REGISTRO OFICIAL
ÓRGANO DE LA REPÚBLICA DEL ECUADOR

CORTE CONSTITUCIONAL DEL ECUADOR

EDICIÓN ESPECIAL

Año I - Nº 755

Quito, jueves 9 de julio de 2020

Servicio gratuito

ING. HUGO DEL POZO BARREZUETA
DIRECTOR

Quito:
Calle Mañosca 201
y Av. 10 de Agosto
Telf.: 3941-800
Exts.: 3131 - 3134

101 páginas

www.registroficial.gob.ec

El Pleno de la Corte Constitucional mediante Resolución Administrativa No. 010-AD-CC-2019, resolvió la gratuidad de la publicación virtual del Registro Oficial y sus productos, así como la eliminación de su publicación en sustrato papel, como un derecho de acceso gratuito de la información a la ciudadanía ecuatoriana.

Al servicio del país
desde el 1º de julio de 1895

MINISTERIO DE DESARROLLO URBANO Y VIVIENDA
MIDUVI

Págs.

Acuerdo Ministerial No. 024-20

Señor Guido Esteban Macchiavello Almeida
MINISTRO DE DESARROLLO URBANO Y VIVIENDA

CONSIDERANDO:

Que, el numeral 1 del artículo 154 de la Constitución de la República del Ecuador establece entre las atribuciones de las ministras y ministros de Estado: Ejercer la rectoría de las políticas públicas del área a su cargo y expedir los acuerdos y resoluciones administrativas que requiera su gestión.

Que, en el artículo 226 de la Constitución de la República del Ecuador establece: *Las instituciones del Estado, sus organismos, dependencias, las servidoras o servidores públicos y las personas que actúen en virtud de una potestad estatal ejercerán solamente las competencias y facultades que les sean atribuidas en la Constitución y la ley. Tendrán el deber de coordinar acciones para el cumplimiento de sus fines y hacer efectivo el goce y ejercicio de los derechos reconocidos en la Constitución.*

Que, en el artículo 227 de la Constitución de la República del Ecuador establece: *La administración pública constituye un servicio a la colectividad que se rige por los principios de eficacia, eficiencia, calidad, jerarquía, desconcentración, descentralización, coordinación, participación, planificación, transparencia y evaluación.*

Que, en el artículo 47 del Código Orgánico Administrativo establece que la máxima autoridad administrativa de la correspondiente entidad pública ejerce su representación para intervenir en todos los actos, contratos y relaciones jurídicas sujetas a su competencia. Esta autoridad no requiere delegación o autorización alguna de un órgano o entidad superior, salvo en los casos expresamente previstos en la ley.

Que, en el artículo 67 del Código Orgánico Administrativo establece: *"El ejercicio de las competencias asignadas a los órganos o entidades administrativos incluye, no solo lo expresamente definido en la ley, sino todo aquello que sea necesario para el cumplimiento de sus funciones. Si en aplicación de esta regla existe conflicto de competencias, se resolverá de conformidad con lo dispuesto en este Código".*

Que, en el capítulo segundo, del Código Orgánico Administrativo establece las directrices para el funcionamiento de los órganos colegiados de Dirección;

Que, el Ministerio de Desarrollo Urbano y Vivienda (MIDUVI), fue creado mediante Decreto Ejecutivo No. 3 de 10 de agosto de 1992, publicado en el Registro Oficial No. 1 de 11 de agosto de 1992;

Que, mediante Decreto Ejecutivo No. 818, de 3 de julio de 2019, el señor Presidente Constitucional de la República del Ecuador, designó al Sr. Guido Esteban Macchiavello Almeida, como Ministro de Desarrollo Urbano y Vivienda**;**

Que, el Artículo 1 del Acuerdo No. 025-2019 del 20 de septiembre de 2019, publicado en el Registro Oficial No. 228 de 10 de enero de 2020, emitido por el Ministerio de Telecomunicaciones y de la Sociedad de la Información-MINTEL, expide el "ESQUEMA GUBERNAMENTAL DE SEGURIDAD DE LA INFORMACIÓN (EGSI);

Que, el Artículo 5 del Acuerdo No. 025-2019 del MINTEL referente al EGSI dispone que la máxima autoridad designará un Comité de Seguridad de la Información (CSI), que estará integrado por los responsables de las siguientes áreas o quienes hagan sus veces: Talento Humano, Administrativo, Planificación y Gestión Estratégica, Comunicación Social, Tecnologías de la Información, Unidades Agregadoras de Valor y el Área Jurídica como asesor.

Que, el Esquema Gubernamental de Seguridad de la Información (EGSI), anexo al presente cuerpo legal, establece un conjunto de directrices prioritarias de cumplimiento obligatorio para la Gestión de la Seguridad de la Información en las Entidades Públicas;

Que, mediante Acuerdo Ministerial Nro. 007-20, de 5 de febrero de 2020, el Ministro de Desarrollo y Vivienda, crea el Comité de Seguridad de la Información del Ministerio de Desarrollo Urbano y Vivienda (MIDUVI).

Que, el artículo 17 del Estatuto del Régimen Jurídico y Administrativo de la Función Ejecutiva, ERJAFE, emitido mediante Decreto Ejecutivo 2428, del 17 de septiembre de 2014, determina: "DE LOS MINISTROS. - Los Ministros de Estado son competentes para el despacho de todos los asuntos inherentes a sus ministerios sin necesidad de autorización alguna del Presidente de la República, salvo los casos expresamente señalados en leyes especiales";

ACUERDA:

Artículo 1.- Aprobar las Políticas de Seguridad de la Información del Ministerio de Desarrollo Urbano y Vivienda, que se encuentran anexas y forma parte integral de este Acuerdo.

Artículo 2.- De la ejecución, monitoreo y seguimiento de las Políticas de Seguridad de la Información del Ministerio de Desarrollo Urbano y Vivienda encárguese al Comité de Seguridad de la Información y al Oficial de Seguridad de la Información.

DISPOSICIÓN GENERAL

PRIMERA. - Las disposiciones constantes en el presente Acuerdo Ministerial, tienen carácter de obligatorio para los servidores del Ministerio de Desarrollo Urbano y Vivienda.

El presente Acuerdo Ministerial, entrará en vigencia a partir de su suscripción sin perjuicio de su publicación en el Registro Oficial.

Dado en el Distrito Metropolitano de Quito, 2020 JUN 17

firmado electrónicamente por:
GUIDO ESTEBAN MACCHIAVELLO ALMEIDA

Señor Guido Esteban Macchiavello Almeida
MINISTRO DE DESARROLLO URBANO Y VIVIENDA

POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN DEL MINISTERIO DE DESARROLLO URBANO Y VIVIENDA

Versión 1.0

Abril de 2020

Contenido

1. INTRODUCCIÓN

La información es el activo más importante de una institución y es un recurso que tiene un valor transcendental en la gestión del Ministerio de Desarrollo Urbano y Vivienda – MIDUVI, y por consiguiente debe ser debidamente protegida.

Las Políticas de Seguridad de la Información ayudan a proteger éste recurso de una amplia gama de amenazas, a fin de garantizar la continuidad de los sistemas de información y servicios institucionales, generar confianza en la ciudadanía, minimizar los riesgos derivados de vulnerabilidades informáticas y asegurar el eficiente cumplimiento de los objetivos de la institución.

Definidas desde el análisis de los riesgos a los que se encuentra propenso el MIDUVI, las Políticas de Seguridad surgen como una herramienta organizacional para concientizar a los funcionarios y servidores públicos de la institución sobre la importancia y sensibilidad de la información que administran y generan en sus puestos de trabajo y permiten a la institución brindar los servicios que requiere la ciudadanía y el entorno institucional. Ante esta situación, el proponer estas políticas requiere un alto compromiso de la organización, para esto, se debe asegurar un trabajo manifiesto de las máximas autoridades de la institución y de los directores de las unidades organizativas para la difusión, consolidación y cumplimiento.

2. ALCANCE

Se aplican en todo el ámbito de la institución; tanto al Talento Humano, a los recursos y a la totalidad de los procesos y servicios.

Las Políticas de Seguridad son elaboradas de acuerdo al análisis de riesgos y de vulnerabilidades, y se dictan en cumplimiento de las disposiciones legales vigentes, con el objeto de gestionar adecuadamente la Seguridad de la Información, los sistemas informáticos y el ambiente tecnológico del MIDUVI.

Debe ser conocida y cumplida por todo el personal del MIDUVI, a nivel nacional, y sea cual fuere su nivel jerárquico dentro de la institución.

3. TÉRMINOS Y DEFINICIONES

A los efectos de este documento se aplican las siguientes definiciones:

3.1. Seguridad de la Información

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

- ***Confidencialidad:*** se garantiza que la información sea accesible sólo a aquellas personas autorizadas a tener acceso a la misma.
- ***Integridad:*** se salvaguarda la exactitud y totalidad de la información y los métodos de procesamiento.
- ***Disponibilidad:*** se garantiza que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con la misma, toda vez que lo requieran.

Adicionalmente, deberán considerarse los conceptos de:

- ***Autenticidad**:* busca asegurar la validez de la información en tiempo, forma y distribución. Además, se garantiza el origen de la información, validando el emisor para evitar suplantación de identidades.
- ***Auditabilidad**:* define que todos los eventos de un sistema deben poder ser registrados para su control posterior.
- ***Protección a la duplicación**:* consiste en asegurar que una transacción sólo se realiza una vez, a menos que se especifique lo contrario. Impedir que se grabe una transacción para luego reproducirla, con el objeto de simular múltiples peticiones del mismo remitente original.
- ***No repudio**:* se refiere a evitar que una entidad que haya enviado o recibido información alegue ante terceros que no la envió o recibió.
- ***Legalidad**:* referido al cumplimiento de las leyes, normas, reglamentaciones o disposiciones a las que está sujeta la Institución.
- ***Confiabilidad de la Información**:* es decir, que la información generada sea adecuada para sustentar la toma de decisiones y la ejecución de las misiones y funciones.

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

- ***Información**:* Se refiere a toda comunicación o representación de conocimiento como datos, en cualquier forma, con inclusión de formas textuales, numéricas, gráficas, cartográficas, narrativas o audiovisuales, y en cualquier medio, ya sea magnético, en papel, en pantallas de computadoras, audiovisual u otro.
- ***Sistema de Información**:* Se refiere a un conjunto independiente de recursos de información organizados para la recopilación, procesamiento, mantenimiento, transmisión y difusión de información según determinados procedimientos, tanto automatizados como manuales.
- ***Tecnología de la Información**:* Se refiere al hardware y software operados por el MIDUVI o por un tercero que procese información en su nombre, para llevar a cabo una función propia de la Institución, sin tener en cuenta la tecnología utilizada, computación de datos, telecomunicaciones u otro tipo.

3.2 Evaluación de Riesgos

Evaluación de las amenazas y vulnerabilidades relativas a la información y a las instalaciones de procesamiento de la misma, la probabilidad de que ocurran y su potencial impacto en la operación de la Institución.

3.3 Administración de Riesgos

Proceso de identificación, control y minimización o eliminación, a un costo aceptable, de los riesgos de seguridad que podrían afectar a la información. Dicho proceso es cíclico y debe llevarse a cabo en forma periódica.

3.4 Comité de Seguridad de la Información

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

3.5 Oficial de Seguridad de la Información

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

3.6 Incidente de Seguridad

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

4 POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

4.1 Objetivos

4.1.1 Objetivo General

Incrementar la seguridad de los recursos de información del MIDUVI, y la tecnología utilizada para su procesamiento, frente a amenazas, internas o externas, deliberadas o accidentales, con el fin de asegurar el cumplimiento de la confidencialidad, integridad, disponibilidad, legalidad y confiabilidad de la información ***MEDIANTE*** directrices claras y procedimientos definidos en los diferentes ámbitos de gestión institucional.

4.1.2 Objetivos Específicos

- Establecer un esquema de seguridad con directrices claras.
- Concientizar a todos los funcionarios y servidores públicos sobre la importancia de seguir un manual de procedimientos de seguridad.
- Involucrar de manera activa a todo el personal del Ministerio en el cumplimiento de las Políticas de Seguridad.

4.2 Responsabilidades

Es responsabilidad de la Dirección de Tecnologías de la Información, desarrollar, revisar y divulgar los procedimientos de seguridad por cualquier medio de difusión (intranet, email, sitio web oficial, etc.).

Todos los Subsecretarios, Coordinadores Generales, Directores Nacionales, Directores Provinciales, Gerentes y demás autoridades a nivel nacional, son responsables del cumplimiento de las Políticas de Seguridad de la Información por parte de su equipo de trabajo dentro de sus dependencias.

Las Políticas de Seguridad de la Información es de aplicación obligatoria para todo el personal de la institución, cualquiera sea su situación contractual, o nivel jerárquico.

La **máxima autoridad de la institución o su delegado** será responsable de aprobar las políticas y de autorizar modificaciones o actualizaciones de ser el caso, y dispondrá la implementación del Esquema Gubernamental de Seguridad de la Información (EGSI) en la institución.

Se difundirá la siguiente Política de Seguridad de la Información como referencia al Acuerdo 025-2019 (emitido el 20 de septiembre de 2019 y publicado en el Registro Oficial Edición Especial 228 de 10 enero de 2020), **Artículo 1:** donde se expide el Esquema Gubernamental de Seguridad de la Información -EGSI-, el cual es de implementación obligatoria en las Instituciones de la Administración Pública Central, Institucional y que dependen de la Función Ejecutiva; **Artículo 3:** Recomendar a las Instituciones de la Administración Pública Central, Institucional y que dependen de la Función Ejecutiva, utilicen como guía las Normas Técnicas Ecuatorianas NTE INEN-ISO/IEC 27000 para la Gestión de Seguridad de la información.

Mediante Acuerdo Ministerial Nro. 007-20 de 05 de febrero de 2020, el Ministro de Desarrollo Urbano y Vivienda, Arq. Guido Macchiavello, acuerda crear el Comité de Seguridad de la Información del MIDUVI, quien procederá a revisar y proponer a la máxima autoridad de la Institución para su aprobación la Política de Seguridad de la Información y las funciones generales en materia de seguridad de la información; y tendrá las siguientes responsabilidades:

a) Gestionar la aprobación de la política y normas institucionales en materia de seguridad de la información, por parte de la máxima autoridad de la Institución.
b) Realizar el seguimiento de los cambios significativos de los riesgos que afectan a los recursos de información frente a las amenazas más importantes.
c) Tomar conocimiento y supervisar la investigación y monitoreo de los incidentes relativos a la seguridad de la información, con nivel de impacto alto.
d) Coordinar la implementación de controles específicos de seguridad de la información para nuevos sistemas o servicios, en base al EGSI.
e) Promover la difusión de la seguridad de la información dentro de la institución.
f) Coordinar el proceso de gestión de la continuidad de la operación de los servicios y sistemas de información de la institución frente a incidentes de seguridad imprevistos.
g) El comité deberá convocarse bimensualmente o cuando las circunstancias lo ameriten, se deberá llevar registros y actas de las reuniones.
h) Informar a la máxima autoridad los avances de la implementación del Esquema Gubernamental de Seguridad de la Información (EGSI).
i) Reportar a la máxima autoridad las alertas que impidan la implementación del Esquema Gubernamental de Seguridad de la Información (EGSI).
j) Recomendar a la máxima autoridad mecanismos que viabilicen la implementación del Esquema Gubernamental de Seguridad de la Información (EGSI).

El **Oficial de Seguridad de la Información** será el responsable de coordinar las acciones del Comité de Seguridad de la Información y de impulsar la implementación y cumplimiento del Esquema Gubernamental de Seguridad de la Información; tendrá las siguientes responsabilidades:

a) Identificar todas las personas o instituciones públicas o privadas, que de alguna forma influyen o impactan en la implementación del EGSI.
b) Generar propuestas para la elaboración de la documentación esencial del Esquema Gubernamental de Seguridad de la Información (EGSI).
c) Asesorar a los funcionarios en la ejecución del Estudio de Gestión de Riesgos de Seguridad de la Información en las diferentes áreas.
d) Elaborar el Plan de concienciación en Seguridad de la Información basado en el Esquema Gubernamental de Seguridad de la Información (EGSI).
e) Elaborar un plan de seguimiento y control de la implementación de las medidas de mejora o acciones correctivas.
f) Coordinar la elaboración del Plan de Continuidad de Seguridad de la Información
g) Orientar y generar un procedimiento adecuado para el manejo de los incidentes de seguridad de la información presentados al interior de la institución.

h) Coordinar la gestión de incidentes de seguridad con nivel de impacto alto a través de otras instituciones gubernamentales.
i) Mantener la documentación de la implementación del EGSI debidamente organizada.
j) Verificar el cumplimiento de las norman procedimientos y controles de seguridad institucionales establecidos.
k) Informar al Comité de Seguridad de la Información, el avance de la implementación del Esquema Gubernamental de Seguridad de la Información (EGSI), así como las alertas que impidan su implementación.
l) Previa la terminación de sus funciones el Oficial de Seguridad realizará la transferencia de la documentación e información de la que fue responsable al nuevo Oficial de Seguridad, en caso de ausencia, al Comité de Seguridad de la Información.

Los **Propietarios de la Información** son responsables de clasificarla de acuerdo con el grado de sensibilidad y criticidad de la misma, de documentar y mantener actualizada la clasificación efectuada, y de definir qué usuarios deberán tener permisos de acceso a la información de acuerdo a sus funciones y competencia.

El **Responsable de la Dirección de Administración del Talento Humano en coordinación con la Dirección de Cambio y Cultura Organizacional y la Dirección de Comunicación Social** cumplirán la función de difundir a todo el personal que ingresa a la Institución de sus obligaciones respecto del cumplimiento de la Política de Seguridad de la Información y de todas las normas, procedimientos y prácticas que de ella surjan. Además, tendrán a su cargo la difusión de la presente Política a todo el personal, de los cambios que en ella se produzcan y las tareas de capacitación continua en materia de seguridad. La Dirección de Administración del Talento Humano será la responsable de la suscripción de los Acuerdos de Confidencialidad (entre otros).

El **Responsable del Área Legal** verificará el cumplimiento de la presente Política en la gestión de todos los contratos, acuerdos u otra documentación de la Institución con los contratistas. Además, asesorará en materia legal a la Institución, en lo que se refiere a la seguridad de la información.

El **Responsable de la Administración de Procesos desarrollará** los procedimientos adecuados de concienciación en materia de seguridad controles de acceso.

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

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

4.3 Aspectos Generales

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

- ***Organización de la Seguridad de la Información;*** orientado a la institución debe definir y asignar claramente todas las responsabilidades para la seguridad de la información administrar

la seguridad de la información dentro de la Institución y establecer un marco gerencial para controlar su implementación.

