios de Internet que se consideren ofensivos se encuentra estrictamente prohibido.

8.5.9.4.- Las Computadoras y Sistemas de la Institución no pueden ser utilizadas para beneficio personal de los Usuarios. Como uso personal también se entiende el ofrecer o vender productos o servicios, otras actividades comerciales, etc.

8.5.9.5.- En caso que se sospeche que se está realizando un uso inadecuado del equipamiento de la Institución, el Encargado de Seguridad de la Información tiene el derecho de examinar sin previo consentimiento o notificación al Usuario, cualquier información que sea transmitida o resguardada por los recursos informáticos de la Institución.

8.5.10. Uso de Computadoras Personales y Portátiles

8.5.10.1.- Todas las computadoras personales (PC's) y portátiles (notebook) de la Institución deben tener como fondo de escritorio y protector de pantalla, imágenes institucionales.

8.5.10.2.- Los Usuarios a quienes se les hace entrega de computadoras portátiles (notebook) son responsables de la custodia de los mismos.

9.- Política: Seguridad de la Información

9.1. Objetivo

Establecer los lineamientos para asegurar una adecuada protección de la información de la Institución que es almacenada, procesada y transmitida por equipamientos informáticos.

9.2. Fundamentos

Proteger y utilizar adecuadamente la información de la Institución, para asegurar una correcta administración de las operaciones y actividades del negocio.

9.3. Alcance y Sectores de Aplicación

Es responsabilidad y obligación de los Propietarios de Procesos, la aplicación de esta Política para asegurar que todos los recursos de información sean protegidos de accesos no autorizados.

9.4. Definiciones

- Integridad: Que la información y los datos sean protegidos contra modificaciones no autorizadas.
- Confidencialidad: Que la información y los datos sean divulgados solamente entre aquellos individuos que tienen derecho a conocerlos.
- Disponibilidad: Que los Sistemas de Aplicación estén disponibles y utilizables cuando sea preciso.

9.5. Contenido

C.P. Fredy A. Garay
Coordinador MECIP
DINAC

9.5.1. Protección de la Información

9.5.1.1.- Todo archivo de datos almacenado, transmitido o procesado es propiedad de la Institución y por lo tanto está prohibida su venta o divulgación sin autorización.

9.5.1.2.- Toda información confiada por Terceros para ser almacenada, transmitida o procesada por la Institución debe ser tratada y protegida como lo especifique el contrato correspondiente, o en su defecto debe ser considerada como Información confidencial propia de La Dirección Nacional de Aeronáutica Civil.

9.5.1.3.- Toda transferencia de información a un tercero debe ser previamente aprobada por la Coordinación General de Tecnología de Información y Comunicación y el Encargado de Seguridad de la Información.

9.5.1.4.- No está permitido informar a Terceros nombres, posiciones o cargos, teléfonos etc. del Personal de la Institución, a menos que sea necesario para conducir las actividades del negocio.

9.5.1.5.- No está permitido realizar copias de información clasificada como confidencial en computadoras portátiles sin la autorización formal de las áreas involucradas en la generación de dicha información.

9.5.1.6.- La información clasificada como Privada no debe ser copiada o transferida de un determinado ambiente de Sistemas a otro, a menos que se asegure que los controles de confidencialidad vigentes en la ubicación de destino se corresponden con los de origen.

9.5.1.7.- Todo documento impreso conteniendo Información Privada debe ser almacenado en un lugar seguro o de acceso restringido fuera del horario de trabajo.

9.5.1.8.- Todo documento impreso conteniendo Información confidencial debe ser destruido en caso de no ser necesaria su conservación.

9.5.2. Propiedad de la Información

9.5.2.1.- Todo mensaje o documento generado por los Usuarios en computadoras o equipos de la Institución es considerado propiedad de la Institución.

9.5.2.2.- En el caso de sospechar o tomar conocimiento de incidentes involucrando la pérdida, divulgación o venta de Información Privada, los Usuarios deben informar a sus superiores y al Encargado de Seguridad de la Información.

9.5.2.3.- Ningún Personal de la Institución puede firmar un acuerdo de confidencialidad con un tercero sin la aprobación del Asesor Legal.

9.5.2.4.- El Encargado de Seguridad de la Información y el personal de la Coordinación General de Tecnología de Información y Comunicación están autorizados a examinar archivos personales de los Usuarios almacenados en sus computadoras personales, cuando haya sospecha o se tenga conocimiento de malware, actividades no autorizadas, caídas de los Sistemas, violaciones a la seguridad, entre otros eventos que afecten a la seguridad.

10.- Política: Conexión y Autenticación

10.1. Objetivo

Establecer los requerimientos de conexión y autenticación para acceder a los Recursos Informáticos de la Institución.

10.2. Fundamentos

Proteger los recursos de información de la Institución, controlando el acceso de las personas a la información.

C.P. Fredy A. Garay
Coordinador MECIP
DINAC

10.3. Alcance y Sectores de Aplicación

Esta Política se aplica al Personal y Terceras Partes que accedan y administren el acceso a los recursos de información de la Institución.