- ***Gestión de Activos;*** orientado a Inventariar, identificar y actualizar todos los activos asociados con la información, y las instalaciones para el procesamiento de la información destinado a mantener una adecuada protección de los activos de la Institución.
- ***Seguridad de los Recursos Humanos;*** orientado a verificar antecedentes de candidatos a ser empleados, contratistas o usuarios de terceras partes, designaciones y promociones de funcionarios de acuerdo con los reglamentos, la ética y las leyes pertinentes, y deben ser proporcionales a la naturaleza y actividades de la institución pública, a la clasificación de la información a la cual se va a tener acceso y los riesgos percibidos. No debe entenderse este control como discriminatorio en ningún aspecto.
- ***Seguridad Física y del Entorno;*** destinada a impedir accesos no autorizados, daños e interferencia a las sedes e información de la Institución.
- ***Gestión de las Comunicaciones y las Operaciones;*** dirigido a garantizar el funcionamiento correcto y seguro de las instalaciones de procesamiento de la información y medios de comunicación.
- ***Control de Acceso;*** orientado a controlar el acceso lógico a la información.
- ***Criptografía;*** orientado a elaborar, implementar y socializar una política que regule el uso de controles criptográficos para la protección de la información, de acuerdo al nivel de protección requerida
- ***Seguridad de las Operaciones;*** orientado a elaborar, implementar y socializar los procedimientos de operación y poner a disposición de los usuarios del área respectiva.
- ***Seguridad en las Comunicaciones;*** orientado a administrar y controlar las redes para proteger la información en sistemas y aplicaciones institucionales.
- ***Adquisición, Desarrollo y Mantenimiento de los Sistemas;*** orientado a garantizar la incorporación de medidas de seguridad en los sistemas de información desde su desarrollo y/o implementación y durante su mantenimiento.
- ***Relaciones con Proveedores;*** orientado a elaborar, implementar y socializar, la política relacionada con el acceso del proveedor y terceras personas, a los activos de la institución, debe documentarse formalmente los acuerdos con el proveedor, para mitigar los riesgos asociados.
- ***Gestión de Incidentes de Seguridad de la Información;*** orientado a establecer formalmente responsabilidades y procedimientos para asegurar una respuesta rápida, efectiva y acorde a los Incidentes de seguridad de la Información que pueden ocurrir en la Institución.
- ***Administración de la Continuidad de las Actividades de la Institución;*** orientado a contrarrestar las interrupciones de las actividades y proteger los procesos críticos de los efectos de fallas significativas o desastres.
- ***Cumplimiento;*** destinado a impedir infracciones y violaciones de las leyes del derecho civil y penal; de las obligaciones establecidas por leyes, estatutos, normas, reglamentos o contratos; y de los requisitos de seguridad.

El Comité de Seguridad de la Información revisará anualmente la presente Política, a efectos de mantenerla actualizada. Además, efectuará toda modificación que sea necesaria en función a posibles cambios que puedan afectar su definición, como: cambios tecnológicos, variación de los costos de los controles, reformas al estatuto orgánico por procesos, impacto de los incidentes de seguridad, etc.

4.4 Sanciones previstas por Incumplimiento

El incumplimiento de la Política de Seguridad de la Información tendrá como resultado la aplicación de diversas sanciones, conforme a la magnitud y característica del aspecto no cumplido; y de acuerdo a lo establecido en la Ley.

5 ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

5.1 Generalidades

La presente Política establece la administración de la Seguridad de la Información, como parte fundamental de los objetivos y actividades del MIDUVI. Por ello, se definirá formalmente un ámbito de gestión para efectuar tareas tales, como: la aprobación de la Política, la coordinación de su implementación y la asignación de funciones y responsabilidades. Además, se contempla la necesidad de disponer de fuentes con conocimiento y experimentadas para el asesoramiento, cooperación y colaboración en materia de seguridad de la información.

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

5.2 Objetivo

- Administrar la seguridad de la información dentro de la Institución y establecer un marco gerencial para iniciar y controlar su implementación, así como para la distribución de funciones y responsabilidades.
- Fomentar la consulta y cooperación con Instituciones especializadas para la obtención de asesoría en materia de seguridad de la información.
- Garantizar la aplicación de medidas de seguridad adecuadas en los accesos de terceros a la información de la Institución.

5.3 Alcance

La Política se aplica a todos los recursos de la Institución y sus relaciones con terceros que implique el acceso a sus datos, recursos y/o a la administración y control de los sistemas de información.

5.4 Responsabilidad

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

El Oficial de Seguridad de la Información asistirá al personal de la Institución en materia de seguridad de la información y coordinará la interacción con Instituciones especializadas. Además, junto con los propietarios de la información, analizará el riesgo de los accesos de terceros a la información de la Institución y verificará la aplicación de las medidas de seguridad necesarias para la protección de la misma.

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

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

6. POLÍTICA

6. 1 Estructura de la Seguridad de la Información

6.1.1 Conformación del Comité de Seguridad de la Información

La seguridad de la información es una responsabilidad de la Institución compartida por todas las Autoridades Políticas, Subsecretarios, Coordinadores, Directores Nacionales o equivalentes, por lo cual se crea el Comité de Seguridad de la Información mediante Acuerdo Ministerial Nro. 007-20 de 05 de febrero de 2020, integrado por representantes de los procesos mencionados, destinado a garantizar el apoyo manifiesto de las autoridades a las iniciativas de seguridad. El mismo contará con un Presidente, quien cumplirá la función de impulsar la implementación de la presente Política.

Conformación del Comité de Seguridad de la Información	
Área / Unidad	**Representante**
Despacho Ministerial	Delegado de la máxima Autoridad.
Subsecretaría de Vivienda	Subsecretario (a) de Vivienda o su delegado.
Subsecretaría de Hábitat y Espacio Público	Subsecretario (a) de Hábitat y Espacio Público o su delegado.
Subsecretaría de Uso, Gestión del Suelo y Catastros	Subsecretario (a) de Uso, Gestión del Suelo y Catastros o su delegado
Coordinación General de Asesoría Jurídica	Coordinador (a) General de Asesoría Jurídica o su delegado.
Director de Talento Humano	Director (a) de Talento Humano o su delegado.
Director Administrativo	Director (a) Administrativo o su delegado.
Director de Comunicación	Director (a) de Comunicación o su delegado.
Coordinación General de Gestión Estratégica y Planificación	Coordinador (a) General de Gestión Estratégica y Planificación o su delegado.
Dirección de Tecnologías de la Información	Director (a) de Tecnologías de la Información.

El delegado de la Coordinación General de Gestión Estratégica y Planificación, actuará como Secretario del Comité.

6.1.2 Asignación de Responsabilidades en Materia de Seguridad de la Información

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

Proceso	**Responsable**
Gestión de Activos	Dirección Administrativa
Seguridad de los Recursos Humanos	Dirección de Administración del Talento Humano
Seguridad Física y del Entorno	Dirección de Administración del Talento Humano y Dirección Administrativa
Gestión de las Comunicaciones y las Operaciones	Dirección de Tecnologías de la Información

Criptografía	Dirección de Tecnologías de la Información
Control de Accesos	Dirección de Tecnologías de la Información
Seguridad de las Operaciones	Dirección de Tecnologías de la Información
Seguridad de las Comunicaciones	Dirección de Tecnologías de la Información
Adquisición, Desarrollo y Mantenimiento de Sistemas	Dirección de Tecnologías de la Información
Relaciones con Proveedores	Dirección Administrativa, Dirección de Tecnologías de la Información
Gestión de Incidentes de Seguridad de la Información	Todas las Direcciones apoyados con Oficial de Seguridad de la Información
Administración de la Continuidad de las Actividades de la Institución	Dirección de Tecnologías de la Información, Dirección de Administración del Talento Humano y Dirección Administrativa
Cumplimiento	El Comité y Oficial de Seguridad de la Información

De igual forma, cada Unidad o Dirección debe detallar los propietarios de la información, quienes serán los Responsables de las Unidades Organizativas o Procesos a cargo del manejo de la misma y de la información que generan y administran.

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

6.1.3 Proceso de Autorización para Instalaciones de Procesamiento de Información

Los nuevos recursos de procesamiento de información serán autorizados por los responsables de las Unidades Organizativas involucradas, considerando su propósito y uso, conjuntamente con el Oficial de Seguridad de la Información, a fin de garantizar que se cumplan todas las políticas y requerimientos de seguridad pertinentes. Cuando corresponda, se verificará el hardware y software para garantizar su compatibilidad con los componentes de otros sistemas de la Institución.

El uso de recursos personales de procesamiento de información en el lugar de trabajo puede ocasionar vulnerabilidades; en consecuencia, su uso será evaluado en cada caso por el Oficial de Seguridad de la Información y deberá ser autorizado por el Director de Tecnologías de la Información y por el Director Nacional (o su equivalente) responsable del área al que se destinen los recursos.

6.1.4 Asesoramiento especializado en materia de Seguridad de la Información

El Oficial de Seguridad de la Información será el encargado de coordinar los conocimientos y las experiencias disponibles en la Institución a fin de brindar ayuda en la toma de decisiones en materia de seguridad. Éste podrá obtener asesoramiento del ente rector de Gobierno Electrónico: el Ministerio de Telecomunicaciones y Sociedad de la Información, con el objeto de optimizar su gestión, se habilitará al Oficial de Seguridad de la Información el contacto con todas las Unidades y/o Áreas de la Institución.

El intercambio de información confidencial para fines de asesoramiento o de transmisión de experiencias, sólo se permite cuando se haya firmado un Compromiso o Acuerdo de Confidencialidad ***(ANEXO 1)*** previo o con aquellas Organizaciones especializadas en temas relativos a la Seguridad de la Información cuyo personal está obligado a mantener la confidencialidad de los temas que trata.

6.1.5 Revisión independiente de la Seguridad de la Información

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

6.2 Seguridad frente al acceso por parte de Terceros

6.2.1 Identificación de Riesgos del Acceso de Terceras Partes

Cuando exista la necesidad de otorgar acceso a terceras partes a información de la Institución, el Oficial de Seguridad de la Información y el propietario de la Información requerida, llevarán a cabo y documentarán una evaluación de riesgos para identificar los requerimientos de controles específicos, teniendo en cuenta, entre otros aspectos:

- El tipo de acceso requerido (físico/lógico y a qué recurso).
- Los motivos para los cuales se solicita el acceso.
- El valor de la información.
- La incidencia de este acceso en la seguridad de la información de la Institución.

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

Se cita a modo de ejemplo:

a) Personal de mantenimiento y soporte de hardware y software.
b) Limpieza, "catering", guardia de seguridad y otros servicios de soporte.
c) Pasantías y otras designaciones de corto plazo.
d) Consultores.

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

6.2.2 Requerimientos de seguridad en Contratos o Acuerdos con Terceros

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

a) Cumplimiento de la Política de Seguridad de la Información de la Institución.
b) Protección de los activos de la Institución, incluyendo:
    - Procedimientos para proteger los bienes de la Institución, abarcando los activos físicos, la información y el software.

- Procedimientos para determinar si ha ocurrido algún evento que comprometa los bienes, por ejemplo, debido a pérdida o modificación de datos.
- Controles para garantizar la recuperación o destrucción de la información y los activos al finalizar el contrato o acuerdo, o en un momento convenido durante la vigencia del mismo.
- Restricciones a la copia y divulgación de información.

c) Descripción de los servicios disponibles.
d) Nivel de servicio esperado y niveles de servicio aceptables.
e) Permiso para el acceso de personal, cuando sea necesario.
f) Obligaciones de las partes emanadas en el acuerdo y responsabilidades legales.
g) Existencia de Derechos de Propiedad Intelectual.
h) Definiciones relacionadas con la protección de datos.
i) Acuerdos de control de accesos que contemplen:
   - Métodos de acceso permitidos, y el control y uso de identificadores únicos como identificadores de usuario y contraseñas de usuarios.
   - Proceso de autorización de accesos y privilegios de usuarios.
   - Requerimiento para mantener actualizada una lista de personas autorizadas a utilizar los servicios que han de implementarse y sus derechos y privilegios con respecto a dicho uso.
j) Definición de criterios de desempeño comprobables, de monitoreo y de presentación de informes.
k) Adquisición de derecho a auditar responsabilidades contractuales o surgidas del acuerdo.
l) Establecimiento de un proceso para la resolución de problemas y en caso de corresponder, disposiciones con relación a situaciones de contingencia.
m) Responsabilidades relativas a la instalación y al mantenimiento de hardware y software.
n) Proceso de elaboración y presentación de informes que contemple un acuerdo con respecto a los formatos.
o) Proceso claro y detallado de administración de cambios.
p) Controles de protección física requeridos y los mecanismos que aseguren la implementación de los mismos.
q) Métodos y procedimientos de entrenamiento de usuarios y administradores en materia de seguridad.
r) Controles que garanticen la protección contra software malicioso.
s) Elaboración y presentación de informes, notificación e investigación de incidentes y violaciones relativos a la seguridad.
t) Relación entre proveedores y subcontratistas.

6.3 Gestión de Activos

6.3.1 Generalidades

La Institución debe tener un conocimiento cabal y minucioso sobre los activos que posee como parte importante de la administración de riesgos. Algunos ejemplos de activos son:

- Recursos de información: bases de datos y archivos, catálogo de procesos, documentación de sistemas, manuales de usuario, material de capacitación, procedimientos operativos o de soporte, planes de continuidad, información archivada, etc.
- Recursos de software: software de aplicaciones, sistemas operativos, herramientas de desarrollo, utilitarios, etc.
- Activos físicos: equipamiento informático (procesadores, monitores, computadoras portátiles, módems), equipos de comunicaciones (routers, PBXs, máquinas de fax, contestadores automáticos, teléfonos IP), medios magnéticos (cintas, discos), otros equipos técnicos (relacionados con el suministro eléctrico, unidades de aire acondicionado), mobiliario, lugares de emplazamiento, etc.

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

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

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

Las pautas de clasificación deben prever y contemplar el hecho de que la clasificación de un ítem de información determinado no necesariamente debe mantenerse invariable por siempre, y que ésta puede cambiar de acuerdo con una Política predeterminada. Se debe considerar la cantidad de categorías a definir para la clasificación.

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

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

6.3.2 Objetivo

- Garantizar que los activos de información reciban un apropiado nivel de protección.
- Clasificar la información para señalar su sensibilidad y criticidad.
- Definir niveles de protección y medidas de tratamiento especial acordes a su clasificación.

6.3.3 Alcance

Se aplica a toda la información administrada en la Institución, cualquiera sea el soporte en que se encuentre.

6.3.4 Responsabilidad

Los propietarios de la información son los encargados de clasificarla de acuerdo con su grado de sensibilidad y criticidad, de documentar y mantener actualizada la clasificación efectuada, y de definir las funciones que deberán tener permisos de acceso a la información.

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

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

6.3.5 Política de Inventario de Activos

Se identificarán los activos importantes asociados a cada sistema de información, sus respectivos propietarios y su ubicación, para luego elaborar un inventario con dicha información.

El mismo será actualizado ante cualquier modificación de la información registrada y revisado con una periodicidad semestral entre la Dirección Administrativa y la Dirección de Tecnologías de la Información.

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

6.3.6 Clasificación de la Información

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

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

- Confidencialidad:
  0- Información que puede ser conocida y utilizada sin autorización por cualquier persona, sea funcionario o servidor público de la Institución o no. **PUBLICO**.
  1- Información que puede ser conocida y utilizada por todos los funcionarios y/o servidores públicos de la Institución y algunas entidades externas debidamente autorizadas, y cuya divulgación o uso no autorizados podría ocasionar riesgos o pérdidas leves para la Institución, al Sector Público Nacional o terceros. **RESERVADA – USO INTERNO**.
  2- Información que sólo puede ser conocida y utilizada por un grupo de funcionarios y/o servidores públicos, que la necesiten para realizar su trabajo, y cuya divulgación o uso no autorizados podría ocasionar pérdidas significativas a la Institución, al Sector Público Nacional o a terceros. **RESERVADA – CONFIDENCIAL.**
  3- Información que sólo puede ser conocida y utilizada por un grupo muy reducido de funcionarios o servidores públicos, generalmente de nivel jerárquico superior o la máxima autoridad de la Institución, y cuya divulgación o uso no autorizados podría ocasionar pérdidas graves al mismo, al Sector Público Nacional o a terceros. **RESERVADA SECRETA**.

- Integridad:
  0- Información cuya modificación no autorizada puede repararse fácilmente, o no afecta la operación de la Institución.
  1- Información cuya modificación no autorizada puede repararse aunque podría ocasionar pérdidas leves para la Institución, al Sector Público Nacional o terceros.
  2- Información cuya modificación no autorizada es de difícil reparación y podría ocasionar pérdidas significativas para la Institución, al Sector Público Nacional o terceros.
  3- Información cuya modificación no autorizada no podría repararse, ocasionando pérdidas graves a la Institución, al Sector Público Nacional o a terceros.

- Disponibilidad:
  0- Información cuya inaccesibilidad no afecta la operatoria de la Institución.
  1- Información cuya inaccesibilidad permanente durante 7 días (definir un plazo no menor a una semana) podría ocasionar pérdidas significativas para la Institución, el Sector Público

Nacional o terceros.

2- Información cuya inaccesibilidad permanente durante 24 horas (definir un plazo no menor a un día) podría ocasionar pérdidas significativas a la Institución, al Sector Público Nacional o a terceros.
3- Información cuya inaccesibilidad permanente durante 1 hora (definir un plazo no menor a una hora) podría ocasionar pérdidas significativas a la Institución, al Sector Público Nacional o a terceros.

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

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

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

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

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

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

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

6.3.7 Rotulado de la Información.

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

- Copia;
- Almacenamiento;
- Transmisión por correo, correo electrónico;
- Transmisión oral (telefonía fija y móvil, correo de voz, contestadores automáticos, etc.).

6.4 Seguridad de los Recursos Humanos

6.4.1 Generalidades

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

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

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

6.4.2 Objetivo

- Reducir los riesgos de error humano, comisión de ilícitos, uso inadecuado de instalaciones y recursos, y manejo no autorizado de la información.
- Explicitar las responsabilidades en materia de seguridad en la etapa de reclutamiento de personal e incluirlas en los acuerdos a firmarse y verificar su cumplimiento durante el desempeño del individuo como empleado.
- Garantizar que los usuarios estén al corriente de las amenazas e incumbencias en materia de seguridad de la información, y se encuentren capacitados para respaldar la Política de Seguridad de la Institución en el transcurso de sus tareas normales.
- Suscribir acuerdo de confidencialidad con todo el personal y usuarios externos de las instalaciones de procesamiento de información.
- Establecer las herramientas y mecanismos necesarios para promover la comunicación de debilidades existentes en materia de seguridad, así como de los incidentes ocurridos, con el objeto de minimizar sus efectos y prevenir su reincidencia.

6.4.3 Alcance

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

6.4.4 Responsabilidad

El Oficial de Seguridad de la Información tiene a cargo el seguimiento, documentación y análisis de los incidentes de seguridad reportados así como su comunicación al Comité de Seguridad de la Información, a los propietarios de la información y a la Dirección de Tecnologías de la Información.

El Comité de Seguridad de la Información será responsable de implementar los medios y canales necesarios para que el Oficial de Seguridad de la Información maneje los reportes de incidentes y

anomalías de los sistemas. Así mismo, dicho Comité, tomará conocimiento, efectuará el seguimiento de la investigación, controlará la evolución e impulsará la resolución de los incidentes relativos a la seguridad.

El Responsable del Área de Talento Humano participará en la elaboración del Acuerdo de Confidencialidad a firmar por los funcionarios, servidores públicos y terceros que desarrollen funciones en la institución,

Todo el personal de la Institución es responsable del reporte de debilidades e incidentes de seguridad que oportunamente se detecten.

6.4.5 Control y Política del Personal

El incumplimiento de lo estipulado en el Acuerdo de Confidencialidad será sancionado según lo estipula la Ley Orgánica de Servicio Público su Reglamento y el Código de Trabajo.

6.4.6 Acuerdo de Confidencialidad

Como parte de sus términos y condiciones iniciales de contrato, los funcionarios y servidores públicos, cualquiera sea su situación de contratación, firmarán un Acuerdo de Confidencialidad o no divulgación, en lo que respecta al tratamiento de la información de la Institución. La copia firmada del Acuerdo deberá ser archivada en el expediente personal de cada servidor público por la Dirección de Administración del Talento Humano...

Además, mediante el Acuerdo de Confidencialidad el funcionario o servidor público declarará conocer y aceptar la existencia de determinadas actividades que pueden ser objeto de control y monitoreo. Estas actividades deben ser detalladas a fin de no violar el derecho a la privacidad del funcionario y/o servidor público.

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

a) Suscripción inicial del Acuerdo por parte de la totalidad del personal.
b) Revisión del contenido del Acuerdo y actualización del mismo cada año.
c) Método de re suscripción en caso de modificación del texto del Acuerdo.

6.4.7 Términos y Condiciones de Contratación

Los términos y condiciones del contrato establecerán la responsabilidad del funcionario y servidor público en materia de seguridad de la información.

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

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

6.4.8 Capacitación del funcionario y servidor público en Materia de Seguridad de la Información

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

Los Responsables de la Dirección de Gestión del Cambio y Cultura Organizacional en coordinación con la Dirección de Comunicación Social serán los encargados de difundir la Política de Seguridad de la Información; y, la Dirección de Administración del Talento Humano será la encargada de coordinar las acciones de capacitación que surjan de la presente Política.

Cada seis meses se revisará el material correspondiente a la capacitación, a fin de evaluar la pertinencia de su actualización, de acuerdo al estado del arte de ese momento.

Las siguientes áreas serán encargadas de producir el material de capacitación

Áreas Responsables del Material de Capacitación

Dirección de Administración del Talento Humano
Dirección de Gestión del Cambio y Cultura Organizacional
Dirección de Comunicación Social
Dirección de Tecnologías de la Información y Comunicación

El personal que ingrese a la Institución recibirá el material referente a seguridad de la información, se le informará el comportamiento esperado en lo que respecta a la seguridad de la información, antes de serle otorgados los privilegios de acceso a los sistemas que correspondan.

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

6.4.9 Respuesta a Incidentes y Anomalías en Materia de Seguridad, Comunicación de Incidentes Relativos a la Seguridad

Los incidentes relativos a la seguridad serán comunicados a través de canales oficiales apropiados tan pronto como sea posible.

Se establecerá un procedimiento formal de comunicación y de respuesta a incidentes, indicando la acción que ha de emprenderse al recibir un informe sobre incidentes.

Dicho procedimiento deberá contemplar que ante la detección de un supuesto incidente o violación de la seguridad, el Oficial de Seguridad de la Información sea informado tan pronto como se haya tomado conocimiento. Este indicará los recursos necesarios para la investigación y resolución del incidente, y se encargará de su monitoreo. Así mismo, mantendrá al Comité de Seguridad al tanto de la ocurrencia de incidentes de seguridad.

Todos los funcionarios, servidores públicos, contratistas, consultores, y personal que integre equipos de trabajo por convenios de asistencia técnica o cooperación internacional que trabajan en la institución; deben conocer el procedimiento de comunicación de incidentes de seguridad, y deben informar de los mismos tan pronto hayan tomado conocimiento de su ocurrencia.

6.4.10 Comunicación de Debilidades en Materia de Seguridad

Los usuarios de servicios de información, al momento de tomar conocimiento directo o indirectamente acerca de una debilidad de seguridad, son responsables de registrar y comunicar las mismas al Oficial de Seguridad de la Información.

Se prohíbe a los usuarios la realización de pruebas para detectar y/o utilizar una supuesta debilidad o falla de seguridad.

6.4.11 Comunicación de Anomalías del Software

Se establecerán procedimientos para la comunicación de anomalías de software, los cuales deberán:

a) Registrar los síntomas del problema y los mensajes que aparecen en pantalla.
b) Establecer las medidas de aplicación inmediata ante la presencia de una anomalía.
c) Alertar inmediatamente al Oficial de Seguridad de la Información o del Activo de que se trate.

Se prohíbe a los usuarios quitar el software que supuestamente tiene una anomalía, a menos que estén autorizados formalmente para hacerlo. La recuperación será realizada por personal experimentado, adecuadamente habilitado.

6.4.12 Aprendiendo de los Incidentes

Se definirá un proceso que permita documentar, cuantificar y monitorear los tipos, volúmenes y costos de los incidentes y anomalías. Esta información se utilizará para identificar aquellos que sean recurrentes o de alto impacto. Esto será evaluado a efectos de establecer la necesidad de mejorar o agregar controles para limitar la frecuencia, daño y costo de casos futuros.

6.4.13 Procesos Disciplinarios

Se seguirá el proceso disciplinario formal contemplado en las normas legales, estatutarias, reglamentarias y convencionales que rigen al personal de la Administración Pública Nacional, para los funcionarios y servidores públicos que violen la Política, Normas y Procedimientos de Seguridad de la Institución.

La primera vez que el usuario haya incumplido una de las Políticas, el Oficial de Seguridad notificará por escrito al responsable de la falta y le recordará las políticas vigentes.

De presentarse un segundo incumplimiento en las Políticas, la DTIC notificará por escrito al Director de Área correspondiente, informándole el tipo y contenido de la falta, suspendiéndole los servicios tecnológicos al usuario hasta que el Director de Área acepte la restauración de los mismos.

En caso de presentarse un tercer incumplimiento en las Políticas por parte del mismo usuario, causará la suspensión inmediata e indefinida del servicio y el caso se escalará a la Dirección correspondiente para determinar si es necesario aplicar sanciones administrativas adicionales. La DTIC se reserva el suspender el acceso a la red del usuario de manera inmediata, si la seguridad se ve comprometida.

6.5 Seguridad Física y del Entorno

6.5.1 Generalidades

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

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

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

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

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

La información almacenada en los sistemas de procesamiento y la documentación contenida en diferentes medios de almacenamiento, son susceptibles de ser recuperadas mientras no están siendo utilizados. Es por ello que el transporte y la disposición final presentan riesgos que deben ser evaluados.
Gran cantidad de información manejada en las oficinas a nivel nacional se encuentra almacenada en papel, por lo que es necesario establecer pautas de seguridad para la conservación de dicha documentación.

6.5.2 Objetivo

- Prevenir e impedir accesos no autorizados, daños e interferencia a las sedes, instalaciones e información de la Institución.
- Proteger el equipamiento de procesamiento de información crítica de la Institución ubicándolo en áreas protegidas y resguardadas por un perímetro de seguridad definido, con medidas de seguridad y controles de acceso apropiados. Además, contemplar la protección del mismo en su traslado y permanencia fuera de las áreas protegidas, por motivos de mantenimiento u otros.
- Controlar los factores ambientales que podrían perjudicar el correcto funcionamiento del equipamiento informático que alberga la información de la Institución.
- Implementar medidas para proteger la información manejada por el personal en las oficinas, en el marco normal de sus labores habituales.
- Proporcionar protección a los riesgos identificados.

6.5.3 Alcance

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

6.5.4 Responsabilidad

El Oficial de Seguridad de la Información definirá junto con el Responsable de la Dirección de Tecnologías de la Información y los propietarios de la Información, según corresponda, las medidas de seguridad física y ambiental para el resguardo de los activos críticos, en función a un análisis de riesgos, y controlará su implementación. Así mismo, verificará el cumplimiento de las disposiciones sobre seguridad física y ambiental indicadas en el presente.

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

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

Los Propietarios de la Información autorizarán formalmente el trabajo fuera de las instalaciones con información de su incumbencia a los funcionarios y servidores públicos de la Institución cuando lo crean conveniente.

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

6.5.5 Política del Perímetro de Seguridad Física

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

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

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

a) Definir y documentar claramente el perímetro de seguridad.
b) Ubicar las instalaciones de procesamiento de información dentro del perímetro de un edificio o área de construcción físicamente sólida (por ejemplo no deben existir aberturas en el perímetro o áreas donde pueda producirse fácilmente una irrupción). Las paredes externas del área deben ser sólidas y todas las puertas que comunican con el exterior

deben estar adecuadamente protegidas contra accesos no autorizados, por ejemplo mediante mecanismos de control, vallas, alarmas, cerraduras, etc.

c) Verificar la existencia de un área de recepción atendida por personal. Si esto no fuera posible se implementarán los siguientes medios alternativos de control de acceso físico al área o edificio. El acceso a dichas áreas y edificios estará restringido exclusivamente al personal autorizado. Los métodos implementados registrarán cada ingreso y egreso en forma precisa.
d) Extender las barreras físicas necesarias desde el piso (real) hasta el techo (real), a fin de impedir el ingreso no autorizado y la contaminación ambiental, por ejemplo por incendio, humedad e inundación.
e) Identificar claramente todas las puertas de incendio de un perímetro de seguridad.

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

a) Identificación del Edificio y Área.
b) Principales elementos a proteger.
c) Medidas de protección física.

6.5.6 Controles de Acceso Físico

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

a) Supervisar o inspeccionar a los visitantes a áreas protegidas y registrar la fecha y horario de su ingreso y egreso. Sólo se permitirá el acceso mediando propósitos específicos y autorizados e instruyéndose al visitante en el momento de ingreso sobre los requerimientos de seguridad del área y los procedimientos de emergencia.
b) Controlar y limitar el acceso a la información clasificada y a las instalaciones de procesamiento de información, exclusivamente a las personas autorizadas. Se utilizarán los siguientes controles de autenticación para autorizar y validar todos los accesos: (por ejemplo: personal de guardia con listado de personas habilitadas o por tarjeta magnética o inteligente y número de identificación personal, etc.). Se mantendrá un registro protegido para permitir auditar todos los accesos.
c) Implementar el uso de una identificación unívoca visible para todo el personal del área protegida, e instruirlo acerca de cuestionar la presencia de desconocidos no escoltados por personal autorizado y a cualquier persona que no exhiba una identificación visible.
d) Revisar y *actualizar cada 6 meses* los derechos de acceso a las áreas protegidas, los que serán documentados y firmados por el Responsable de la Unidad Organizativa de la que dependa.
e) Revisar los registros de acceso a las áreas protegidas. Esta tarea la realizará la Unidad de Auditoría Interna o en su defecto quien sea propuesto por el Comité de Seguridad de la Información.

6.5.7 Protección de Oficinas, Recintos e Instalaciones

Para la selección y el diseño de un área protegida se tendrá en cuenta la posibilidad de daño producido por incendio, inundación, explosión, agitación civil, y otras formas de desastres naturales o provocados por el hombre. También se tomarán en cuenta las disposiciones y normas (estándares) en materia de sanidad y seguridad. Así mismo, se considerarán las amenazas a la

seguridad que representan los edificios y zonas aledañas, por ejemplo, filtración de agua desde otras instalaciones.

La Dirección Administrativa deberá definir los sitios considerados como áreas protegidas de la Institución; sobre la base del requerimiento del Oficial de Seguridad de la Información.

La Dirección Administrativa deberá supervisar el cumplimiento de los contratos o convenios con terceros sobre la seguridad y accesos físicos a las instalaciones de la institución y áreas protegidas. (Entiéndase por terceros a empresas o instituciones externas que dan el servicio de Seguridad, en este caso INMOBILIAR (Plataforma Gubernamental de lo Social); y BEV (Cordero y 10 de Agosto)).

Se establecen las siguientes medidas de protección para áreas protegidas:

a) Ubicar las instalaciones críticas en lugares a los cuales no pueda acceder personal no autorizado.
b) Establecer que los edificios o sitios donde se realicen actividades de procesamiento de información serán discretos y ofrecerán un señalamiento mínimo de su propósito, sin signos obvios, exteriores o interiores.
c) Ubicar las funciones y el equipamiento de soporte, por ejemplo: impresoras, fotocopiadoras, etc., adecuadamente dentro del área protegida para evitar solicitudes de acceso, el cual podría comprometer la información.
d) Establecer que las puertas y ventanas permanecerán cerradas cuando no haya vigilancia. Se agregará protección externa a las ventanas, en particular las que se encuentran en planta baja o presenten riesgos especiales.
e) Implementar los siguientes mecanismos de control para la detección de intrusos: Sistema de Registro y control en todos los puntos de ingreso y salida de nuestros locales; sistema de monitoreo por cámaras de Seguridad en el Edificio BEV; el mismo que alberga el Centro de Datos del MIDUVI.
f) Separar las instalaciones de procesamiento de información administradas por la Institución de aquellas administradas por terceros.
g) Restringir el acceso público a las guías telefónicas y listados de teléfonos internos que identifican las ubicaciones de las instalaciones de procesamiento de información sensible.
h) Almacenar los equipos redundantes y la información de resguardo (back up) en un sitio seguro y distante del lugar de procesamiento, para evitar daños ocasionados ante eventuales contingencias en el sitio principal, por petición expresa del Oficial de Seguridad de la Información

6.5.8 Desarrollo de Tareas en Áreas Protegidas

Para incrementar la seguridad de las áreas protegidas, se establecen los siguientes controles y lineamientos adicionales. Esto incluye controles para el personal que trabaja en el área protegida, así como para las actividades de terceros que tengan lugar allí:

a) Dar a conocer al personal la existencia del área protegida, o de las actividades que allí se llevan a cabo, sólo si es necesario para el desarrollo de sus funciones.
b) Evitar la ejecución de trabajos por parte de terceros sin supervisión.
c) Bloquear físicamente e inspeccionar periódicamente las áreas protegidas desocupadas.
d) Limitar el acceso al personal del servicio de soporte externo a las áreas protegidas o a las instalaciones de procesamiento de información sensible. Este acceso, como el de

cualquier otra persona ajena que requiera acceder al área protegida, será otorgado solamente cuando sea necesario y se encuentre autorizado y monitoreado. Se mantendrá un registro de todos los accesos de personas ajenas.

e) Pueden requerirse barreras y perímetros adicionales para controlar el acceso físico entre áreas con diferentes requerimientos de seguridad, y que están ubicadas dentro del mismo perímetro de seguridad.
f) Impedir el ingreso de equipos de computación móvil, fotográficos, de vídeo, audio o cualquier otro tipo de equipamiento que registre información, a menos que hayan sido formalmente autorizadas por el Responsable de dicho área o el Responsable de la Dirección de Tecnologías de la Información y el Oficial de Seguridad de la Información.
g) Prohibir comer, beber y fumar dentro de las instalaciones de procesamiento de la información.

6.5.9 Aislamiento de las Áreas de Recepción y Distribución

Se controlarán las áreas de Recepción y Distribución, las cuales estarán aisladas de las instalaciones de procesamiento de información, a fin de impedir accesos no autorizados.

Para ello se establecerán controles físicos que considerarán los siguientes lineamientos:

a) Limitar el acceso a las áreas de depósito, desde el exterior de la sede de la Institución, sólo al personal previamente identificado y autorizado.
b) Diseñar el área de depósito de manera tal que los suministros puedan ser descargados sin que el personal que realiza la entrega acceda a otros sectores del edificio.
c) Inspeccionar el material entrante para descartar peligros potenciales antes de ser trasladado desde el área de depósito hasta el lugar de uso.
d) Registrar el material entrante al ingresar al sitio pertinente.

6.5.10 Ubicación y Protección del Equipamiento y copias de Seguridad

El equipamiento será ubicado y protegido de tal manera que se reduzcan los riesgos ocasionados por amenazas y peligros ambientales, y las oportunidades de acceso no autorizado, teniendo en cuenta los siguientes puntos:

a) Ubicar el equipamiento en un sitio donde se minimice el acceso innecesario y provea un control de acceso adecuado.
b) Ubicar las instalaciones de procesamiento y almacenamiento de información que manejan datos clasificados, en un sitio que permita la supervisión durante su uso.
c) Aislar los elementos que requieren protección especial para reducir el nivel general de protección requerida.
d) Adoptar controles adecuados para minimizar el riesgo de amenazas potenciales, por:

Amenazas Potenciales	Controles
Robo o hurto	Control de ingreso y salida y Cámaras de Seguridad
Incendio	Sistema de Detección de Incendios, Seguro contra incendios.
Humo	Sistema de Detección de Incendios, seguro contra incendios.
Inundaciones o filtraciones de agua (o falta de suministro)	Plan de mantenimiento de instalaciones hídricas

Polvo	Monitoreo al Servicio de Limpieza a través de la Dirección Administrativa. Talento Humano debe implementar matrices de riesgos.
Vibraciones	Talento Humano debe implementar matrices de riesgos.
Interferencia en el suministro de energía eléctrica (cortes de suministro, variación de tensión)	Tenemos Generadores Eléctricos que proporcionan energía alterna; en el Centro de Datos en el edificio BEV, Calle Cordero y 10 de Agosto
Derrumbes	Seguro contra incendios y líneas aliadas

e) Revisar regularmente las condiciones ambientales para verificar que las mismas no afecten de manera adversa el funcionamiento de las instalaciones de procesamiento de la información. Esta revisión se realizará cada 6 meses.
f) Considerar así mismo el impacto de las amenazas citadas en el punto d) que tengan lugar en zonas próximas a la sede de la Institución.

6.5.11 Suministros de Energía

El equipamiento estará protegido con respecto a las posibles fallas en el suministro de energía u otras anomalías eléctricas. El suministro de energía estará de acuerdo con las especificaciones del fabricante o proveedor de cada equipo. Para asegurar la continuidad del suministro de energía, se contemplarán las siguientes medidas de control:

a) Disponer de múltiples enchufes o líneas de suministro para evitar un único punto de falla en el suministro de energía.
b) Contar con un suministro de energía ininterrumpible (UPS) para asegurar el apagado regulado y sistemático o la ejecución continua del equipamiento que sustenta las operaciones críticas de la Institución. La determinación de dichas operaciones críticas, será el resultado del análisis de impacto realizado por el Oficial de Seguridad de la Información conjuntamente con los Propietarios de la Información con incumbencia. Los planes de contingencia contemplarán las acciones que han de emprenderse ante una falla de la UPS. Los equipos de UPS serán inspeccionados y probados periódicamente para asegurar que funcionan correctamente y que tienen la autonomía requerida.
c) Montar un generador de respaldo para los casos en que el procesamiento deba continuar ante una falla prolongada en el suministro de energía. Deberá realizarse un análisis de impacto de las posibles consecuencias ante una interrupción prolongada del procesamiento, con el objeto de definir qué componentes será necesario abastecer de energía alternativa. Dicho análisis será realizado por el Oficial de Seguridad de la Información conjuntamente con los Propietarios de la Información. Se dispondrá de un adecuado suministro de combustible para garantizar que el generador pueda funcionar por un período prolongado. Cuando el encendido de los generadores no sea automático, se asegurará que el tiempo de funcionamiento de la UPS permita el encendido manual de los mismos. Los generadores serán inspeccionados y probados periódicamente para asegurar que funcionen según lo previsto.

Así mismo, se procurará que los interruptores de emergencia se ubiquen cerca de las salidas de emergencia de las salas donde se encuentra el equipamiento, a fin de facilitar un corte rápido de la energía en caso de producirse una situación crítica. Se proveerá de iluminación de emergencia en caso de producirse una falla en el suministro principal de energía. Se implementará protección contra descargas eléctricas en todos los edificios y líneas de comunicaciones externas de acuerdo a las normativas vigentes.