10.4. Definiciones

- **Accesos Privilegiados:** Perfil de Usuario que maneja permisos especiales o superiores al normal, ya sea por sus parámetros de definición (ej. Contraseña que no expira), por las funciones que puedan ejecutar (ej. Administradores de Bases de Datos) o por el acceso que posean a recursos (ej. Acceso a todos los archivos de un sistema o ambiente).

- **Autenticación:** Proceso mediante el cual un sistema computarizado confirma la ID-Usuario de un Usuario a través de la validación de una cuenta y un esquema de verificación de Contraseñas.

- **Formulario:** Formato impreso o digital que debe ser completado con un determinado propósito (Ej. Autorización de Acceso a un determinado recurso).

- **Perfil:** Es el conjunto de privilegios y accesos que tiene asignados un Usuario para poder acceder a un sistema.

- **Software de Base:** Conjunto de programas y datos que cumplen una o varias funciones relativas a generar un ambiente de trabajo adecuado para el correcto funcionamiento de los sistemas aplicativos.

10.5. Contenido

10.5.1. Requisitos de Acceso

10.5.1.1.- La Coordinación General de Tecnología de Información y Comunicación debe autorizar al Usuario, a través de la Planilla de Autorización de Acceso al Sistema, para que pueda acceder a los recursos informáticos requeridos para su función y normativas relacionadas al traslado, rotación o a las designaciones.

10.5.1.2. - Toda Solicitud para una nueva Identificación de Usuario o cambio en los permisos de acceso debe ser entregado por escrito mediante un formulario físico o electrónico. La Solicitud debe ser aprobada por el Jefe Inmediato.

10.5.1.3.- La Solicitud debe incluir como mínimo la siguiente información:

- Nombre y Apellido completo del Usuario para el que se solicita el acceso.
- Número de Documento de identificación.
- Cargo, función y/o Perfil del Usuario.
- Fecha de Solicitud.
- Fecha para la cual el acceso es requerido.
- Nombre del Área que pertenece el Usuario que lo solicita.
- Identificación y cargo de quien autoriza dicho pedido.

10.5.1.4.- El acceso a los recursos informáticos sólo debe ser concedido luego de que los Usuarios hayan finalizado con toda la documentación y procesos requeridos.

10.5.1.5.- Todo Usuario que acceda a computadoras, sistemas o utilitarios de la Institución debe haber firmado previamente un documento de confidencialidad y aceptación de las responsabilidades que le competen en relación a las Políticas de Seguridad de la Dirección Nacional de Aeronáutica Civil.

10.5.1.6 – En el caso de usuarios genéricos, se debe seguir los mismos lineamientos utilizados

C.P. Fredy A. Garay
Coordinador MECIP
DINAC

para todos los usuarios, previo comunicado vía email a la Coordinación General de Tecnología de Información y Comunicación. Estas cuentas deben tener una fecha de expiración de modo de que sean revocadas una vez finalizado el periodo.

10.5.1.7 – Las cuentas genéricas deben tener un responsable físico que será quien gestione y firme la solicitud de acceso.

10.5.2. Identificación de Usuario y Cambio de Contraseñas

10.5.2.1.- Antes de comenzar a utilizar los Recursos Informáticos de la Institución, los Usuarios deben ser reconocidos por la Plataforma a la que se vinculan por medio de una Identificación de Usuario y una Contraseña de acceso secreta, o por otros medios que proporcionen igual o mayor seguridad.ñ

10.5.2.2.- Los Usuarios de los Sistemas de la Institución solo deben tener una Identificación de Usuario por Plataforma.

10.5.2.3.- La Identificación de Usuario debe pertenecer en forma unívoca y exclusiva a un Usuario.

10.5.2.4.- Las Identificaciones de Usuarios que se han desvinculados de la Institución no deben ser reutilizadas.

10.5.2.5.- Los Usuarios son responsables por toda actividad realizada con su Identificación de Usuario.

10.5.2.6.- Los Identificaciones de Usuarios sólo deben ser utilizados por aquellos Personales de la Institución a los que se les haya asignado.

10.5.2.7.- Los Usuarios no deben permitir que otros Usuarios realicen actividades con su Identificación de Usuario. De la misma forma, no tienen permitido realizar actividades con la Identificación de Usuario de otro Personal.

10.5.2.8.- Debe ser empleado el uso de software o utilitarios de seguridad para forzar a los Usuarios a cambiar sus Contraseñas a ser desarrollado en un procedimiento.

10.5.2.9.- Solo debe ser permitida una sola sesión por Usuario (por aplicación y por dispositivo), salvo que existan razones operativas expresamente autorizadas por la Coordinación General de TIC.

10.5.3. Autenticación

10.5.3.1.- Solo deben acceder a los Sistemas los Usuarios autenticados. Para ello deben identificarse mediante una contraseña, huellas dactilares, tarjetas inteligentes, firmas digitales u otro medio de reconocimiento aprobado por el Departamento de Desarrollo de Sistemas.