6.5.12 Seguridad del Cableado

El cableado de energía eléctrica y de comunicaciones que transporta datos o brinda apoyo a los servicios de información estará protegido contra intercepción o daño, mediante las siguientes acciones:

a) Cumplir con los requisitos técnicos vigentes en el País.
b) Utilizar producto o cableado empotrado en la pared, siempre que sea posible, cuando corresponda a las instalaciones de procesamiento de información. En su defecto estarán sujetas a la siguiente protección alternativa: Tecnología Power Line Communications (PLC).
c) Proteger el cableado de red contra intercepción no autorizada o daño mediante los siguientes controles:
   - Uso de conductos de protección.
   - Evitar trayectos que atraviesen áreas públicas sin protección.
   - Uso de canaletas, tuberías plásticas.
   - Construir e implementar canalizaciones adecuadas.
d) Separar los cables de energía de los cables de comunicaciones para evitar interferencias.
e) Proteger el tendido del cableado troncal (backbone) mediante la utilización de ductos blindados.
f) Para los sistemas sensibles o críticos como cableado inteligente o bandejas de fibras ópticas fusionadas se implementarán los siguientes controles adicionales:
   - Instalar conductos blindados y recintos o cajas con cerradura en los puntos terminales y de inspección.
   - Utilizar rutas o medios de transmisión alternativos.

6.5.13 Mantenimiento de Equipos

Se realizará el mantenimiento del equipamiento para asegurar su disponibilidad e integridad permanentes. Para ello se debe considerar:

a) Someter el equipamiento a tareas de mantenimiento preventivo, de acuerdo con los intervalos de servicio y especificaciones recomendados por el proveedor y con la autorización formal del Responsable de la Dirección de Tecnologías de la Información; quien mantendrá un listado actualizado del equipamiento con el detalle de la frecuencia en que se realizará el mantenimiento preventivo (ver formulario en el **ANEXO 2**).
b) Establecer que sólo el personal de mantenimiento autorizado puede brindar mantenimiento y llevar a cabo reparaciones en el equipamiento.
c) Registrar todas las fallas supuestas o reales y todo el mantenimiento preventivo y correctivo realizado.
d) Registrar el retiro de equipamiento de la sede de la Institución para su mantenimiento.
e) Eliminar la información confidencial que contenga cualquier equipamiento que sea necesario retirar, realizándose previamente las respectivas copias de resguardo. Registrar todo equipo informático que ingresa para mantenimiento a la Dirección de Tecnologías de la Información (ver formulario en el **ANEXO 2**).

6.5.14 Seguridad de los Equipos fuera de las Instalaciones.

El uso de equipamiento destinado al procesamiento de información, fuera del ámbito de la Institución, será autorizado por el responsable del bien. En el caso de que en el mismo se almacene información clasificada, deberá ser aprobado además por el Propietario de la misma. 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.

Se respetarán permanentemente las instrucciones del fabricante respecto del cuidado del equipamiento. Así mismo, se mantendrá una adecuada cobertura de seguro para proteger el equipamiento fuera del ámbito de la Institución, cuando sea conveniente.

6.5.15 Desafectación o reutilización segura de los Equipos.

La información puede verse comprometida por una desafectación o una reutilización descuidada del equipamiento. Los medios de almacenamiento conteniendo material sensible, por ejemplo discos rígidos no removibles, previa solicitud de los interesados, deberán ser respaldados y formateados, para finalmente reasignarlos a otros funcionarios de la institución.

En caso de que el medio de almacenamiento se encuentre en mal estado, se recomienda realizar los procedimientos respectivos para darlo de baja.

6.5.16 Retiro de los Bienes

El equipamiento, la información y el software no serán retirados de la sede de la Institución sin autorización formal.
Periódicamente, se llevarán a cabo comprobaciones puntuales para detectar el retiro no autorizado de activos de la Institución, las que serán llevadas a cabo por Control de Bienes. El personal será puesto en conocimiento de la posibilidad de realización de dichas comprobaciones

6.6 Políticas de Escritorios y Pantallas Limpias.

Se adopta una política de escritorios limpios para proteger documentos en papel y dispositivos de almacenamiento removibles y una política de pantallas limpias en las instalaciones de procesamiento de información, a fin de reducir los riesgos de acceso no autorizado, pérdida y daño de la información, tanto durante el horario normal de trabajo como fuera del mismo.
Se aplicarán los siguientes lineamientos:

a) Almacenar bajo llave, cuando corresponda, los documentos en papel y los medios informáticos, en gabinetes y/u otro tipo de mueble seguro cuando no están siendo utilizados, especialmente fuera del horario de trabajo.
b) Guardar bajo llave la información sensible o crítica de la Institución (preferentemente en una caja fuerte o gabinete a prueba de incendios) cuando no está en uso, especialmente cuando no hay personal en la oficina.
c) Desconectar de la red / sistema / servicio las computadoras personales, terminales e impresoras asignadas a funciones críticas, cuando están desatendidas. Las mismas deben ser protegidas mediante cerraduras de seguridad, contraseñas u otros controles cuando no están en uso (como por ejemplo la utilización de protectores de pantalla con contraseña). Los responsables de cada área mantendrán un registro de las contraseñas o copia de las llaves de seguridad utilizadas en el sector a su cargo. Tales elementos se encontrarán protegidos en sobre cerrado o caja de seguridad para impedir accesos no autorizados, debiendo dejarse constancia de todo acceso a las mismas, y de los motivos que llevaron a tal acción.
d) Proteger los puntos de recepción y envío de correo postal y las máquinas de fax no atendidas.
e) Bloquear las fotocopiadoras (o protegerlas de alguna manera del uso no autorizado) fuera del horario normal de trabajo.

f) Retirar inmediatamente la información sensible o confidencial, una vez impresa.

6.7 Gestión de Comunicaciones y Operaciones

6.7.1 Generalidades

La proliferación de software malicioso, como virus, troyanos, etc., hace necesario que se adopten medidas de prevención, a efectos de evitar la ocurrencia de tales amenazas.
Es conveniente separar los ambientes de desarrollo, prueba y operaciones de los sistemas de la Institución, estableciendo procedimientos que aseguren la calidad de los procesos que se implementen en el ámbito operativo, a fin de minimizar los riesgos de incidentes producidos por la manipulación de información operativa.

Los sistemas de información están comunicados entre sí, tanto dentro de la Institución como con terceros fuera de él. Por lo tanto es necesario establecer criterios de seguridad en las comunicaciones que se establezcan.

Las comunicaciones establecidas permiten el intercambio de información, que deberá estar regulado para garantizar las condiciones de confidencialidad, integridad y disponibilidad de la información que se emite o recibe por los distintos canales.

6.7.2 Objetivo

- Garantizar el funcionamiento correcto y seguro de las instalaciones de procesamiento de la información y comunicaciones.
- Establecer responsabilidades y procedimientos para su gestión y operación, incluyendo instrucciones operativas, procedimientos para la respuesta a incidentes y separación de funciones.

6.7.3 Alcance

Todas las instalaciones de procesamiento y transmisión de información de la Institución.

6.7.4 Responsabilidad

El Oficial de Seguridad de la Información tendrá a su cargo, entre otros:
- Definir procedimientos para el control de cambios a los procesos operativos documentados, los sistemas e instalaciones de procesamiento de información, y verificar su cumplimiento, de manera que no afecten la seguridad de la información.
- Establecer criterios de aprobación para nuevos sistemas de información, actualizaciones y nuevas versiones, contemplando la realización de las pruebas necesarias antes de su aprobación definitiva. Verificar que dichos procedimientos de aprobación de software incluyan aspectos de seguridad para las aplicaciones de Gobierno Electrónico.
- Definir procedimientos para el manejo de incidentes de seguridad y para la administración de los medios de almacenamiento.
- Definir y documentar una norma clara con respecto al uso del correo electrónico.
- Controlar los mecanismos de distribución y difusión de información dentro de la Institución.
- Definir y documentar controles para la detección y prevención del acceso no autorizado, la protección contra software malicioso y para garantizar la seguridad de los datos y los servicios conectados en las redes de la Institución.
- Desarrollar procedimientos adecuados de concientización de usuarios en materia de

seguridad, controles de acceso al sistema y administración de cambios.
- Verificar el cumplimiento de las normas, procedimientos y controles establecidos.

El Responsable de la Dirección de Tecnologías tendrá a su cargo lo siguiente:
- Controlar la existencia de documentación actualizada relacionada con los procedimientos de comunicaciones y operaciones.
- Evaluar el posible impacto operativo de los cambios previstos a sistemas y equipamiento y verificar su correcta implementación, asignando responsabilidades.
- Administrar los medios técnicos necesarios para permitir la segregación de los ambientes de procesamiento.
- Monitorear las necesidades de capacidad de los sistemas en operación y proyectar las futuras demandas de capacidad, a fin de evitar potenciales amenazas a la seguridad del sistema o a los servicios del usuario.
- Controlar la realización de las copias de resguardo de información, así como la prueba periódica de su restauración.
- Asegurar el registro de las actividades realizadas por el personal operativo, para su posterior revisión.
- Desarrollar y verificar el cumplimiento de procedimientos para comunicar las fallas en el procesamiento de la información o los sistemas de comunicaciones, que permita tomar medidas correctivas.
- Implementar los controles de seguridad definidos (software malicioso y accesos no autorizados).
- Definir e implementar procedimientos para la administración de medios informáticos de almacenamiento, como cintas, discos, casetes e informes impresos y para la eliminación segura de los mismos.
- Participar en el tratamiento de los incidentes de seguridad, de acuerdo a los procedimientos establecidos.

El Oficial de Seguridad de la Información junto con el Responsable de la Dirección de Tecnologías de la Información y el Responsable del Área Legal de la Institución evaluará los contratos y acuerdos con terceros para garantizar la incorporación de consideraciones relativas a la seguridad de la información involucrada en la gestión de los productos o servicios prestados.

Cada Propietario de la Información, junto con el Oficial de Seguridad de la Información y el Responsable de la Dirección de Tecnologías de la Información, determinará los requerimientos para resguardar la información por la cual es responsable. Además, aprobará los servicios de mensajería autorizados para transportar la información cuando sea requerido, de acuerdo a su nivel de criticidad.

El servidor propuesto por el Comité de Seguridad de la Información , revisará las actividades que no hayan sido posibles segregar. Así mismo, revisará los registros de actividades del personal operativo.

6.7.5 Política Documentación de los Procedimientos Operativos

Se documentarán y mantendrán actualizados los procedimientos operativos identificados en esta Política y sus cambios serán autorizados por el Oficial de Seguridad de la Información.
Los procedimientos especificarán instrucciones para la ejecución detallada de cada tarea, incluyendo:

a) Procesamiento y manejo de la información.

b) Requerimientos de programación de procesos, interdependencias con otros sistemas, tiempos de inicio de las primeras tareas y tiempos de terminación de las últimas tareas.
c) Instrucciones para el manejo de errores u otras condiciones excepcionales que puedan surgir durante la ejecución de tareas.
e) Restricciones en el uso de utilitarios del sistema. Personas de soporte a contactar en caso de dificultades operativas o técnicas imprevistas.
f) Instrucciones especiales para el manejo de "salidas", como el uso de papelería especial o la administración de salidas confidenciales, incluyendo procedimientos para la eliminación segura de salidas fallidas de tareas.
g) Reinicio del sistema y procedimientos de recuperación en caso de producirse fallas en el sistema.

Se preparará adicionalmente documentación sobre procedimientos referidos a las siguientes actividades:

a) Instalación y mantenimiento de equipamiento para el procesamiento de información y comunicaciones.
b) Instalación y mantenimiento de las plataformas de procesamiento.
c) Monitoreo del procesamiento y las comunicaciones.
d) Inicio y finalización de la ejecución de los sistemas.
e) Programación y ejecución de procesos.
f) Gestión de servicios.
g) Resguardo de información.
h) Gestión de incidentes de seguridad en el ambiente de procesamiento y comunicaciones.
i) Reemplazo o cambio de componentes del ambiente de procesamiento y comunicaciones.
j) Uso del correo electrónico.

6.7.6 Control de Cambios en las Operaciones

Se definirán procedimientos para el control de los cambios en el ambiente operativo y de comunicaciones. Todo cambio deberá ser evaluado previamente en aspectos técnicos y de seguridad.

El Oficial de Seguridad de la Información controlará que los cambios en los componentes operativos y de comunicaciones no afecten la seguridad de los mismos ni de la información que soportan. El Responsable de la Dirección de Tecnologías de la Información evaluará el posible impacto operativo de los cambios previstos y verificará su correcta implementación.
Se retendrá un registro de auditoría que contenga toda la información relevante de cada cambio implementado.

Los procedimientos de control de cambios contemplarán los siguientes puntos:

a) Identificación y registro de cambios significativos.
b) Evaluación del posible impacto de dichos cambios.
c) Aprobación formal de los cambios propuestos.
d) Planificación del proceso de cambio.
e) Prueba del nuevo escenario.
f) Comunicación de detalles de cambios a todas las personas pertinentes.
g) Identificación de las responsabilidades por la cancelación de los cambios fallidos y la recuperación respecto de los mismos.

6.7.7 Procedimientos de manejo de Incidentes

Se establecerán funciones y procedimientos de manejo de incidentes garantizando una respuesta rápida, eficaz y sistemática a los incidentes relativos a seguridad. Se deben considerar los siguientes ítems:

a) Contemplar y definir todos los tipos probables de incidentes relativos a seguridad, incluyendo
   1. Fallas operativas.
   2. Código malicioso.
   3. Intrusiones.
   4. Fraude informático.
   5. Error humano.
   6. Catástrofes naturales.
b) Comunicar los incidentes a través de canales oficiales apropiados, tan pronto como sea posible para evitar los incidentes de seguridad de la información.
c) Contemplar los siguientes puntos en los procedimientos para los planes de contingencia normales (diseñados para recuperar sistemas y servicios tan pronto como sea posible):
   1. Definición de las primeras medidas a implementar
   2. Análisis e identificación de la causa del incidente.
   3. Planificación e implementación de soluciones para evitar la repetición del mismo, si fuera necesario.
   4. Comunicación con las personas afectadas o involucradas con la recuperación, del incidente.
   5. Notificación de la acción a la autoridad y/o Instituciones pertinentes.
d) Registrar pistas de auditoría y evidencia similar para:
   1. Análisis de problemas internos.
   2. Uso como evidencia en relación con una probable violación contractual o infracción normativa, o en marco de un proceso judicial.
   3. Negociación de compensaciones por parte de los proveedores de software y de servicios.
e) Implementar controles detallados y formalizados de las acciones de recuperación respecto de las violaciones de la seguridad y de corrección de fallas del sistema, garantizando:
   1. Acceso a los sistemas y datos existentes sólo al personal claramente identificado y autorizado.
   2. Documentación de todas las acciones de emergencia emprendidas en forma detallada.
   3. Comunicación de las acciones de emergencia al titular de la Unidad Organizativa y revisión de su cumplimiento.
   4. Constatación de la integridad de los controles y sistemas de la Institución en un plazo mínimo.

En los casos en los que se considere necesario, se solicitará la participación del Responsable del Área Legal de la Institución en el tratamiento de incidentes de seguridad ocurridos.

6.7.8 Separación de Funciones

Se separará la gestión o ejecución de ciertas tareas o áreas de responsabilidad, a fin de reducir el riesgo de modificaciones no autorizadas o mal uso de la información o los servicios por falta de independencia en la ejecución de funciones críticas.

Si este método de control no se pudiera cumplir en algún caso, se implementarán controles como:

a) Monitoreo de las actividades.
b) Registros de auditoría y control periódico de los mismos.
c) Supervisión por parte de la Unidad de Auditoría Interna o en su defecto quien sea propuesto a tal efecto, siendo independiente al área que genera las actividades auditadas.

Así mismo, se documentará la justificación formal por la cual no fue posible efectuar la segregación de funciones.

Se asegurará la independencia de las funciones de auditoría de seguridad, tomando recaudos para que ninguna persona pueda realizar actividades en áreas de responsabilidad única sin ser monitoreada, y la independencia entre el inicio de un evento y su autorización, considerando los siguientes puntos:

a) Separar actividades que requieren complicidad para defraudar, por ejemplo efectuar una orden de compra y verificar que la mercadería fue recibida.
b) Diseñar controles, si existe peligro de connivencia de manera tal que dos o más personas estén involucradas, reduciendo la posibilidad de conspiración.

6.7.9 Separación entre Instalaciones de Desarrollo e Instalaciones Operativas

Los ambientes de desarrollo, prueba y operaciones, siempre que sea posible, estarán separados preferentemente en forma física, y se definirán y documentarán las reglas para la transferencia de software desde el estado de desarrollo hacia el estado operativo.

Para ello, se tendrán en cuenta los siguientes controles:

a) Ejecutar el software de desarrollo y de operaciones, en diferentes ambientes de operaciones, equipos, o directorios.
b) Separar las actividades de desarrollo y prueba, en entornos diferentes.
c) Impedir el acceso a los compiladores, editores y otros utilitarios del sistema en el ambiente operativo, cuando no sean indispensables para el funcionamiento del mismo.
d) Utilizar sistemas de autenticación y autorización independientes para los diferentes ambientes, así como perfiles de acceso a los sistemas. Prohibir a los usuarios compartir contraseñas en estos sistemas. Las interfaces de los sistemas identificarán claramente a qué instancia se está realizando la conexión.
e) Definir propietarios de la información para cada uno de los ambientes de procesamiento existentes.
f) El personal de desarrollo no tendrá acceso al ambiente operativo. De ser extrema dicha necesidad, se establecerá un procedimiento de emergencia para la autorización, documentación y registro de dichos accesos.

Para el caso que no puedan mantener separados los distintos ambientes en forma física, deberán implementarse los controles indicados en el punto “Separación de Funciones”.

En el **ANEXO 3** se presenta un esquema modelo de segregación de ambientes de procesamiento.

6.7.10 Gestión de Instalaciones Externas

En el caso de tercerizar algún servicio, se acordarán controles con el proveedor y se incluirán en el contrato, contemplando las siguientes cuestiones específicas (Ver 6.2.2 Requerimientos de seguridad en Contratos o Acuerdos con Terceros?):

a) Identificar las aplicaciones sensibles o críticas que convenga retener en la Institución.
b) Obtener la aprobación de los propietarios de aplicaciones específicas.
c) Identificar las implicancias para la continuidad de los planes de las actividades de la Institución.
d) Especificar las normas de seguridad y el proceso de medición del cumplimiento.
e) Asignar funciones específicas y procedimientos para monitorear todas las actividades de seguridad.
f) Definir las funciones y procedimientos de comunicación y manejo de incidentes relativos a la seguridad.

Dichas consideraciones deberán ser acordadas entre el Oficial de Seguridad de la Información, el Responsable de la Dirección de Tecnologías de la Información y el Responsable del Área Legal de la Institución.

6.8 Planificación y Aprobación de Sistemas

6.8.1 Planificación de la Capacidad

El Responsable de la Dirección de Tecnologías de la Información, o el personal que éste designe, efectuará el monitoreo de las necesidades de capacidad de los sistemas en operación y proyectará las futuras demandas, a fin de garantizar un procesamiento y almacenamiento adecuados. Para ello tomará en cuenta además los nuevos requerimientos de los sistemas, así como las tendencias actuales y proyectadas en el procesamiento de la información de la Institución para el período estipulado de vida útil de cada componente. Además, informará las necesidades detectadas a las autoridades competentes para que puedan identificar y evitar potenciales cuellos de botella, que podrían plantear una amenaza a la seguridad o a la continuidad del procesamiento, y puedan planificar una adecuada acción correctiva.

6.8.2 Aprobación del Sistema

El Responsable de la Dirección de Tecnologías de la Información y el Oficial de Seguridad de la Información sugerirán criterios de aprobación para nuevos sistemas de información, actualizaciones y nuevas versiones, solicitando la realización de las pruebas necesarias antes de su aprobación definitiva. Se deben considerar los siguientes puntos:

a) Verificar el impacto en el desempeño y los requerimientos de capacidad de las computadoras.
b) Garantizar la recuperación ante errores.
c) Preparar y poner a prueba los procedimientos operativos de rutina según normas definidas.
d) Garantizar la implementación de un conjunto acordado de controles de seguridad.
e) Confeccionar disposiciones relativas a la continuidad de las actividades de la Institución.
f) Asegurar que la instalación del nuevo sistema no afectará negativamente los sistemas existentes, especialmente en los períodos pico de procesamiento.
g) Considerar el efecto que tiene el nuevo sistema en la seguridad global de la Institución.
h) Disponer la realización de entrenamiento en la operación y/o uso de nuevos sistemas.

6.9 Protección Contra Software Malicioso

6.9.1 Controles Contra Software Malicioso

El Oficial de Seguridad de la Información, definirá controles de detección y prevención para la protección contra software malicioso. El Responsable de la Dirección de Tecnologías de la Información, o el personal designado por éste, implementarán dichos controles.

El Oficial de Seguridad de la Información desarrollará procedimientos adecuados de concientización de usuarios en materia de seguridad, controles de acceso al sistema y administración de cambios.

Estos controles deberán considerar las siguientes acciones:

a) Prohibir el uso de software no autorizado por la Institución.
b) Redactar procedimientos para evitar los riesgos relacionados con la obtención de archivos y software desde o a través de redes externas, o por cualquier otro medio, señalando las medidas de protección a tomar.
c) Instalar y actualizar periódicamente software de detección y reparación de virus, examinado computadoras y medios informáticos, como medida preventiva y rutinaria.
d) Mantener los sistemas al día con las últimas actualizaciones de seguridad disponibles (probar dichas actualizaciones en un entorno de prueba previamente si es que constituyen cambios críticos a los sistemas).
e) Revisar periódicamente el contenido de software y datos de los equipos de procesamiento que sustentan procesos críticos de la Institución, investigando formalmente la presencia de archivos no aprobados o modificaciones no autorizadas.
f) Verificar antes de su uso, la presencia de virus en archivos de medios electrónicos de origen incierto, o en archivos recibidos a través de redes no confiables.
g) Redactar procedimientos para verificar toda la información relativa a software malicioso, garantizando que los boletines de alerta sean exactos e informativos.
h) Concientizar al personal acerca del problema de los falsos virus (hoax) y de cómo proceder frente a los mismos.

6.9.2 Mantenimiento Resguardo de la Información

El Oficial de Seguridad de la Información junto al Responsable de la Dirección de Tecnologías de la Información y los Propietarios de Información, determinarán los requerimientos para resguardar cada software o dato en función de su criticidad. En base a ello, se definirá y documentará un esquema de resguardo de la información.

El Responsable de la Dirección de Tecnologías de la Información dispondrá y controlará la realización de dichas copias, así como la prueba periódica de su restauración. Para esto se deberá contar con instalaciones de resguardo que garanticen la disponibilidad de toda la información y del software crítico de la Institución. Los sistemas de resguardo deberán probarse periódicamente, asegurándose que cumplen con los requerimientos de los planes de continuidad de las actividades de la institución.

Se definirán procedimientos para el resguardo de la información, que deberán considerar los siguientes puntos:

a) Definir un esquema de rótulo de las copias de resguardo, que permita contar con toda la información necesaria para identificar cada una de ellas y administrarlas debidamente.
b) Establecer un esquema de reemplazo de los medios de almacenamiento de las copias de resguardo, una vez concluida la posibilidad de ser reutilizados, de acuerdo a lo indicado por el proveedor, y asegurando la destrucción de los medios desechados.
c) Almacenar en una ubicación remota copias recientes de información de resguardo junto con registros exactos y completos de las mismas y los procedimientos documentados de restauración, a una distancia suficiente como para evitar daños provenientes de un

desastre en el sitio principal. Se deberán retener al menos tres generaciones o ciclos de información de resguardo para la información y el software esenciales para la Institución. Para la definición de información mínima a ser resguardada en el sitio remoto, se deberá tener en cuenta el nivel de clasificación otorgado a la misma, en términos de disponibilidad (Ver 6.3.6. Clasificación de la información) y requisitos legales a los que se encuentre sujeta.

d) Asignar a la información de resguardo un nivel de protección física y ambiental según las normas aplicadas en el sitio principal. Extender los mismos controles aplicados a los dispositivos en el sitio principal al sitio de resguardo.
e) Probar periódicamente los medios de resguardo.
f) Verificar y probar periódicamente los procedimientos de restauración garantizando su eficacia y cumplimiento dentro del tiempo asignado a la recuperación en los procedimientos operativos.

Los procedimientos de realización de copias de resguardo y su almacenamiento deberán respetar las disposiciones del punto 6.3. Gestión de Activos.

6.9.3 Registro de Actividades del Personal Operativo

El responsable de la Dirección de Tecnologías de la Información asegurará el registro de las actividades realizadas en los sistemas, incluyendo según corresponda:

a) Tiempos de inicio y cierre del sistema.
b) Errores del sistema y medidas correctivas tomadas.
c) Intentos de acceso a sistemas, recursos o información crítica o acciones restringidas.
d) Ejecución de operaciones críticas.
e) Cambios a información crítica.

La Unidad de Auditoría Interna o en su defecto quien sea propuesto por el Comité de Seguridad de la Información contrastará los registros de actividades del personal operativo con relación a los procedimientos operativos.

6.9.4 Registro de Fallas

El Responsable de la Dirección de Tecnologías de la Información desarrollará y verificará el cumplimiento de procedimientos para comunicar las fallas en el procesamiento de la información o los sistemas de comunicaciones, que permita tomar medidas correctivas.

Se registrarán las fallas comunicadas, debiendo existir reglas claras para el manejo de las mismas, con inclusión de:

a) Revisión de registros de fallas para garantizar que las mismas fueron resueltas satisfactoriamente.
b) Revisión de medidas correctivas para garantizar que los controles no fueron comprometidos, y que las medidas tomadas fueron autorizadas.
c) Documentación de la falla con el objeto de prevenir su repetición o facilitar su resolución en caso de reincidencia.

6.10 Administración de la Red

6.10.1 Controles de Redes

El Oficial de Seguridad de la Información definirá controles para garantizar la seguridad de los datos y los servicios conectados en las redes de la Institución, contra el acceso no autorizado, considerando la ejecución de las siguientes acciones:

a) Establecer los procedimientos para la administración del equipamiento remoto, incluyendo los equipos en las áreas usuarias, la que será llevada a cabo por el responsable establecido en el punto "6.1.2 Asignación de Responsabilidades en Materia de Seguridad de la Información".
b) Establecer controles especiales para salvaguardar la confidencialidad e integridad del procesamiento de los datos que pasan a través de redes públicas, y para proteger los sistemas conectados. Implementar controles especiales para mantener la disponibilidad de los servicios de red y computadoras conectadas.
c) Garantizar mediante actividades de supervisión, que los controles se aplican uniformemente en toda la estructura de procesamiento de información.

El Responsable de la Dirección de Tecnologías de la Información implementará dichos controles.

6.11 Administración y Seguridad de los medios de Almacenamiento

6.11.1 Administración de medios Informáticos Removibles

El Responsable de la Dirección de Tecnologías de la Información, con la asistencia del Oficial de Seguridad de la Información, implementará procedimientos para la administración de medios informáticos removibles, como cintas, discos, casetes e informes impresos. El cumplimiento de los procedimientos se hará de acuerdo al punto 6.14 Control de Accesos.

Se deberán considerar las siguientes acciones para la implementación de los procedimientos:

a) Eliminar de forma segura los contenidos, si ya no son requeridos, de cualquier medio reutilizable que ha de ser retirado o reutilizado por la Institución. (Ver 6.5.15 Desafectación o Reutilización Segura de los Equipos).
b) Requerir autorización para retirar cualquier medio de la Institución y realizar un control de todos los retiros a fin de mantener un registro de auditoría.
c) Almacenar todos los medios en un ambiente seguro y protegido, de acuerdo con las especificaciones de los fabricantes o proveedores.

Se documentarán todos los procedimientos y niveles de autorización, en concordancia con el capítulo 6.3. Gestión de Activos.

6.11.2 Eliminación de medios de Información

El Responsable de la Dirección de Tecnologías de la Información, junto con el Oficial de Seguridad de la Información definirá procedimientos para la eliminación segura de los medios de información respetando la normativa vigente.
Los procedimientos deberán considerar que los siguientes elementos requerirán almacenamiento y eliminación segura:

a) Documentos en papel.
b) Voces u otras grabaciones.
c) Papel carbónico.
d) Informes de salida.
e) Cintas de impresora de un solo uso.

f) Cintas magnéticas.
g) Discos o casetes removibles.
h) Medios de almacenamiento óptico (todos los formatos incluyendo todos los medios de distribución de software del fabricante o proveedor).
i) Listados de programas.
j) Datos de prueba.
k) Documentación del sistema.

Además, se debe considerar que podría ser más eficiente disponer que todos los medios sean recolectados y eliminados de manera segura, antes que intentar separar los ítems sensibles.

6.11.3 Procedimientos de manejo de la Información

Se definirán procedimientos para el manejo y almacenamiento de la información de acuerdo a la clasificación establecida en el capítulo 6.3. “Gestión de Activos”.

En los procedimientos se contemplarán las siguientes acciones:
a) Incluir en la protección a documentos, sistemas informáticos, redes, computación móvil, comunicaciones móviles, correo, correo de voz, comunicaciones de voz en general, multimedia, servicios e instalaciones postales, uso de máquinas de fax y cualquier otro ítem potencialmente sensible.
b) Restringir el acceso solo al personal debidamente autorizado.
c) Mantener un registro formal de los receptores autorizados de datos.
d) Garantizar que los datos de entrada son completos, que el procesamiento se lleva a cabo correctamente y que se valida las salidas.
e) Proteger los datos en espera ("colas").
f) Conservar los medios de almacenamiento en un ambiente que concuerde con las especificaciones de los fabricantes o proveedores.

6.11.4 Seguridad de la documentación del Sistema

La documentación del sistema puede contener información sensible, por lo que se considerarán los siguientes recaudos para su protección:
a) Almacenar la documentación del sistema en forma segura.
b) Restringir el acceso a la documentación del sistema al personal estrictamente necesario. Dicho acceso será autorizado por el Propietario de la Información relativa al sistema.

6.12 Intercambios de Información y Software

6.12.1 Acuerdos de Intercambio de Información y Software

Cuando se realicen acuerdos entre organizaciones para el intercambio de información y software, se especificarán el grado de sensibilidad de la información de la Institución involucrada y las consideraciones de seguridad sobre la misma. Se tendrán en cuenta los siguientes aspectos:

a) Responsabilidades gerenciales por el control y la notificación de transmisiones, envíos y recepciones.
b) Procedimientos de notificación de emisión, transmisión, envío y recepción.
c) Normas técnicas para el empaquetado y la transmisión.
d) Pautas para la identificación del prestador del servicio de correo.
e) Responsabilidades y obligaciones en caso de pérdida de datos.
f) Uso de un sistema convenido para el rotulado de información clasificada, garantizando

que el significado de los rótulos sea inmediatamente comprendido y que la información sea adecuadamente protegida.

g) Términos y condiciones de la licencia bajo la cual se suministra el software.
h) Información sobre la propiedad de la información suministrada y las condiciones de su uso.
i) Normas técnicas para la grabación y lectura de la información y del software.
j) Controles especiales que puedan requerirse para proteger ítems sensibles (claves criptográficas, etc.).

6.12.2 Seguridad de los medios en Tránsito

Los procedimientos de transporte de medios informáticos entre diferentes puntos (envíos postales y mensajería) deberán contemplar:

a) La utilización de medios de transporte o servicios de mensajería confiables. El propietario de la Información a transportar determinará qué servicio de mensajería se utilizará conforme la criticidad de la información a transmitir.
b) Suficiente embalaje para envío de medios a través de servicios postales o de mensajería, siguiendo las especificaciones de los fabricantes o proveedores.
c) La adopción de controles especiales, cuando resulte necesario, a fin de proteger la información sensible contra divulgación o modificación no autorizadas. Entre los ejemplos se incluyen:
    1. Uso de recipientes cerrados.
    2. Entrega en mano.
    3. Embalaje a prueba de apertura no autorizada (que revele cualquier intento de acceso).
    4. En casos excepcionales, división de la mercadería a enviar en más de una entrega y envío por diferentes rutas.

6.12.3 Seguridad del Gobierno Electrónico

El Oficial de Seguridad de la Información verificará que los procedimientos de aprobación de Software incluyan los siguientes aspectos para las aplicaciones de Gobierno Electrónico:

a) **Autenticación**: Nivel de confianza recíproca suficiente sobre la identidad del usuario y la Institución.
b) **Autorización**: Niveles de Autorización adecuados para establecer disposiciones, emitir o firmar documentos clave, etc... Forma de comunicarlo al otro participante de la transacción electrónica.
c) **Procesos de oferta y contratación pública**: Requerimientos de confidencialidad, integridad y prueba de envío y recepción de documentos clave y de no repudio de contratos.
d) **Trámites en línea**: Confidencialidad, integridad y no repudio de los datos suministrados con respecto a trámites y presentaciones ante el Estado y confirmación de recepción.
e) **Verificación**: Grado de verificación apropiado para constatar la información suministrada por los usuarios.
f) **Cierre de la transacción**: Forma de interacción más adecuada para evitar fraudes.
g) **Protección a la duplicación**: Asegurar que una transacción sólo se realiza una vez, a menos que se especifique lo contrario.
h) **No repudio**: Manera de evitar que una entidad que haya enviado o recibido información alegue que no la envió o recibió.
i) **Responsabilidad**: Asignación de responsabilidades ante el riesgo de eventuales presentaciones, tramitaciones o transacciones fraudulentas.

Se darán a conocer a los usuarios, los términos y condiciones aplicables.

Todas las medidas vinculadas al plan de gobierno electrónico de la institución deberán dictarse conforme lo dispuesto por el Decreto Ejecutivo No. 149 del 20 de noviembre de 2013, publicado en el Registro Oficial Suplemento No. 146 el 18 de diciembre de 2013; y el Acuerdo No. 1063 emitido por la Secretaría Nacional de la Administración Pública, que expide el Plan Nacional de Gobierno Electrónico.

6.13 Seguridad del Correo Electrónico

6.13.1 Riesgos de Seguridad

Se implementarán controles para reducir los riesgos de incidentes de seguridad en el correo electrónico, contemplando:

a) La vulnerabilidad de los mensajes al acceso o modificación no autorizados o a la negación de servicio.
b) La posible intercepción y el consecuente acceso a los mensajes en los medios de transferencia que intervienen en la distribución de los mismos.
c) Las posibles vulnerabilidades a errores, por ejemplo, consignación incorrecta de la dirección o dirección errónea, y la confiabilidad y disponibilidad general del servicio.
d) La posible recepción de código malicioso en un mensaje de correo, el cual afecte la seguridad de la terminal receptora o de la red a la que se encuentra conectada.
e) El impacto de un cambio en el medio de comunicación en los procesos de la Institución.
f) Las consideraciones legales, como la necesidad potencial de contar con prueba de origen, envío, entrega y aceptación.
g) Las implicancias de la publicación externa de listados de personal, accesibles al público.
h) El acceso de usuarios remotos a las cuentas de correo electrónico.
i) El uso inadecuado por parte del personal.

6.13.2 Política de Correo Electrónico

El Oficial de Seguridad de la Información junto con el Responsable de la Dirección de Tecnologías de la Información, definirán y documentarán normas y procedimientos claros con respecto al uso del correo electrónico, que incluya al menos los siguientes aspectos:

a) Protección contra ataques al correo electrónico, por ejemplo virus, intercepción, etc.
b) Protección de archivos adjuntos de correo electrónico.

Uso de técnicas criptográficas para proteger la confidencialidad e integridad de los mensajes electrónicos (Ver “6.1 Controles criptográficos” del Acuerdo 025-2019).

c) Retención de mensajes que, si se almacenaran, pudieran ser usados en caso de litigio.
d) Controles adicionales para examinar mensajes electrónicos que no pueden ser autenticados.
e) Aspectos operativos para garantizar el correcto funcionamiento del servicio (ej.: tamaño máximo de información transmitida y recibida, cantidad de destinatarios, tamaño máximo del buzón del usuario, etc.).
f) Definición de los alcances del uso del correo electrónico por parte del personal de la Institución.

Estos dos últimos puntos deben ser leídos a la luz de las normas vigentes que no sólo prohíben a los funcionarios y servidores públicos a hacer uso indebido o con fines particulares del patrimonio

estatal sino que también imponen la obligación de usar los bienes y recursos del estado con los fines autorizados y de manera racional, evitando su abuso, derroche o desaprovechamiento.

Entender al correo electrónico como una herramienta más de trabajo provista al servidor público o y funcionario a fin de ser utilizada conforme el uso al cual está destinada, faculta al empleador a implementar sistemas de controles destinados a velar por la protección y el buen uso de sus recursos. Esta facultad, sin embargo, deberá ejercerse salvaguardando la dignidad del trabajador y su derecho a la intimidad. Por tal motivo, la Institución debe informar claramente a sus funcionarios y servidores públicos:

a) Cuál es el uso que la institución espera que los funcionarios y servidores públicos hagan del correo electrónico provisto por la institución;
b) Bajo qué condiciones los mensajes pueden ser objeto de control y monitoreo.

6.13.3 Seguridad de los Sistemas Electrónicos de Oficina

Se controlarán los mecanismos de distribución y difusión tales como documentos, computadoras, computación móvil, comunicaciones móviles, correo, correo de voz, comunicaciones de voz en general, multimedia, servicios o instalaciones postales, equipos de fax, etc.

Al interconectar dichos medios, se considerarán las implicancias en lo que respecta a la seguridad y a las actividades propias de la Institución, incluyendo:

a) Vulnerabilidades de la información en los sistemas de oficina, por ejemplo la grabación de llamadas telefónicas o videoconferencias, la confidencialidad de las llamadas, el almacenamiento de faxes, la apertura o distribución del correo.
b) Procedimientos y controles apropiados para administrar la distribución de información, por ejemplo el uso de boletines electrónicos institucionales.
c) Exclusión de categorías de información sensible de la Institución, si el sistema no brinda un adecuado nivel de protección.
d) Limitación del acceso a la información de las actividades que desarrollan determinadas personas, por ejemplo aquellas que trabaja en proyectos sensibles.
e) La aptitud del sistema para dar soporte a las aplicaciones de la Institución, como la comunicación de órdenes o autorizaciones.
f) Categorías de personal y contratistas o terceros a los que se permite el uso del sistema y las ubicaciones desde las cuales se puede acceder al mismo.
g) Restricción de acceso a determinadas instalaciones específicas.
h) Identificación de la posición o categoría de los usuarios, por ejemplo funcionarios y servidores públicos de la Institución o contratistas, en directorios accesibles por otros usuarios.
i) Retención y resguardo de la información almacenada en el sistema.
j) Requerimientos y disposiciones relativos a sistemas de soporte de reposición de información previa.

6.13.4 Sistemas de Acceso Público

Se tomarán recaudos para la protección de la integridad de la información publicada electrónicamente, a fin de prevenir la modificación no autorizada que podría dañar la reputación de la Institución que emite la publicación. Es posible que la información de un sistema de acceso público, por ejemplo la información en un servidor Web accesible por Internet, deba cumplir con ciertas normas de la jurisdicción en la cual se localiza el sistema o en la cual tiene lugar la transacción electrónica.

Se implementará un proceso de autorización formal antes de que la información se ponga a disposición del público, estableciéndose en todos los casos los encargados de dicha aprobación.