10.5.3.2.- El inicio de sesión de los Sistemas debe incluir un texto aclaratorio que explique que, a partir del presente acceso, toda información es propiedad de la Institución y solo puede ser accedida por personal autorizado y por una necesidad relacionada con su trabajo.

10.5.4. - Certificados de Accesos

10.5.4.1.- Los Propietarios de Procesos son los responsables por revisar periódicamente los perfiles de acceso a los Sistemas y de solicitar la revocación inmediata de todos los privilegios que no sean requeridos para dichos perfiles o funciones.

10.5.4.2.- El Encargado de Seguridad de la Información es responsable por asegurar que los Propietarios de Procesos sean provistos de los reportes adecuados para la revisión de los accesos y privilegios que poseen los Usuarios.

C.P. Fredy A. Garay
Coordinador MECIP
DINAC

10.5.4.3.- El Encargado de Seguridad de la Información es responsable por revisar con periodicidad anual que toda Plataforma Tecnológica de la Institución cumpla con las Políticas y Estándares de Seguridad de la Dirección Nacional de Aeronáutica Civil.

10.5.5. Contraseñas

10.5.5.1.- Las Contraseñas creadas por los Usuarios, siempre que el entorno operativo lo permita, deben ser de un mínimo 8 (ocho) caracteres de longitud y estar compuestas por una combinación de números y letras.

10.5.5.2.- Las Contraseñas deben ser difíciles de deducir. En la creación no se deben utilizar series de números o letras, palabras del diccionario ni referencias al entorno personal como nombres propios, nombres de familiares, nombres de mascotas, número de documento, número de legajo, dirección etc. Tampoco se deben crear Contraseñas fijas donde solo se modifica en forma cíclica una parte de ella.

10.5.5.3.- Toda vez que un Usuario sospeche o sepa que su Contraseña de acceso pudo haber sido utilizada por otra persona debe inmediatamente:

a. Informar al Encargado de Seguridad de la Información.
b. Cambiar su contraseña o en caso de que el sistema no lo permita, solicitar el cambio de su Contraseña de acceso.

10.5.5.4.- Las Contraseñas no deben estar incorporadas en los programas de seguridad o de aplicaciones, ni deben ser almacenadas en forma legible en los archivos, equipos de control de acceso, o en cualquier otra locación de donde puedan ser recuperadas. Tampoco deben ser almacenadas en programas fuente, teclas de función en terminales, archivos en discos rígidos locales, papeles autoadhesivos o algún otro lugar donde personas no autorizadas puedan encontrarlas.

10.5.5.5.- Las Contraseñas utilizadas por procesos automáticos no deben estar incluidas en la codificación de las aplicaciones. En el caso de no ser posible la aplicación de esta norma se debe:

a. Obtener la autorización del Encargado de Seguridad de la Información.
b. Restringir el acceso al código fuente de las aplicaciones.
c. Notificar con anticipación al Encargado de Seguridad de la Información cualquier cambio a las aplicaciones.

10.5.5.6.- Las Contraseña fijas de procesos o equipos de computación que no requieran de cambios periódicos, deben ser modificadas anualmente.

10.5.5.7.- Las aplicaciones deben utilizar la Identificación de Usuario y Contraseña de acceso de la Plataforma en que se ejecutan. Un nuevo mecanismo adicional de autenticación debe ser autorizado por el Encargado de Seguridad de la Información.

10.5.6. Accesos Privilegiados

10.5.6.1.- Los accesos privilegiados sólo deben ser otorgados de manera restringida a la necesidad de trabajo y contar con la aprobación escrita del Encargado de Seguridad de la Información y la Coordinación General de TIC respectivamente.

10.5.6.2.- Los derechos de acceso de los Usuarios privilegiados deben ser revisados en forma periódica por el Encargado de Seguridad de la Información, para asegurar que dichos derechos siguen siendo necesarios.

10.5.7. Bloqueo de Accesos

10.5.7.1.- Las Identificaciones de Usuarios deben ser bloqueadas o revocadas automáticamente cuando registren:

C.P. Prelly A. Garay
Coordinador MECIP
DINAC

- 5 (cinco) intentos de acceso con Contraseña errónea.
- 30 (treinta) días Como máximo desde la emisión del código sin haber sido recibido
- 90 (noventa) días como máximo consecutivos sin actividad.
- Por eventos específicos solicitados y/o autorizados por la Alta Dirección.

10.5.7.2.- Las Identificaciones de Usuarios bloqueadas o revocadas deberán ser autorizadas sólo por el Encargado de Seguridad de la Información y rehabilitadas por la Coordinación General de Tecnología de Información y Comunicación.

10.5.8. Inhabilitación por Tiempo de Inactividad

10.5.8.1.- Las sesiones de Sistemas inactivas por un periodo máximo de 30 (treinta) minutos deben ser automáticamente finalizadas, en la medida en que la Plataforma brinde dicha funcionalidad. Salvo excepciones definidas por la Coordinación General de Tecnología de Información y Comunicación o el Encargado de Seguridad de la Información.