Todos los sistemas de acceso público deberán prever que:

a) La información se obtenga, procese y proporcione de acuerdo a la normativa vigente.
b) La información que se ingresa al sistema sea procesada en forma completa, exacta y oportuna.
c) La información sensible sea protegida durante el proceso de recolección y su almacenamiento.
d) El acceso al sistema de publicación no permita el acceso accidental a las redes a las cuales se conecta el mismo.
e) Se registre al responsable de la publicación de información en sistemas de acceso público.
f) La información se publique teniendo en cuenta las normas establecidas al respecto.
g) Se garantice la validez y vigencia de la información publicada.

6.13.5 Otras formas de intercambio de Información

Se implementarán normas, procedimientos y controles para proteger el intercambio de información a través de medios de comunicaciones de voz, fax y vídeo, contemplando las siguientes acciones:

a) Concientizar al personal sobre la toma de debidas precauciones, por ejemplo no revelar información sensible como para evitar ser escuchado o interceptado, al hacer una llamada telefónica, por:
    1. Personas cercanas, en especial al utilizar teléfonos móviles.
    2. Terceros que tengan acceso a la comunicación mediante la intervención de la línea telefónica, y otras formas de escucha secretas, a través del acceso físico al aparato o a la línea telefónica, o mediante equipos de barrido de frecuencias al utilizar teléfonos móviles análogos.
    3. Terceros en el lado receptor.
b) Recordar al personal que no sostengan conversaciones confidenciales en lugares públicos u oficinas abiertas y lugares de reunión con paredes delgadas.

c) No dejar mensajes en contestadores automáticos puesto que éstos pueden ser escuchados por personas no autorizadas, almacenados en sistemas públicos o almacenados incorrectamente como resultado de un error de discado.
d) Recordar al personal los problemas ocasionados por el uso de máquinas de fax, en particular:
    1. El acceso no autorizado a sistemas incorporados de almacenamiento de mensajes con el objeto de recuperarlos.
    2. La programación deliberada o accidental de equipos para enviar mensajes a determinados números.
    3. El envío de documentos y mensajes a un número equivocado por errores de discado o por utilizar el número almacenado equivocado.

6.14 Control de Accesos

6.14.1 Generalidades

El acceso por medio de un sistema de restricciones y excepciones a la información es la base de todo sistema de seguridad informática. Para impedir el acceso no autorizado a los sistemas de información se deben implementar procedimientos formales para controlar la asignación de derechos de acceso a los sistemas de información, bases de datos y servicios de información, y

estos deben estar claramente documentados, comunicados y controlados en cuanto a su cumplimiento.

Los procedimientos comprenden todas las etapas del ciclo de vida de los accesos de los usuarios de todos los niveles, desde el registro inicial de nuevos usuarios hasta la privación final de derechos de los usuarios que ya no requieren el acceso.

La cooperación de los usuarios es esencial para la eficacia de la seguridad, por lo tanto es necesario concientizar a los mismos acerca de sus responsabilidades por el mantenimiento de controles de acceso eficaces, en particular aquellos relacionados con el uso de contraseñas y la seguridad del equipamiento.

6.14.2 Objetivo

- Impedir el acceso no autorizado a los sistemas de información, base de datos y servicios de información.
- Implementar seguridad en los accesos de usuarios por medio de técnicas de autenticación y autorización.
- Controlar la seguridad en la conexión entre la red de la Institución y otras redes públicas o privadas.
- Registrar y revisar eventos y actividades críticas llevadas a cabo por los usuarios en los sistemas.
- Concientizar a los usuarios respecto de su responsabilidad frente a la utilización de contraseñas y equipos.
- Garantizar la seguridad de la información cuando se utiliza computación móvil e instalaciones de trabajo remoto.

6.14.3 Alcance

La Política definida en este documento se aplica a todas las formas de acceso de aquellos a quienes se les haya otorgado permisos sobre los sistemas de información, bases de datos o servicios de información de la Institución, cualquiera sea la función que desempeñe.
Además se aplica al personal técnico que define, instala, administra y mantiene los permisos de acceso y las conexiones de red, y a los que administran su seguridad.

6.14.4 Responsabilidad

El Oficial de Seguridad de la Información estará a cargo de:

- Definir normas y procedimientos para: la gestión de accesos a todos los sistemas, bases de datos y servicios de información multiusuario; el monitoreo del uso de las instalaciones de procesamiento de la información; la solicitud y aprobación de accesos a Internet; el uso de computación móvil, trabajo remoto y reportes de incidentes relacionados; la respuesta a la activación de alarmas silenciosas; la revisión de registros de actividades; y el ajuste de relojes de acuerdo a un estándar preestablecido.
- Definir pautas de utilización de Internet para todos los usuarios.
- Participar en la definición de normas y procedimientos de seguridad a implementar en el ambiente informático (ej.: sistemas operativos, servicios de red, enrutadores o gateways, etc.) y validarlos periódicamente.
- Controlar la asignación de privilegios a usuarios.
- Analizar y sugerir medidas a ser implementadas para efectivizar el control de acceso a Internet de los usuarios.

- Verificar el cumplimiento de las pautas establecidas, relacionadas con control de accesos, registración de usuarios, administración de privilegios, administración de contraseñas, utilización de servicios de red, autenticación de usuarios y nodos, uso controlado de utilitarios del sistema, alarmas silenciosas, desconexión de terminales por tiempo muerto, limitación del horario de conexión, registro de eventos, protección de puertos, subdivisión de redes, control de conexiones a la red, control de ruteo de red, etc.
- Concientizar a los usuarios sobre el uso apropiado de contraseñas y de equipos de trabajo.
- Verificar el cumplimiento de los procedimientos de revisión de registros de auditoría.
- Asistir a los usuarios que corresponda en el análisis de riesgos a los que se expone la información y los componentes del ambiente informático que sirven de soporte a la misma.

Los propietarios de la Información estarán encargados de:

- Evaluar los riesgos a los cuales se expone la información con el objeto de:
  - Determinar los controles de accesos, autenticación y utilización a ser implementados en cada caso.
  - Definir los eventos y actividades de usuarios a ser registrados en los sistemas de procesamiento de su incumbencia y la periodicidad de revisión de los mismos.
  - Aprobar y solicitar la asignación de privilegios a usuarios.
  - Llevar a cabo un proceso formal y periódico de revisión de los derechos de acceso a la información.
  - Definir un cronograma de depuración de registros de auditoría en línea.

Los propietarios de la Información junto con la Unidad de Auditoría Interna o en su defecto quien sea propuesto por el Comité de Seguridad de la Información , definirán un cronograma de depuración de registros en línea en función a normas vigentes y a sus propias necesidades.

Los responsables de las Unidades, junto con el Oficial de Seguridad de la Información, autorizarán el trabajo remoto del personal a su cargo, en los casos en que se verifique que son adoptadas todas las medidas que correspondan en materia de seguridad de la información, de modo de cumplir con las normas vigentes. Además autorizarán el acceso de los usuarios a su cargo a los servicios y recursos de red y a internet.

El Responsable de la Dirección de Tecnologías de la Información cumplirá las siguientes funciones:

- Implementar procedimientos para la activación y desactivación de derechos de acceso a las redes.
- Analizar e implementar los métodos de autenticación y control de acceso definidos en los sistemas, bases de datos y servicios.
- Evaluar el costo y el impacto de la implementación de “enrutadores” o “gateways” adecuados para subdividir la red y recomendar el esquema apropiado.
- Implementar el control de puertos, de conexión a la red y de ruteo de red.
- Implementar el registro de eventos o actividades de usuarios de acuerdo a lo definido por los propietarios de la información, así como la depuración de los mismos.
- Definir e implementar los registros de eventos y actividades correspondientes a sistemas operativos y otras plataformas de procesamiento.
- Evaluar los riesgos sobre la utilización de las instalaciones de procesamiento de información, con el objeto de definir medios de monitoreo y tecnologías de identificación y autenticación de usuarios (Ej.: biometría, verificación de firma, uso de autenticadores de hardware).

- Definir e implementar la configuración que debe efectuarse para cada servicio de red, de manera de garantizar la seguridad en su operatoria.
- Analizar las medidas a ser implementadas para efectivizar el control de acceso a Internet de los usuarios.
- Otorgar acceso a los servicios y recursos de red, únicamente de acuerdo al pedido formal correspondiente.

La Unidad de Auditoría Interna o en su defecto quien sea propuesto por el Comité de Seguridad de la Información , tendrá acceso a los registros de eventos a fin de colaborar en el control y efectuar recomendaciones sobre modificaciones a los aspectos de seguridad.

El Comité de Seguridad de la Información aprobará el análisis de riesgos de la información efectuado. Además, aprobará el período definido para el mantenimiento de los registros de auditoría generados.

6.14.5 Política de Control de Accesos

En la aplicación de controles de acceso, se contemplarán los siguientes aspectos:

a) Identificar los requerimientos de seguridad de cada una de las aplicaciones.
b) Identificar toda la información relacionada con las aplicaciones.
c) Establecer criterios coherentes entre esta Política de Control de Acceso y la Política de Clasificación de Información de los diferentes sistemas y redes (Ver 6.3. Gestión de Activos).
d) Identificar la legislación aplicable y las obligaciones contractuales con respecto a la protección del acceso a datos y servicios.
e) Definir los perfiles de acceso de usuarios estándar, comunes a cada categoría de puestos de trabajo.
f) Administrar los derechos de acceso en un ambiente distribuido y de red, que reconozcan todos los tipos de conexiones disponibles.

6.14.6 Reglas de Control de Acceso

Las reglas de control de acceso especificadas, deberán:

a) Indicar expresamente si las reglas son obligatorias u optativas.
b) Establecer reglas sobre la premisa "*Todo debe estar prohibido a menos que se permita expresamente*" y no sobre la premisa inversa de "*Todo está permitido a menos que se prohíba expresamente*".
c) Controlar los cambios en los rótulos de información que son iniciados automáticamente por herramientas de procesamiento de información, de aquellos que son iniciados a discreción del usuario (Ver 6.3. Gestión de Activos).
d) Controlar los cambios en los permisos de usuario que son iniciados automáticamente por el sistema de información y aquellos que son iniciados por el administrador.
e) Controlar las reglas que requieren la aprobación del administrador o del propietario de la Información de que se trate, antes de entrar en vigencia, y aquellas que no requieren aprobación.

6.14.7 Administración de Accesos de Usuarios

Con el objetivo de impedir el acceso no autorizado a la información se implementarán procedimientos formales para controlar la asignación de derechos de acceso a los sistemas, datos y servicios de información.

6.14.8 Registro de Usuarios

El Oficial de Seguridad de la Información definirá un procedimiento formal de registro de usuarios para otorgar y revocar el acceso a todos los sistemas, bases de datos y servicios de información multiusuario, el cual debe comprender:

a) Utilizar identificadores de usuario únicos, de manera que se pueda identificar a los usuarios por sus acciones evitando la existencia de múltiples perfiles de acceso para un mismo empleado. El uso de identificadores grupales sólo debe ser permitido cuando sean convenientes para el trabajo a desarrollar debido a razones operativas.
b) Verificar que el usuario tiene autorización del propietario de la Información para el uso del sistema, base de datos o servicio de información.
c) Verificar que el nivel de acceso otorgado es adecuado para el propósito de la función del usuario y es coherente con la Política de Seguridad de la Institución, por ejemplo que no compromete la separación de tareas.
d) Entregar a los usuarios un detalle escrito de sus derechos de acceso.
e) Requerir que los usuarios firmen declaraciones señalando que comprenden y aceptan las condiciones para el acceso.
f) Garantizar que los proveedores de servicios no otorguen acceso hasta que se hayan completado los procedimientos de autorización.
g) Mantener un registro formal de todas las personas registradas para utilizar el servicio.
h) Cancelar inmediatamente los derechos de acceso de los usuarios que cambiaron sus tareas, o de aquellos a los que se les revocó la autorización, se desvincularon de la Institución o sufrieron la pérdida/robo de sus credenciales de acceso.
i) Efectuar revisiones periódicas con el objeto de:
   - cancelar identificadores y cuentas de usuario redundantes.
   - inhabilitar cuentas inactivas por más de 60 días.
   - eliminar cuentas inactivas por más de 90 días.

   En el caso de existir excepciones, deberán ser debidamente justificadas y aprobadas.
j) Garantizar que los identificadores de usuario redundantes no se asignen a otros usuarios.
k) Incluir cláusulas en los contratos de personal y de servicios que especifiquen sanciones si el personal o los agentes que prestan un servicio intentan accesos no autorizados.
l) El identificador de usuario estará compuesto por las iniciales de los nombres más el apellido paterno; en caso de, repetirse el identificador, al nuevo requerido se le agregará la inicial del apellido materno.

6.14.9 Administración de privilegios

Se limitará y controlará la asignación y uso de privilegios, debido a que el uso inadecuado de los privilegios del sistema resulta frecuentemente en el factor más importante que contribuye a la falla de los sistemas a los que se ha accedido ilegalmente.
Los sistemas multiusuario que requieren protección contra accesos no autorizados, deben prever una asignación de privilegios controlada mediante un proceso de autorización formal. Se deben tener en cuenta los siguientes pasos:

a) Identificar los privilegios asociados a cada producto del sistema, por ejemplo sistema operativo, sistema de administración de bases de datos y aplicaciones, y las categorías de personal a las cuales deben asignarse los productos.
b) Asignar los privilegios a individuos sobre la base de la necesidad de uso y evento por evento, por ejemplo el requerimiento mínimo para su rol funcional.
c) Mantener un proceso de autorización y un registro de todos los privilegios asignados. Los privilegios no deben ser otorgados hasta que se haya completado el proceso formal de autorización.
d) Establecer un período de vigencia para el mantenimiento de los privilegios (en base a la utilización que se le dará a los mismos) luego del cual los mismos serán revocados.
e) Promover el desarrollo y uso de rutinas del sistema para evitar la necesidad de otorgar privilegios a los usuarios.

Los propietarios de Información serán los encargados de aprobar la asignación de privilegios a usuarios y solicitar su implementación, lo cual será supervisado por el Oficial de Seguridad de la Información.

6.14.10 Administración de contraseñas de Usuario

La asignación de contraseñas se controlará a través de un proceso de administración formal, mediante el cual deben respetarse los siguientes pasos:

a) Requerir que los usuarios firmen una declaración por la cual se comprometen a mantener sus contraseñas personales en secreto y las contraseñas de los grupos de trabajo exclusivamente entre los miembros del grupo. Esta declaración bien puede estar incluida en el Acuerdo de Confidencialidad (Ver 6.4.6. Acuerdo de Confidencialidad)
b) Garantizar que los usuarios cambien las contraseñas iniciales que les han sido asignadas la primera vez que ingresan al sistema. Las contraseñas provisorias, que se asignan cuando los usuarios olvidan su contraseña, sólo debe suministrarse una vez identificado el usuario.
c) Generar contraseñas provisorias seguras para otorgar a los usuarios. Se debe evitar la participación de terceros o el uso de mensajes de correo electrónico sin protección (texto claro) en el mecanismo de entrega de la contraseña y los usuarios deben dar acuse de recibo cuando la reciban.
d) Almacenar las contraseñas sólo en sistemas informáticos protegidos.
e) Utilizar otras tecnologías de autenticación y autorización de usuarios, como la biométrica (por ejemplo verificación de huellas dactilares), verificación de firma, uso de autenticadores de hardware (como las tarjetas de circuito integrado), etc. El uso de esas herramientas se dispondrá cuando la evaluación de riesgos realizada por el Oficial de Seguridad de la Información conjuntamente con el Responsable del Área de Tecnologías de la Información y el Propietario de la Información lo determine necesario (o lo justifique).
f) Configurar los sistemas de tal manera que:
    - Las contraseñas tengan al menos 8 caracteres combinados entre mayúsculas, minúsculas y caracteres especiales.
    - Suspendan o bloqueen permanentemente al usuario luego de 3 intentos de entrar con una contraseña incorrecta (deberá pedir la rehabilitación ante quien corresponda).
    - Solicitar el cambio de la contraseña cada 30 días.
    - Impedir que las últimas 6 contraseñas sean reutilizadas,
    - Establecer un tiempo de vida mínimo de 3 días para las contraseñas.

6.14.11 Administración de contraseñas críticas

En los diferentes ambientes de procesamiento existen cuentas de usuarios con las cuales es posible efectuar actividades críticas como instalación de plataformas o sistemas, habilitación de servicios, actualización de software, configuración de componentes informáticos, etc. Dichas cuentas no serán de uso habitual (diario), sino que sólo serán utilizadas ante una necesidad específica de realizar alguna tarea que lo requiera y se encontrarán protegidas por contraseñas con un mayor nivel de complejidad que el habitual.

El Oficial de Seguridad de la Información definirá procedimientos para la administración de dichas contraseñas críticas que contemplen lo siguiente:

a) Se definirán las causas que justificarán el uso de contraseñas críticas así como el nivel de autorización requerido.
b) Las contraseñas seleccionadas serán seguras, y su definición será efectuada como mínimo por dos personas, de manera que ninguna de ellas conozca la contraseña completa.
c) Las contraseñas y los nombres de las cuentas críticas a las que pertenecen serán resguardadas debidamente.
d) La utilización de las contraseñas críticas será registrada, documentando las causas que determinaron su uso, así como el responsable de las actividades que se efectúen con la misma.
e) Cada contraseña crítica se renovará una vez utilizada y se definirá un período luego del cual la misma será renovada en caso de que no se la haya utilizado.
f) Se registrarán todas las actividades que se efectúen con las cuentas críticas para luego ser revisadas. Dicho registro será revisado posteriormente por el Responsable de Seguridad de la Información.

6.14.12 Revisión de derechos de Acceso de Usuarios

A fin de mantener un control eficaz del acceso a los datos y servicios de información, el propietario de la Información de que se trate, llevará a cabo un proceso formal, a fin de revisar los derechos de acceso de los usuarios. Se deberán contemplar los siguientes controles:

a) Revisar los derechos de acceso de los usuarios a intervalos de 6 meses.
b) Revisar las autorizaciones de privilegios especiales de derechos de acceso a intervalos de 3 meses.
c) Revisar las asignaciones de privilegios a intervalos de 6 meses, a fin de garantizar que no se obtengan privilegios no autorizados.

6.14.13 Responsabilidades del Usuario en uso de contraseñas

Los usuarios deben seguir buenas prácticas de seguridad en la selección y uso de contraseñas.
Las contraseñas constituyen un medio de validación y autenticación de la identidad de un usuario, y consecuentemente un medio para establecer derechos de acceso a las instalaciones o servicios de procesamiento de información.
Los usuarios deben cumplir las siguientes directivas:

a) Mantener las contraseñas en secreto.
b) Pedir el cambio de la contraseña siempre que exista un posible indicio de compromiso del sistema o de las contraseñas.
c) Seleccionar contraseñas de calidad, de acuerdo a las prescripciones informadas por el Responsable del Activo de Información de que se trate, que:
    - Sean fáciles de recordar.

- No estén basadas en algún dato que otra persona pueda adivinar u obtener fácilmente mediante información relacionada con la persona, por ejemplo nombres, números de teléfono, fecha de nacimiento, etc.
- No tengan caracteres idénticos consecutivos o grupos totalmente numéricos o totalmente alfabéticos.

d) Cambiar las contraseñas cada vez que el sistema se lo solicite y evitar reutilizar o reciclar viejas contraseñas.
e) Cambiar las contraseñas provisorias en el primer inicio de sesión ("log on").
f) Evitar incluir contraseñas en los procesos automatizados de inicio de sesión, por ejemplo, aquellas almacenadas en una tecla de función o macro.
g) Notificar de acuerdo a lo establecido, cualquier incidente de seguridad relacionado con sus contraseñas: pérdida, robo o indicio de pérdida de confidencialidad.