10.5.8.2.- El Usuario que esté haciendo uso de Sistemas de la Dirección Nacional de Aeronáutica Civil, bajo ninguna circunstancia debe dejar su puesto de trabajo sin desconectar su sesión.

10.5.9. Registros de Auditoría

10.5.9.1.- Los Sistemas de Aplicaciones en producción deben registrar cada incorporación, modificación o eliminación de datos en la Base de Datos de la Institución, como así también debe consignar el código de Usuario, fecha, hora e información necesaria que identifique la terminal que lo ejecuta.

10.5.9.2.- Se deben registrar para todos los Usuarios, los eventos relevantes de seguridad como:

a. Intentos de ingreso con Contraseña errónea.
b. Intentos de acceso no autorizados.
c. Modificaciones al Software de Base.
d. Modificaciones al Sistema de Aplicación.
e. Ejecución de comandos críticos.

10.5.9.3.- No se debe permitir la desactivación, modificación o eliminación de los Registros de Auditoria. Dichos Registros deben estar protegidos de manera tal que puedan ser accedidos con permiso de lectura por el Encargado de Seguridad de la Información.

10.5.9.4.- Los Registros de Auditoria deben ser controlados periódicamente y estar resguardados en forma segura como mínimo por 2 (dos) años.

10.5.10. Contraseñas Iniciales

10.5.10.1.- Las Contraseñas iniciales asignadas por la CGTIC, deben:

a. Ser temporarias o pre expiradas.
b. Tener 8 (ocho) caracteres de longitud mínima.
c. Ser válidas sólo para la primera sesión de cada Usuario.

10.5.10.2.- Los Sistemas deben forzar a los Usuarios a cambiar la Contraseña pre expirada antes de ejecutar cualquier otra acción, por una Contraseña que ellos definan conforme a las presentes normas.

10.5.10.3.- Las Contraseñas genéricas utilizadas en los procesos de instalación de Sistemas, Aplicaciones o Base de Datos, deben ser cambiadas durante la instalación o inmediatamente al finalizar la misma, y siempre antes de su ejecución en el ambiente de producción.

C.P. Fredy A. Gaia
Coordinador MEC
DINAC

10.5.10.4.- Las Contraseñas y los códigos de Usuario deben ser comunicados a los Usuarios en forma segura, de manera que sea posible verificar la ID-Usuario de los mismos. La entrega debe realizarse por medios digitales y/o electrónicos que pueda identificar al usuario.

10.5.11. Eliminación de Accesos

10.5.11.1.- El Encargado de Seguridad de la Información debe eliminar los accesos a los Sistemas, cuando un Funcionario fuera cesado en las funciones que requieran acceso a los Sistemas de Información y que sea informado por la Coordinación General de Talento Humano de forma inmediata al correo de la Coordinación General de TIC.

10.5.11.2.- El Propietario de Procesos es responsable de verificar que los privilegios de acceso están alineados con las necesidades del negocio.

11.- Política: Acceso Remoto

11.1. Objetivo

Establecer los requerimientos mínimos de seguridad y control para acceder en forma remota a las Redes de la Institución.

11.2. Fundamentos

Definir los requerimientos mínimos de protección para el acceso remoto a la información, sistemas y servicios informáticos, redes y datos.

11.3. Alcance y Sectores de Aplicación

Esta Política se aplica para todo el Personal de la Institución y Terceros relacionados con el mismo, que requieran acceder en forma remota a los Sistemas de la Institución.

11.4. Definiciones

Acceso Remoto: Conexión con los Recursos Informáticos de la Red de la Institución desde una ubicación remota y a través de una Red Pública.

11.5. Contenido

11.5.1. Acceso Remoto a Recursos Informáticos de la Dirección Nacional de Aeronáutica Civil.

11.5.1.1.- Los mecanismos que permitan el acceso remoto a los Recursos Informáticos de la Institución, deben ser aprobados por la Coordinación General de TIC antes de ser utilizados.

11.5.1.2.- Para el acceso remoto a los Recursos Informáticos de la Institución deben ser tenidas en cuenta las normas referidas en los procedimientos de Conexión y Autenticación.

11.5.1.3.- Para el acceso remoto a través de Internet a los Recursos Informáticos de la Institución, se deben utilizar los métodos acordados que gestionen la encriptación de Datos.

11.5.1.4.- El superior inmediato debe autorizar este modo de acceso solamente a los Usuarios que lo requieran para desempeñar sus funciones.

11.5.1.5.- Todo acceso a los puertos de comunicaciones debe ser estrictamente controlado. Cualquier Usuario que requiera establecer una conexión interna o externa debe obtener aprobación del Encargado de Seguridad de la Información.

11.5.1.6.- El Encargado de Seguridad de la Información debe acceder a los registros exactos y

C.P. Fredy A. Garay
Coordinador MECIP
DINAC

actualizados de la ubicación física de todos los canales de comunicación de datos.

11.5.1.7.- El uso de cualquier otro dispositivo de conexión dentro de la red de la Institución se encuentra prohibido, salvo aprobación del Encargado de Seguridad de la Información.

11.5.1.8.- Los proveedores que requieran acceso remoto a los Sistemas informáticos de la Institución, deben tener el acceso limitado para el desarrollo de sus actividades.

11.5.1.9.- Todo acceso remoto a las computadoras o equipos debe ser realizado mediante recursos informáticos de propiedad de la Institución u otros debidamente autorizados por el Encargado de Seguridad de la Información.

12.- Política: Información Impresa y Formatos Equivalentes

12.1. Objetivo

Establecer los lineamientos para el manejo de Información Privada que se encuentre en forma impresa o en formatos equivalentes.

12.2. Fundamentos

Proteger la información clasificada como Privada soportada en medios impresos y formatos equivalentes desde que es emitida, durante el periodo de utilización y hasta su eliminación.

12.3. Alcance y Sectores de Aplicación

Esta Política es aplicable para todos los Personales de la Institución y Terceras Partes que creen, accedan, distribuyan o reciban Información Privada en forma impresa o formatos equivalentes.

12.4. Definiciones

- Información Impresa y Formatos Equivalentes: Toda información que se encuentre registrada en un papel. Esta puede ser: listados impresos, fotocopias, memorandos, etc.

- Información Privada: Se aplica a la información que está destinada para uso interno de la Institución.
  Su revelación no autorizada podría afectar a la Institución de manera grave y/o adversa.

- Información Pública: Información que puede ser accedida por el público pero que puede ser modificada y/o eliminada sólo por personal autorizado. Ej. Páginas del Sitio Web de la Dirección Nacional de Aeronáutica Civil.

12.5. Contenido

12.5.1.- Respaldo en Formato Impreso o Equivalente

12.5.1.1.- La información de la Institución debe ser emitida en forma impresa o en formato equivalente en la medida que lo requieran las operaciones de la Institución.

12.5.1.2.- Las copias de la información de la Institución deben ser mantenidas en números reducidos para facilitar su control y distribución.

12.5.1.3.- En caso de no ser utilizada, la información en formato impreso o su equivalencia debe ser resguardada en compartimientos al que solo tenga acceso el personal autorizado.

12.5.1.4.- Se deben tomar medidas adecuadas de seguridad sobre la Información Privada que es transferida en forma impresa o en formatos equivalentes.

12.5.2.- Destrucción de Material Impreso y Formatos Equivalentes

C.P. Fredy A. Garay
Coordinador MECIP
DINAC

12.5.2.1. Toda información que esté en forma impresa o en formato equivalente, debe ser destruida cuando entre en desuso.

12.5.2.2. Para la destrucción de Documentación se deben utilizar máquinas destructoras de documentos o servicios de Terceras Partes que garanticen procedimientos apropiados para la destrucción de la Documentación.

13. Política: Conexiones a Redes Externas

13.1. Objetivo
Establecer los requerimientos para permitir la conectividad entre Redes Internas y Externas de la Institución.

13.2. Fundamentos
- Asegurar la integridad, confidencialidad y disponibilidad de la información de la Institución, sus proveedores y clientes.
- Normar los requerimientos generales y de conexión a Internet y Extranet.

13.3. Alcance y Sectores de Aplicación
Personal de la Institución y Terceras Partes asociadas con el mismo.

13.5. Contenido

13.5.1. Requerimientos Generales

13.5.1.1.- Todos los cambios que se realicen sobre la configuración de Routers y Firewalls, deben respetar los lineamientos establecidos en las políticas vigentes de la Institución.

13.5.1.2.- Los servidores que utilicen protocolos que permiten el reenvío o re-enrutamiento de paquetes deben tener deshabilitada esta función.

13.5.1.3.- Las direcciones internas, configuraciones y datos relativos al diseño de la Red de la Institución no deben ser visibles ante conexiones externas, y deben estar protegidos de modo tal que los Usuarios y Sistemas no puedan acceder a esta información.

13.5.1.4.- Los Sistemas Operativos de Firewalls y Routers deben contar con la funcionalidad de filtrar direcciones IP, tanto de destino como de origen.

13.5.2. Conexión a Internet y Extranet

13.5.2.1.- Todas las conexiones a Internet que se originen dentro de la Red de la Institución deben pasar por:

a. Servidores aprobados por la Coordinación General de TIC.
b. Firewalls aprobados por la Coordinación General de TIC.

13.5.2.2.- El Departamento de Redes e Internet debe revisar la configuración de los Firewalls periódicamente o al producirse cambios sobre los sistemas relacionados con Internet.

13.5.2.3.- Todos los cambios críticos que se practiquen sobre la configuración de Firewalls y Routers, deben ser comunicados a la Coordinación Tecnologías de Información y Comunicación y el Encargado de Seguridad de la Información.

13.5.2.4.- Los Firewalls deben ser instalados y localizados en áreas de acceso restringido y controlado.

13.5.2.5.- Todas las conexiones de la Red de la Dirección Nacional de Aeronáutica Civil con Redes de Terceros deben pasar por un Firewall cuya configuración debe ser aprobada por la Coordinación General de TIC.