Si los usuarios necesitan acceder a múltiples servicios o plataformas y se requiere que mantengan múltiples contraseñas, se notificará a los mismos que pueden utilizar una única contraseña para todos los servicios que brinden un nivel adecuado de protección de las contraseñas almacenadas y en tránsito.

6.14.14 Equipos desatendidos en Áreas de Usuarios

Los usuarios deberán garantizar que los equipos desatendidos sean protegidos adecuadamente.

Los equipos instalados en áreas de usuarios, por ejemplo estaciones de trabajo o servidores de archivos, requieren una protección específica contra accesos no autorizados cuando se encuentran desatendidos.

El Oficial de Seguridad de la Información debe coordinar con la Dirección de Tecnologías de la Información y Comunicación las tareas de concientización a todos los usuarios y contratistas, acerca de los requerimientos y procedimientos de seguridad, para la protección de equipos desatendidos, así como de sus funciones en relación a la implementación de dicha protección.

Los usuarios cumplirán con las siguientes pautas:

a) Concluir las sesiones activas al finalizar las tareas, a menos que puedan protegerse mediante un mecanismo de bloqueo adecuado, por ejemplo, un protector de pantalla protegido por contraseña.
b) Proteger las PC's o terminales contra usos no autorizados mediante un bloqueo de seguridad o control equivalente, por ejemplo, contraseña de acceso cuando no se utilizan.

6.14.15 Política de acceso y utilización de los Servicios de Red

Las conexiones no seguras a los servicios de red pueden afectar a toda la Institución, por lo tanto, se controlará el acceso a los servicios de red tanto internos como externos. Esto es necesario para garantizar que los usuarios que tengan acceso a las redes y a sus servicios, no comprometan la seguridad de los mismos.

El Responsable de la Dirección de Tecnologías de la Información tendrá a cargo el otorgamiento del acceso a los servicios y recursos de red, únicamente de acuerdo al pedido formal del titular de una Unidad Organizativa que lo solicite para personal de su incumbencia.

Este control es particularmente importante para las conexiones de red a aplicaciones que procesen información clasificada o aplicaciones críticas, o a usuarios que utilicen el acceso desde

sitios de alto riesgo, por ejemplo áreas públicas o externas que están fuera de la administración y del control de seguridad de la Institución.

Para ello, se desarrollarán procedimientos para la activación y desactivación de derechos de acceso a las redes, los cuales comprenderán:

a) Identificar las redes y servicios de red a los cuales se permite el acceso.
b) Realizar normas y procedimientos de autorización para determinar las personas y las redes y servicios de red a los cuales se les otorgará el acceso.
c) Establecer controles y procedimientos de gestión para proteger el acceso a las conexiones y servicios de red.

Esta Política será coherente con la Política de Control de Accesos de la Institución (Ver 6.14.5. Política de Control de Accesos).

6.14.16 Camino forzado

Las redes están diseñadas para permitir el máximo alcance de distribución de recursos y flexibilidad en la elección de la ruta a utilizar. Estas características también pueden ofrecer oportunidades para el acceso no autorizado a las aplicaciones de la Institución, o para el uso no autorizado de servicios de información. Por esto, el camino de las comunicaciones será controlado.

Se limitarán las opciones de elección de la ruta entre la terminal de usuario y los servicios a los cuales el mismo se encuentra autorizado a acceder, mediante la implementación de controles en diferentes puntos de la misma.

A continuación se enumeran algunos ejemplos a considerar en caso de implementar estos controles a los sistemas existentes:

a) Asignar números telefónicos o líneas, en forma dedicada.
b) Establecer la conexión automática de puertos a gateways de seguridad o a sistemas de aplicación específicos.
c) Limitar las opciones de menú y submenú de cada uno de los usuarios.
d) Evitar la navegación ilimitada por la red.
e) Imponer el uso de sistemas de aplicación y/o gateways de seguridad específicos para usuarios externos de la red.
f) Controlar activamente las comunicaciones con origen y destino autorizados a través de un gateway, por ejemplo utilizando firewalls.
g) Restringir el acceso a redes, estableciendo dominios lógicos separados, por ejemplo, redes privadas virtuales para grupos de usuarios dentro o fuera de la Institución.

Los requerimientos relativos a caminos forzados se basarán en la Política de Control de Accesos de la Institución (Ver 6.14.5. Política de Control de Accesos). El Oficial de Seguridad de la Información, conjuntamente con el Propietario de la Información de que se trate, realizará una evaluación de riesgos a fin de determinar los mecanismos de control que corresponda en cada caso.

6.14.17 Autenticación de Usuarios para conexiones externas

Las conexiones externas son de gran potencial para accesos no autorizados a la información de la Institución. Por consiguiente, el acceso de usuarios remotos estará sujeto al cumplimiento de

procedimientos de autenticación. Existen diferentes métodos de autenticación, algunos de los cuales brindan un mayor nivel de protección que otros. El Oficial de Seguridad de la Información, conjuntamente con el Propietario de la Información de que se trate, realizará una evaluación de riesgos a fin de determinar el mecanismo de autenticación que corresponda en cada caso.

La autenticación de usuarios remotos puede llevarse a cabo utilizando:

a) Un método de autenticación físico (por ejemplo tokens de hardware), para lo que debe implementarse un procedimiento que incluya:
   - Asignación de la herramienta de autenticación.
   - Registro de los poseedores de autenticadores.
   - Mecanismo de rescate al momento de la desvinculación del personal al que se le otorgó.
   - Método de revocación de acceso del autenticador, en caso de compromiso de seguridad.
b) Un protocolo de autenticación (por ejemplo desafío / respuesta), para lo que debe implementarse un procedimiento que incluya:
   - Establecimiento de las reglas con el usuario.
   - Establecimiento de un ciclo de vida de las reglas para su renovación.
c) También pueden utilizarse líneas dedicadas privadas o una herramienta de verificación de la dirección del usuario de red, a fin de constatar el origen de la conexión.

Los procedimientos y controles de re-llamada, o dial-back, pueden brindar protección contra conexiones no autorizadas a las instalaciones de procesamiento de información de la Institución. Al aplicar este tipo de control, la Institución no debe utilizar servicios de red que incluyan desvío de llamadas. Si por alguna causa es preciso mantener el desvío de llamadas, no será posible aplicar el control de re-llamada. Además, es importante que el proceso de re-llamada garantice que se produzca a su término, una desconexión real del lado de la Institución.

6.14.18 Autenticación de Nodos

Una herramienta de conexión automática a una computadora remota podría brindar un medio para obtener acceso no autorizado a una aplicación de la Institución. Por consiguiente, las conexiones a sistemas informáticos remotos serán autenticadas. Esto es particularmente importante si la conexión utiliza una red que está fuera de control de la gestión de seguridad de la Institución. En el punto anterior se mencionan algunos ejemplos de autenticación y de cómo puede lograrse. La autenticación de nodos puede servir como un medio alternativo de autenticación de grupos de usuarios remotos, cuando éstos están conectados a un servicio informático seguro y compartido.

6.14.19 Protección de los Puertos (Ports) de diagnóstico remoto

Muchas computadoras y sistemas de comunicación son instalados y administrados con una herramienta de diagnóstico remoto. Si no están protegidos, estos puertos de diagnóstico proporcionan un medio de acceso no autorizado. Por consiguiente, serán protegidos por un mecanismo de seguridad apropiado, con las mismas características del punto 6.14.15 “Autenticación de Usuarios para Conexiones Externas”. También para este caso deberá tenerse en cuenta el punto 6.14.16 “Camino Forzado”.

6.14.20 Subdivisión de Redes

Para controlar la seguridad en redes extensas, se podrán dividir en dominios lógicos separados. Para esto se definirán y documentarán los perímetros de seguridad que sean convenientes. Estos perímetros se implementarán mediante la instalación de “gateways” con funcionalidades de “firewall” o redes privadas virtuales, para filtrar el tráfico entre los dominios (Ver 6.14.20 Control de

Conexión a la Red y 6.14.21 Control de Ruteo de Red) y para bloquear el acceso no autorizado de acuerdo a la Política de Control de Accesos, ver 6.14.5.

La subdivisión en dominios de la red tomará en cuenta criterios como los requerimientos de seguridad comunes de grupos de integrantes de la red, la mayor exposición de un grupo a peligros externos, separación física, u otros criterios de aglutinamiento o segregación preexistentes.

Basándose en la Política de Control de Accesos y los requerimientos de acceso el Responsable de la Dirección de Tecnologías de la Información evaluará el costo relativo y el impacto en el desempeño que ocasione la implementación de enrutadores o gateways adecuados (Ver 6.14.20. Control de Conexión a la Red y 6.14.21. Control de Ruteo de Red) para subdividir la red. Luego decidirá, junto con el Oficial de Seguridad de la Información, el esquema más apropiado a implementar.

6.14.21 Acceso a Internet

El acceso a Internet será utilizado con propósitos autorizados o con el destino por el cual fue provisto.

El Oficial de Seguridad de la Información definirá procedimientos para solicitar y aprobar accesos a Internet. Los accesos serán autorizados formalmente por el Responsable de la Unidad a cargo del personal que lo solicite. Además, se definirán las pautas de utilización de Internet para todos los usuarios.

Se evaluará la conveniencia de generar un registro de los accesos de los usuarios a Internet, con el objeto de realizar revisiones de los accesos efectuados o analizar casos particulares. Dicho control será comunicado a los usuarios de acuerdo a lo establecido en el punto 6.4.6. “Acuerdo de Confidencialidad”. Para ello, el Oficial de Seguridad de la Información junto con el Responsable de Tecnologías de la Información analizarán las medidas a ser implementadas para efectivizar dicho control, como ser la instalación de “firewalls”, “proxies”, etc.

6.14.22 Control de Conexión a la Red

Sobre la base de lo definido en el punto "Requerimientos”, se implementarán controles para limitar la capacidad de conexión de los usuarios. Dichos controles se podrán implementar en los “gateways” que separen los diferentes dominios de la red (Ver 6.14.18. Subdivisión de Redes).

Algunos ejemplos de los entornos a las que deben implementarse restricciones son:

a) Correo electrónico.
b) Transferencia de archivos.
c) Acceso interactivo.
d) Acceso a la red fuera del horario laboral.

6.14.23 Control de Ruteo de Red

En las redes compartidas, especialmente aquellas que se extienden fuera de los límites de la Institución, se incorporarán controles de ruteo, para asegurar que las conexiones informáticas y los flujos de información no violen la Política de Control de Accesos (Ver 6.14.5. Política de Control de Accesos).

Estos controles contemplarán mínimamente la verificación positiva de direcciones de origen y destino. Adicionalmente, para este objetivo pueden utilizarse diversos métodos incluyendo entre otros autenticación de protocolos de ruteo, ruteo estático, traducción de direcciones y listas de control de acceso.

6.14.24 Seguridad de los Servicios de Red

El Oficial de Seguridad de la Información junto con el Responsable de la Dirección de Tecnologías de la Información definirán las pautas para garantizar la seguridad de los servicios de red de la Institución, tanto públicos como privados.

Para ello se tendrán en cuenta las siguientes directivas:
- Mantener instalados y habilitados sólo aquellos servicios que sean utilizados.
- Controlar el acceso lógico a los servicios, tanto a su uso como a su administración.
- Configurar cada servicio de manera segura, evitando las vulnerabilidades que pudieran presentar.
- Instalar periódicamente las actualizaciones de seguridad.

Dicha configuración será revisada periódicamente por el Oficial de Seguridad de la Información.

6.14.25 Control de acceso al Sistema Operativo

El Oficial de Seguridad de la Información junto con el Responsable de la Dirección de Tecnologías de la Información realizará una evaluación de riesgos a fin de determinar el método de protección adecuado para el acceso al Sistema Operativo.

Si del análisis realizado surgiere la necesidad de proveer un método de identificación de terminales, se redactará un procedimiento que indique:
a) El método de identificación automática de terminales utilizado.
b) El detalle de transacciones permitidas por terminal.

6.14.26 Procedimientos de Conexión de Terminales

El acceso a los servicios de información sólo será posible a través de un proceso de conexión seguro. El procedimiento de conexión en un sistema informático será diseñado para minimizar la oportunidad de acceso no autorizado.

Este procedimiento, por lo tanto, debe divulgar la mínima información posible acerca del sistema, a fin de evitar proveer de asistencia innecesaria a un usuario no autorizado.

El procedimiento de identificación deberá:
a) Mantener en secreto los identificadores de sistemas o aplicaciones hasta tanto se halla llevado a cabo exitosamente el proceso de conexión.
b) Desplegar un aviso general advirtiendo que sólo los usuarios autorizados pueden acceder a la computadora.
c) Evitar dar mensajes de ayuda que pudieran asistir a un usuario no autorizado durante el procedimiento de conexión.
d) Validar la información de la conexión sólo al completarse la totalidad de los datos de entrada. Si surge una condición de error, el sistema no debe indicar que parte de los datos es correcta o incorrecta.
e) Limitar el número de intentos de conexión no exitosos permitidos y:
   - Registrar los intentos no exitosos.

- Impedir otros intentos de identificación, una vez superado el límite permitido.
- Desconectar conexiones de comunicaciones de datos.

f) Limitar el tiempo máximo permitido para el procedimiento de conexión. Si este es excedido, el sistema debe finalizar la conexión.
g) Desplegar la siguiente información, al completarse una conexión exitosa:
   - Fecha y hora de la conexión exitosa anterior.
   - Detalles de los intentos de conexión no exitosos desde la última conexión exitosa.

6.14.27 Identificación y autenticación de los Usuarios

Todos los usuarios (incluido el personal de soporte técnico, como los operadores, administradores de red, programadores de sistemas y administradores de bases de datos) tendrán un identificador único (ID de usuario) solamente para su uso personal exclusivo, de manera que las actividades puedan rastrearse con posterioridad hasta llegar al individuo responsable. Los identificadores de usuario no darán ningún indicio del nivel de privilegio otorgado.

En circunstancias excepcionales, cuando existe un claro beneficio para la Institución, podrá utilizarse un identificador compartido para un grupo de usuarios o una tarea específica. Para casos de esta índole, se documentará la justificación y aprobación del Propietario de la Información de que se trate.

Si se utilizará un método de autenticación físico (por ejemplo autenticadores de hardware), deberá implementarse un procedimiento que incluya:

a) Asignar la herramienta de autenticación.
b) Registrar los poseedores de autenticadores.
c) Rescatar el autenticador al momento de la desvinculación del personal al que se le otorgó.
d) Revocar el acceso del autenticador, en caso de compromiso de seguridad.

6.14.28 Sistema de Administración de Contraseñas

Las contraseñas constituyen uno de los principales medios de validación de la autoridad de un usuario para acceder a un servicio informático. Los sistemas de administración de contraseñas deben constituir una herramienta eficaz e interactiva que garantice contraseñas de calidad.

El sistema de administración de contraseñas debe:

a) Imponer el uso de contraseñas individuales para determinar responsabilidades.
b) Permitir que los usuarios seleccionen y cambien sus propias contraseñas (luego de cumplido el plazo mínimo de mantenimiento de las mismas) e incluir un procedimiento de confirmación para contemplar los errores de ingreso.
c) Imponer una selección de contraseñas de calidad según lo señalado en el punto “Uso de Contraseñas”.
d) Imponer cambios en las contraseñas en aquellos casos en que los usuarios mantengan sus propias contraseñas, según lo señalado en el punto 6.14.9 Administración de Contraseñas de Usuario
e) Obligar a los usuarios a cambiar las contraseñas provisorias en su primer procedimiento de identificación, en los casos en que ellos seleccionen sus contraseñas.
f) Mantener un registro de las últimas contraseñas utilizadas por el usuario, y evitar la reutilización de las mismas.
g) Evitar mostrar las contraseñas en pantalla, cuando son ingresadas.
h) Almacenar en forma separada los archivos de contraseñas y los datos de sistemas de aplicación.

i) Almacenar las contraseñas en forma cifrada utilizando un algoritmo de cifrado unidireccional.
j) Modificar todas las contraseñas predeterminadas por el vendedor, una vez instalado el software y el hardware (por ejemplo claves de impresoras, hubs, routers, etc.).
k) Garantizar que el medio utilizado para acceder/utilizar el sistema de contraseñas, asegure que no se tenga acceso a información temporal o en tránsito de forma no protegida.

6.14.29 Uso de Utilitarios de Sistema

La mayoría de las instituciones tienen uno o más programas utilitarios que podrían tener la capacidad de pasar por alto los controles de sistemas y aplicaciones. Es esencial que su uso sea limitado y minuciosamente controlado. Se deben considerar los siguientes controles:

a) Utilizar procedimientos de autenticación para utilitarios del sistema.
b) Separar entre utilitarios del sistema y software de aplicaciones.
c) Limitar el uso de utilitarios del sistema a la cantidad mínima viable de usuarios fiables y autorizados.
d) Evitar que personas ajenas a la Institución tomen conocimiento de la existencia y modo de uso de los utilitarios instalados en las instalaciones informáticas.
e) Establecer autorizaciones para uso ad hoc de utilitarios de sistema.
f) Limitar la disponibilidad de utilitarios de sistema, por ejemplo durante el transcurso de un cambio autorizado.
g) Registrar todo uso de utilitarios del sistema.
h) Definir y documentar los niveles de autorización para utilitarios del sistema.
i) Remover todo el software basado en utilitarios y software de sistema innecesarios.

6.14.30 Alarmas silenciosas para la Protección de los Usuarios

Se considerará la provisión de alarmas silenciosas para los usuarios que podrían ser objetos de coerción. La decisión de suministrar una alarma de esta índole se basará en una evaluación de riesgos que realizará el Oficial de Seguridad de la Información junto con el Responsable de la Dirección de Tecnologías de la Información. En este caso, se definirán y asignarán funciones y procedimientos para responder a la utilización de una alarma silenciosa.

6.14.31 Desconexión de Terminales por tiempo muerto

El Oficial de Seguridad de la Información, junto con los Propietarios de la Información de que se trate definirán cuáles se consideran terminales de alto riesgo, por ejemplo áreas públicas o externas fuera del alcance de la gestión de seguridad de la Institución, o que sirven a sistemas de alto riesgo. Las mismas se apagarán después de un periodo definido de inactividad, tiempo muerto, para evitar el acceso de personas no autorizadas. Esta herramienta de desconexión por tiempo muerto deberá limpiar la pantalla de la terminal y deberá cerrar tanto la sesión de la aplicación como la de red. El lapso por tiempo muerto responderá a los riesgos de seguridad del área y de la información que maneje la terminal.

Para las PC’s, se implementará la desconexión por tiempo muerto, que limpie la pantalla y evite el acceso no autorizado, pero que no cierra las sesiones de aplicación o de red.

Por otro lado, si un funcionario debe abandonar su puesto de trabajo momentáneamente, activará protectores de pantalla con contraseñas, a los efectos de evitar que terceros puedan ver su trabajo o continuar con la sesión de usuario habilitada.

6.14.32 Limitación del Horario de Conexión

Las restricciones al horario de conexión deben suministrar seguridad adicional a las aplicaciones de alto riesgo. La limitación del periodo durante el cual se permiten las conexiones de terminales a los servicios informáticos reduce el espectro de oportunidades para el acceso no autorizado. Se implementará un control de esta índole para aplicaciones informáticas sensibles, especialmente aquellas terminales instaladas en ubicaciones de alto riesgo, por ejemplo áreas públicas o externas que estén fuera del alcance de la gestión de seguridad de la Institución.