C.P. Fredy A. Garay
Coordinador MECIP
DINAC

13.5.2.6.- Toda Computadora de la Institución que pueda ser accedida desde Redes Externas debe ser protegida con un software de control de acceso aprobado por la Coordinación General de TIC.

13.5.2.7.- Toda acción requerida por un Usuario desde una ubicación interna o externa no debe ser atendida, a menos que el Usuario haya sido identificado satisfactoriamente con anterioridad.

13.5.2.8.- Todas las conexiones de Instituciones Externas a Plataformas y Aplicaciones de la Institución, debe ser física o lógicamente acotadas a las necesidades requeridas.

13.5.2.9.- Bajo ningún aspecto el personal de Terceros debe tener acceso ilimitado a las Computadoras o Redes de la Institución.

Parte IV - Políticas de Seguridad Física

14.- Política: Seguridad Física

14.1. Objetivo
Contar con una Normativa que proporcione un ambiente físico apropiado para las Instalaciones y Recursos de TI contra riesgos naturales o provocados por terceros.

14.2. Fundamentos
- Implementar medidas para asegurar la integridad física de los Recursos de TI de la Institución.
- Minimizar riesgos que puedan poner en peligro la vida de las personas y las instalaciones.

14.3. Alcance y Sectores de Aplicación
Este procedimiento es de aplicación en todo el ámbito de la Institución.

14.4. Definiciones
- **Instalaciones de TI:** Instalaciones utilizadas para el funcionamiento de la Coordinación General de Tecnologías de Información y Comunicación.
- **Área Crítica de TI:** Sala de Servidores de la Coordinación General de Tecnología de Información y Comunicación.
- **Área de Backup de TI**: Sala de Almacenamiento de Dispositivos y medios de Respaldo de Datos y Sistemas de Aplicación de la Dirección Nacional de Aeronáutica Civil.
- **Soportes de TI:** Equipos de Computación y Dispositivos de TI.
- **Incidencias:** Fenómenos que pueden producirse en los Centros de Procesamiento de Información tales como:

  a. Interrupción del Suministro Eléctrico.
  b. Interrupción de las Comunicaciones.
  c. Interrupción de la Refrigeración.
  d. Detección y Prevención de Fuego.
  e. Detección y Prevención de Inundaciones.

- **UPS:** Equipo que utiliza baterías para mantener el suministro de electricidad.

14.5. Contenido

14.5.1. Control de Acceso Físico

14.5.1.1.- Las Instalaciones de TI se deben encontrar en recintos cerrados donde exista acceso físico restringido por medio de un tipo de cerradura (electrónica o mecánica), que impida el paso de personas no autorizadas y minimizar la contaminación ambiental como polvo, etc.

14.5.1.2.- Las llaves de acceso (tarjetas, llaves, mecanismos electrónicos, etc.) correspondientes a las Instalaciones de TI, sólo las pueden tener en forma permanente los miembros de la

C.P. Pedro A. Gara
Coordinador MECIP
DINAC

Coordinación General de Tecnologías de Información y Comunicación y el Encargado de Seguridad de la Información.

14.5.1.3.- Las llaves de acceso (tarjetas, llaves, mecanismos electrónicos, etc.) correspondientes a las Áreas Crítica de TI, sólo las pueden tener en forma permanente los siguientes miembros de la Coordinación General de Tecnología de Información y el Encargado de Seguridad de la Información:

a. Coordinador General.
b. Gerente.
c. Jefes de Departamentos.
d. Técnicos de las áreas afectadas.

14.5.1.4.- La Coordinación General de Tecnología de Información y Comunicación establecerá la nómina de personas que podrán tener acceso a las Áreas Críticas de TI.

14.5.1.5.- Debe registrarse el ingreso y la salida de todas las personas que acceden a las Áreas Críticas de TI y no sean miembros de la Coordinación General de Tecnologías de Información y Comunicación, ya sea en registros manuales o a través de los mecanismos electrónicos, y deberá ser retenido por lo menos un año.

El registro debe contar como mínimo con los siguientes datos:

a. Nombre de la Empresa a la que pertenece la persona.
b. Nombre de la Persona.
c. Fecha y Hora de Llegada / Salida.
d. Motivo del Ingreso.
e. Funcionario autorizado que acompañó el ingreso.

14.5.1.6.- El acceso a las Instalaciones de TI de funcionarios de otras Áreas y de personas que no pertenezcan a la Institución, deben ser autorizados por la Coordinación General de Tecnologías de Información y Comunicación.

14.5.1.7.- Toda persona que no posea acceso autorizado y pertenezca o no a la Institución debe estar siempre acompañado por un miembro de la Coordinación General de Tecnología de Información y Comunicación, el que controlará las actividades que dichos visitantes desarrollen.

14.5.1.8.- El acceso a las Instalaciones de TI debe realizarse sólo a través de las puertas controladas, por lo tanto, el resto de aberturas (por ejemplo, salidas de emergencia o ventanas), deben poseer los recaudos físicos para que permanezcan cerradas.

14.5.1.9.- Los funcionarios dependientes de la Coordinación General de Tecnología de Información y Comunicación serán responsables de controlar el acceso de las personas a las Instalaciones de TI.

14.5.1.10.- Todos los visitantes o terceras personas, que ingresen a un área de procesamiento deberán poseer una identificación a la vista que claramente los identifique como tales. Asimismo, queda restringida la grabación digital a los centros de procesamiento de información de la DINAC.

14.5.1.11.- En caso de pérdidas de llaves de acceso debe notificarse a la Coordinación General de Tecnologías de Información y Comunicación para que las mismas no puedan ser utilizadas por terceras personas no autorizadas para lograr acceso, tomando medidas de seguridad tales como cambio de cerraduras., inhabilitación de códigos, aviso a la vigilancia y otros.

14.5.1.12.- Se deben realizar programas de concientización y entrenamiento para los usuarios en cuanto a temas de seguridad y acceso físico a las áreas de TI.

14.5.1.13.- El Encargado de Seguridad de la Información y/o la Coordinación General de Tecnología de Información y Comunicación debe requerir las llaves de acceso cuando un miembro de la Coordinación General de TIC se retira de ésta o cambia su función. En el caso de llaves magnéticas es conveniente desactivar el código de acceso por un período mínimo de un año.

C.P. Fredy A. Garay
Coordinador MECIP
DINAC

14.5.1.14.- Los miembros de la Coordinación General de Tecnología de Información y Comunicación deben poseer una lista del personal con acceso autorizado a las Instalaciones de TI, y la misma debe ser utilizada con toda persona que intente ingresar fuera de horario o los días no laborales.

14.5.1.15.- El Encargado de Seguridad de la Información debe revisar periódicamente y mantener actualizadas las listas de personal con acceso autorizado a las Instalaciones de TI, y el registro de entradas y salidas a las mismas.

14.5.1.16.- Deben tomarse medidas de acceso restringido a todos los elementos críticos de comunicación, los que estén fuera de las áreas restringidas de procesamiento deben estar instalados en rack con cerraduras, y las llaves deben estar en poder del Encargado de Seguridad de la Información y/o de la Coordinación General de Tecnología de Información y Comunicación.

14.5.1.17.- Los materiales peligrosos o combustibles deben ser almacenados en lugares seguros a una distancia prudencial del área crítica de TI. Los suministros a granel, como los útiles de escritorio, formularios continuos no deben ser almacenados en el área crítica de TI hasta que sean requeridos.

14.5.1.18.- Todas las reglas precedentemente desarrolladas deben ser exigidas a aquellas Instalaciones de TI que ejecuten sistemas y/o procesen información de la Institución, sean propiedad de ésta o no.

14.5.2. Dispositivos de Seguridad

14.5.2.1.- Las Instalaciones de TI deben disponer de dispositivos para solucionar rápidamente incidencias mínimas. Las incidencias mínimas a contemplar son:

a. Interrupción del suministro eléctrico.
b. Interrupción de las comunicaciones.
c. Interrupción de la refrigeración.
d. Detección y prevención de fuego.

14.5.2.2.- Está prohibido el ingreso de alimentos y bebidas en el área crítica de TI.

14.5.2.3.- Está prohibido fumar en las Instalaciones de TI.

14.5.3.- Suministro Eléctrico

14.5.3.1.- Las Instalaciones de TI deben contar con UPS´s para poder mantener la operatividad de los Soportes de TI.

14.5.3.2.- Las Instalaciones de TI deben contar con un Generador de Electricidad para poder mantener la operatividad de los Soportes de TI ante cortes prolongados de Electricidad.

14.5.3.3.- Debe garantizarse que las UPS´s reaccionen inmediatamente ante la ausencia de energía eléctrica sin producir micro interrupciones que puedan perjudicar los Soportes de TI o la información procesada.

14.5.3.4.- Las UPS´s deben ser revisadas periódicamente por la Coordinación General de Tecnología de Información y Comunicación, observando elementos tales como carga, mantenimiento efectuado, última prueba realizada.

14.5.3.5.- Los Generadores Eléctricos deben ser revisados y probados periódicamente por la Coordinación General de Información y Comunicación, de acuerdo a las especificaciones del proveedor.

14.5.3.6.- Se deben implementar protecciones contra descargas eléctricas atmosférica en las

C.P. Fredy A. Gara
Coordinador MECIP
DINAC

instalaciones de TI.

14.5.3.7.- Se deben implementar sistemas de aterramiento contra descargas eléctricas en todas las líneas de comunicaciones externas utilizadas en las instalaciones de TI.

14.5.3.8.- Una vez establecidos los controles necesarios sobre el suministro eléctrico en las Instalaciones de TI, cualquier cambio sobre los mismos debe ser informado al Encargado de Seguridad de la Información para una adecuada evaluación.

14.5.4. Comunicaciones

14.5.4.1.- Ante incidencias con los medios de comunicación principales, se deben contar con métodos alternativos de comunicación o procesamiento que permitan mantener operativos los Sistemas de Aplicación de acuerdo a su criticidad.

14.5.4.2.- Los Elementos de Comunicación (Equipos de Comunicación, Cableado, etc.), deben estar en lugares adecuados con baja probabilidad de inundaciones, incendios y de acceso restringido. Además, deben estar debidamente aislados de fuentes de energía y elementos de combustión.

14.5.4.3.- Se deben ubicar todos los cables y líneas de comunicación tanto de voz como de datos en áreas seguras.

14.5.5. Refrigeración

14.5.5.1.- Las Instalaciones de TI deben contar con equipos de aire acondicionado de precisión adecuados.

14.5.5.1.- El Área Crítica de TI debe contar con Equipos de aire acondicionado de precisión alternativos.

14.5.6. Detección / Extinción de Incendios

14.5.6.1.- Las Instalaciones de TI deben tener instalados detectores de calor y humo en forma adecuada y en número suficiente como para detectar el más mínimo principio de incendio. Su instalación debe cumplir con los requisitos de los fabricantes o normas de calidad de la industria.

14.5.6.2.- Los detectores de calor y humo deben ser probados con una periodicidad que cumpla con el mantenimiento preventivo previsto por los fabricantes.

14.5.6.3.- El material del Área Crítica de TI no debe ser combustible, y en la construcción deben haberse contemplado puertas contra incendios. Los paneles eléctricos deben estar cubiertos por cajas ignífugas.

14.5.6.4.- Las Instalaciones de TI deben poseer extintores de incendios en número suficiente y con características adecuadas (aptos para fuegos eléctricos). Los extintores deben estar instalados en lugares de fácil acceso y claramente indicados, visibles incluso ante ausencia de luz.

14.5.6.5.- El Área Crítica de TI debe contar con extintores de incendio con capacidad de cubrir toda el Área.

14.5.7. Detección / Prevención de Inundaciones

14.5.7.1.- Las Instalaciones de TI deben estar ubicadas en pisos de altura superior al nivel de la calle a fin de evitar inundaciones.

14.5.7.2.- En las Instalaciones de TI no deben pasar cañerías de líquidos por sus techos, ni ser colindantes a sectores húmedos tales como torres de enfriamiento, depósito de líquidos, tanques

C.P. Fredy A. Garay
Coordinador MECIP
DINAC

de agua etc.

14.5.7.3.- El Área Crítica de TI debe tener medidores de humedad y temperatura. La Coordinación General de Tecnología de Información y Comunicación debe efectuar diariamente el monitoreo y registro de la humedad y temperatura del area crítica de TI.

14.5.7.4.- El Encargado de Seguridad de la Información debe verificar regularmente las Instalaciones de TI como parte de su programa de mantenimiento y la Coordinación General de Tecnología de Información y Comunicación debe efectuar su monitoreo.

14.5.8.- Seguridad Física de las salas técnicas

14.5.8.1.- Por el Área de donde se encuentran los servidores de TI no deben pasar cañerías con fluidos, deben existir controles de humedad y temperatura, así como detectores de humo y fuego.

14.5.8.2.- El Área de donde se encuentran los servidores de TI debe ser de uso exclusivo, es decir con ese único fin, para evitar el paso de personas ajenas a su administración.

14.5.8.3.- El Encargado de Seguridad de la Información debe constatar con una periodicidad adecuada que los controles se encuentren correctamente implantados.

14.5.8.4.- Todos los cambios estructurales dentro de los lugares destinados a Áreas Críticas de TI deben ser informados a la Coordinación General de Tecnología de Información y Comunicación, a fin de que el mismo evalúe antes de la realización de los mismos las posibles consecuencias sobre la seguridad física establecida sobre los medios de almacenamiento.

14.5.9. Seguridad de Dispositivos de Información fuera del Ámbito de Procesamiento

14.5.9.1.- La seguridad provista debe ser equivalente a la suministrada dentro del ámbito de la Institución, para un propósito similar, teniendo en cuenta los riesgos de trabajar fuera de la misma.

14.5.9.2.- El equipamiento y dispositivos retirados del ámbito de la Institución no deben permanecer desatendidos en lugares públicos. Las computadoras personales deben ser transportadas como equipaje de mano durante el viaje.

14.5.9.3.- Se deben respetar permanentemente las instrucciones del fabricante en relación a:

a) Temperatura fuera de rango, polvo y humedad.
b) Voltaje e intensidad de alimentación eléctrica.
c) Exposición a golpes.

Parte V – Divulgación y Reforma

1. Esta política de seguridad deberá seguir un proceso de actualización periódica sujeto a los cambios organizacionales relevantes: crecimiento de la planta de personal, cambio en la infraestructura computacional, desarrollo de nuevos servicios, entre otros.
2. El documento que contiene la política de seguridad debe ser difundido a todo el personal involucrado en la definición de estas políticas.
3. Las revisiones se realizarán cada 2 años.
4. Complementariamente a las presentes políticas, es necesario definir procedimientos que apoyen las actividades a ser implementadas.

C.P. Fredy A. Garay
Coordinador MECIP
DINAC