Entre los controles que se deben aplicar, se enuncian:

a) Utilizar lapsos predeterminados, por ejemplo para transmisiones de archivos en lote, o sesiones interactivas periódicas de corta duración.
b) Limitar los tiempos de conexión al horario normal de oficina, de no existir un requerimiento operativo de horas extras o extensión horaria.
c) Documentar debidamente los agentes que no tienen restricciones horarias y las razones de su autorización. También cuando el Propietario de la Información autorice excepciones para una extensión horaria ocasional.

6.14.33 Restricción del acceso a la Información

Los usuarios de sistemas de aplicación, con inclusión del personal de soporte, tendrán acceso a la información y a las funciones de los sistemas de aplicación de conformidad con la Política de Control de Acceso definida, sobre la base de los requerimientos de cada aplicación, y conforme a la Política de la Institución para el acceso a la información.

Se aplicarán los siguientes controles, para brindar apoyo a los requerimientos de limitación de accesos:

a) Proveer una interfaz para controlar el acceso a las funciones de los sistemas de aplicación. El Propietario de la Información involucrada será responsable de la adjudicación de accesos a las funciones. En el caso de que las actividades involucradas en el otorgamiento de acceso revistan un carácter técnico elevado, las mismas serán llevadas a cabo por personal del área de sistemas, conforme a una autorización formal emitida por el Propietario de la Información.
b) Restringir el conocimiento de los usuarios acerca de la información o de las funciones de los sistemas de aplicación a las cuales no sean autorizados a acceder, con la adecuada edición de la documentación de usuario.
c) Controlar los derechos de acceso de los usuarios, por ejemplo, lectura, escritura, supresión y ejecución.
d) Garantizar que las salidas de los sistemas de aplicación que administran información sensible, contengan sólo la información que resulte pertinente para el uso de la salida, y que la misma se envíe solamente a las terminales y ubicaciones autorizadas.
e) Revisar periódicamente dichas salidas a fin de garantizar la remoción de la información redundante.
f) Restringir el acceso a la información por fuera del sistema encargado de su procesamiento, es decir, la modificación directa del dato almacenado.

6.14.34 Aislamiento de los Sistemas Sensibles

Los sistemas sensibles podrían requerir de un ambiente informático dedicado (aislado). Algunos sistemas de aplicación son suficientemente sensibles a pérdidas potenciales y requieren un tratamiento especial. La sensibilidad puede señalar que el sistema de aplicación debe ejecutarse

en una computadora dedicada, que sólo debe compartir recursos con los sistemas de aplicación confiables, o no tener limitaciones. Son aplicables las siguientes consideraciones:

a) Identificar y documentar claramente la sensibilidad de un sistema de aplicación. Esta tarea será llevada a cabo por el administrador de la aplicación (Ver 6.3. Gestión de Activos).
b) Identificar y acordar con el administrador de la aplicación sensible cuando la aplicación ha de ejecutarse en un ambiente compartido, los sistemas de aplicación con los cuales ésta compartirá los recursos.
c) Coordinar con el Responsable de la Dirección de Tecnologías de la Información, qué servicios estarán disponibles en el entorno donde se ejecutará la aplicación, de acuerdo a los requerimientos de operación y seguridad especificados por el administrador de la aplicación.
d) Considerar la seguridad en la administración de las copias de respaldo de la información que procesan las aplicaciones.
e) Considerar las mismas precauciones de seguridad y privacidad, en la elaboración del plan de continuidad y/o contingencia de la ejecución de la aplicación. Ejemplo: el equipamiento alternativo o las instalaciones de emergencia donde restablecer la aplicación.

6.15 Monitoreo del Acceso y Uso de los Sistemas

6.15.1 Registro de Eventos

Se generarán registros de auditoría que contengan excepciones y otros eventos relativos a la seguridad.
Los registros de auditoría deberán incluir:

a) Identificación del usuario.
b) Fecha y hora de inicio y terminación.
c) Identidad o ubicación de la terminal, si se hubiera dispuesto identificación automática para la misma (Ver 6.14.26. Procedimiento de Conexión de Terminales).
d) Registros de intentos exitosos y fallidos de acceso al sistema.
e) Registros de intentos exitosos y fallidos de acceso a datos y otros recursos.

En todos los casos, los registros de auditoría serán archivados preferentemente en un equipo diferente al que los genere y conforme los requerimientos de la Política de Retención de Registros.

Los propietarios de la Información junto con la Unidad de Auditoría Interna o en su defecto quien sea propuesto por el Comité de Seguridad de la Información, definirán un cronograma de depuración de registros en línea en función a normas vigentes y a sus propias necesidades.

6.15.2 Procedimientos y Áreas de Riesgo

Se desarrollarán procedimientos para monitorear el uso de las instalaciones de procesamiento de la información, a fin de garantizar que los usuarios sólo estén desempeñando actividades que hayan sido autorizadas explícitamente.

Todos los funcionarios y servidores públicos deben conocer el alcance preciso del uso adecuado de los recursos informáticos, y se les advertirá que determinadas actividades pueden ser objeto de control y monitoreo (Ver 6.4.6. Acuerdo de Confidencialidad).

El alcance de estos procedimientos deberá corresponderse a la evaluación de riesgos que realice el Responsable de la Dirección de Tecnologías de la Información y el Oficial de Seguridad de la Información (Ver 6.17.10 Control del Software Operativo).

Entre las áreas que deben tenerse en cuenta se enumeran las siguientes:

a) Acceso no autorizado, incluyendo detalles como:
   - Identificación del usuario.
   - Fecha y hora de eventos clave.
   - Tipos de eventos.
   - Archivos a los que se accede.
   - Utilitarios y programas utilizados.

b) Todas las operaciones con privilegio, como:
   - Utilización de cuenta de supervisor.
   - Inicio y cierre del sistema.
   - Conexión y desconexión de dispositivos de Ingreso y Salida de información o que permitan copiar datos.
   - Cambio de fecha/hora.
   - Cambios en la configuración de la seguridad.
   - Alta de servicios.

c) Intentos de acceso no autorizado, como:
   - Intentos fallidos.
   - Violaciones de la Política de Accesos y notificaciones para “gateways” de red y “firewalls”.
   - Alertas de sistemas de detección de intrusiones.

d) Alertas o fallas de sistema como:
   - Alertas o mensajes de consola.
   - Excepciones del sistema de registro.
   - Alarmas del sistema de administración de redes.
   - Accesos remotos a los sistemas.

6.15.3 Factores de Riesgo

Entre los factores de riesgo que se deben considerar, se encuentran:

a) La criticidad de los procesos de aplicaciones.
b) El valor, la sensibilidad o criticidad de la información involucrada.
c) La experiencia acumulada en materia de infiltración y uso inadecuado del sistema.
d) El alcance de la interconexión del sistema (en particular las redes públicas).

Los propietarios de la Información manifestarán la necesidad de registrar aquellos eventos que consideren críticos para la operatoria que se encuentra bajo su responsabilidad.

6.15.4 Registro y revisión de Eventos

Se implementará un procedimiento de registro y revisión de los registros de auditoría, orientado a producir un informe de las amenazas detectadas contra los sistemas y los métodos utilizados. La periodicidad de dichas revisiones será definida por los propietarios de la Información y el Oficial de Seguridad de la Información, de acuerdo a la evaluación de riesgos efectuada.

Si el volumen de la información contenida en alguno de los registros fuera muy grande, el procedimiento indicará cuales de los registros más significativos se copiarán automáticamente en registros auxiliares.
Por otra parte, el Responsable de la Dirección de Tecnologías de la Información, podrá disponer la utilización de herramientas de auditoría o utilitarios adecuados para llevar a cabo el control de los registros.

En la asignación de funciones en materia de seguridad de la información (Ver 5. Organización de la Seguridad de la Información), se deberá separar las funciones entre quienes realizan la revisión y aquellos cuyas actividades están siendo monitoreadas.

Las herramientas de registro deberán contar con los controles de acceso necesarios, a fin de garantizar que no ocurra:

a) La desactivación de la herramienta de registro.
b) La alteración de mensajes registrados.
c) La edición o supresión de archivos de registro.
d) La saturación de un medio de soporte de archivos de registro.
e) La falla en los registros de los eventos.
f) La sobre escritura de los registros.

La Unidad de Auditoría Interna o en su defecto quien sea propuesto por el Comité de Seguridad de la Información, tendrá acceso a los registros de eventos a fin de colaborar en el control y efectuar recomendaciones sobre modificaciones a los aspectos de seguridad. Adicionalmente podrían evaluar las herramientas de registro, pero no tendrán libre acceso a ellas.

6.15.5 Sincronización de Relojes

A fin de garantizar la exactitud de los registros de auditoría, al menos los equipos que realicen estos registros, deberán tener una correcta configuración de sus relojes.

Para ello, se dispondrá de un procedimiento de ajuste de relojes, el cual indicará también la verificación de los relojes contra una fuente externa del dato y la modalidad de corrección ante cualquier variación significativa.

6.16 Computación Móvil y Trabajo Remoto

6.16.1. Computación Móvil

Cuando se utilizan dispositivos informáticos móviles se debe tener especial cuidado en garantizar que no se comprometa la información de la Institución.

Se deberá tener en cuenta en este sentido, cualquier dispositivo móvil y/o removible, incluyendo: Notebooks, Laptop o tablets, Teléfonos Celulares y sus tarjetas de memoria, dispositivos de Almacenamiento removibles, tales como CDs, DVDs, y cualquier dispositivo de almacenamiento de conexión USB, tarjetas de identificación personal (control de acceso), dispositivos criptográficos, cámaras digitales, etc.

Esta lista no es específica, ya que deberán incluirse todos los dispositivos que pudieran contener información confidencial de la Institución y por lo tanto, ser susceptibles de sufrir un incidente en el que se comprometa la seguridad del mismo.

Se desarrollarán procedimientos adecuados para estos dispositivos, que abarquen los siguientes conceptos:

a) La protección física necesaria
b) El acceso seguro a los dispositivos
c) La utilización de los dispositivos en lugares públicos.
d) El acceso a los sistemas de información y servicios de la Institución a través de dichos dispositivos.
e) Las técnicas criptográficas a utilizar para la transmisión de información clasificada.

f) Los mecanismos de resguardo de la información contenida en los dispositivos.
g) La protección contra software malicioso.

La utilización de dispositivos móviles incrementa la probabilidad de ocurrencia de incidentes del tipo de pérdida, robo o hurto. En consecuencia deberá entrenarse especialmente al personal que los utilice. Se desarrollarán normas y procedimientos sobre los cuidados especiales a observar ante la posesión de dispositivos móviles, que contemplarán las siguientes recomendaciones:

a) Permanecer siempre cerca del dispositivo.
b) No dejar desatendidos los equipos.
c) No llamar la atención acerca de portar un equipo valioso.
d) No poner identificaciones de la Institución en el dispositivo, salvo los estrictamente necesarios.
e) No poner datos de contacto técnico en el dispositivo.
f) Mantener cifrada la información clasificada.

Por otra parte, se confeccionarán procedimientos que permitan al propietario del dispositivo reportar rápidamente cualquier incidente sufrido y mitigar los riesgos a los que eventualmente estuvieran expuestos los sistemas de información de la Institución, los que incluirán:

a) Revocación de las credenciales afectadas.
b) Notificación a grupos de Trabajo donde potencialmente se pudieran haber comprometido recursos.

6.16.2 Trabajo Remoto

El trabajo remoto utiliza tecnología de comunicaciones para permitir que el personal trabaje en forma remota desde un lugar externo a la Institución.

El trabajo remoto sólo será autorizado por el Responsable de la Unidad, o superior jerárquico correspondiente, a la cual pertenezca el usuario solicitante, conjuntamente con el Oficial de Seguridad de la Información, cuando se verifique que son adoptadas todas las medidas que correspondan en materia de seguridad de la información, de modo de cumplir con la política, normas y procedimientos existentes.
Estos casos serán de excepción y serán contemplados en situaciones que justifiquen la imposibilidad de otra forma de acceso y la urgencia, tales como horarios de la Institución, solicitud de las autoridades, etc.

Para ello, se establecerán normas y procedimientos para el trabajo remoto, que consideren los siguientes aspectos:

a) La seguridad física existente en el sitio de trabajo remoto, tomando en cuenta la seguridad física del edificio y del ambiente local.
b) El ambiente de trabajo remoto propuesto.
c) Los requerimientos de seguridad de comunicaciones, tomando en cuenta la necesidad de acceso remoto a los sistemas internos de la Institución, la sensibilidad de la información a la que se accederá y que pasará a través del vínculo de comunicación y la sensibilidad del sistema interno.
d) La amenaza de acceso no autorizado a información o recursos por parte de otras personas que utilizan el lugar, por ejemplo, familia y amigos.
e) Evitar la instalación / desinstalación de software no autorizada por la Institución.

Los controles y disposiciones comprenden:

a) Proveer de mobiliario para almacenamiento y equipamiento adecuado para las actividades de trabajo remoto.

b) Definir el trabajo permitido, el horario de trabajo, la clasificación de la información que se puede almacenar en el equipo remoto desde el cual se accede a la red de la Institución y los sistemas internos y servicio a los cuales el trabajador remoto está autorizado a acceder.
c) Proveer de un adecuado equipo de comunicación, con inclusión de métodos para asegurar el acceso remoto.
d) Incluir seguridad física.
e) Definir reglas y orientación respecto del acceso de terceros al equipamiento e información.
f) Proveer el hardware y el soporte y mantenimiento del software.
g) Definir los procedimientos de backup y de continuidad de las operaciones.
h) Efectuar auditoría y monitoreo de la seguridad.
i) Realizar la anulación de las autorizaciones, derechos de acceso y devolución del equipo cuando finalicen las actividades remotas.
j) Asegurar el reintegro del equipamiento en las mismas condiciones en que fue entregado, en el caso en que cese la necesidad de trabajar en forma remota.

Se implementarán procesos de auditoría específicos para los casos de accesos remotos, que serán revisados regularmente. Se llevará un registro de incidentes a fin de corregir eventuales fallas en la seguridad de este tipo de accesos.

6.17 Adquisición, Desarrollo y mantenimiento de Sistemas

6.17.1 Generalidades

La adquisición, el desarrollo y mantenimiento de las aplicaciones es un punto crítico de la seguridad.
Durante el análisis y diseño de los procesos que soportan estas aplicaciones se deben identificar, documentar y aprobar los requerimientos de seguridad a incorporar durante las etapas de desarrollo e implementación. Adicionalmente, se deberán diseñar controles de validación de datos de entrada, procesamiento interno y salida de datos.

Dado que los analistas y programadores tienen el conocimiento total de la lógica de los procesos en los sistemas, se deben implementar controles que eviten maniobras dolosas por parte de estas personas u otras que puedan operar sobre los sistemas, bases de datos y plataformas de software de base (por ejemplo, operadores que puedan manipular los datos y/o atacantes que puedan comprometer / alterar la integridad de las bases de datos) y en el caso de que se lleven a cabo, identificar rápidamente al responsable.

Además, es necesaria una adecuada administración de la estructura de base, Sistemas Operativos y Software de Base, en las distintas plataformas, para asegurar una correcta implementación de la seguridad, ya que en general los aplicativos se asientan sobre este tipo de software.

6.17.2 Objetivo

- Asegurar la inclusión de controles de seguridad y validación de datos en el desarrollo de los sistemas de información.
- Definir y documentar las normas y procedimientos que se aplicarán durante el ciclo de vida de los aplicativos y en la estructura de base en la cual se apoyan.
- Definir los métodos de protección de la información crítica o sensible.

6.17.3 Alcance

Esta Política se aplica a todos los sistemas informáticos, tanto desarrollos propios o de terceros, y a todos los Sistemas Operativos y/o Software de Base que integren cualquiera de los ambientes administrados por la Institución en donde residan los desarrollos mencionados.

6.17.4 Responsabilidad

El Oficial de Seguridad de la Información junto con el Propietario de la Información y la Unidad de Auditoría Interna, definirán los controles a ser implementados en los sistemas desarrollados internamente o por terceros, en función de una evaluación previa de riesgos.
El Oficial de Seguridad de la Información, junto con el Propietario de la Información, definirá en función a la criticidad de la información, los requerimientos de protección mediante métodos criptográficos. Luego, el Oficial de Seguridad de la Información definirá junto con el Responsable de la Dirección de Tecnologías de la Información, los métodos de encriptación a ser utilizados.

Además, el Oficial de Seguridad de la Información cumplirá las siguientes funciones:
- Definir los procedimientos de administración de claves.
- Verificar el cumplimiento de los controles establecidos para el desarrollo y mantenimiento de sistemas.
- Garantizar el cumplimiento de los requerimientos de seguridad para el software.
- Definir procedimientos para: el control de cambios a los sistemas; la verificación de la seguridad de las plataformas y bases de datos que soportan e interactúan con los sistemas; el control de código malicioso; y la definición de las funciones del personal involucrado en el proceso de entrada de datos.

El Responsable de la Dirección de Tecnologías de la Información, propondrá para su aprobación por parte del superior jerárquico que corresponda, la asignación de funciones de “implementador” y “administrador de programas fuentes” al personal de su área que considere adecuado, cuyas responsabilidades se detallan en el presente capítulo. Además, verificará el cumplimiento de las definiciones establecidas sobre los controles y las medidas de seguridad a ser incorporadas a los sistemas.

La Dirección de Tecnologías de la Información propondrá quiénes realizarán la administración de las técnicas criptográficas y claves.

El Responsable del Área de Administración incorporará aspectos relacionados con el licenciamiento, la calidad del software y la seguridad de la información en los contratos con terceros por el desarrollo de software. El Responsable del Área Legal participará en dicha tarea.

6.17.5 Política, análisis y especificaciones de los requerimientos de Seguridad

Esta Política se implementa para incorporar seguridad a los sistemas de información (propios o de terceros) y a las mejoras o actualizaciones que se les incorporen.
Los requerimientos para nuevos sistemas o mejoras a los existentes especificarán la necesidad de controles. Estas especificaciones deben considerar los controles automáticos a incorporar al sistema, como así también controles manuales de apoyo.

Se deben tener en cuenta las siguientes consideraciones:
- Definir un procedimiento para que durante las etapas de análisis y diseño del sistema, se incorporen a los requerimientos, los correspondientes controles de seguridad. Este

procedimiento debe incluir una etapa de evaluación de riesgos previa al diseño, para definir los requerimientos de seguridad e identificar los controles apropiados. En esta tarea deben participar las áreas usuarias, de sistemas, de seguridad informática y auditoría, especificando y aprobando los controles automáticos a incorporar al sistema y las necesidades de controles manuales complementarios. Las áreas involucradas podrán solicitar certificaciones y evaluaciones independientes para los productos a utilizar.

- Evaluar los requerimientos de seguridad y los controles requeridos, teniendo en cuenta que éstos deben ser proporcionales en costo y esfuerzo al valor del bien que se quiere proteger y al daño potencial que pudiera ocasionar a las actividades realizadas.

Considerar que los controles introducidos en la etapa de diseño, son significativamente menos costosos de implementar y mantener que aquellos incluidos durante o después de la implementación.

6.17.6 Seguridad en los Sistemas de Aplicación

Para evitar la pérdida, modificación o uso inadecuado de los datos pertenecientes a los sistemas de información, se establecerán controles y registros de auditoría, verificando:

- La validación de datos de entrada.
- El procesamiento interno.
- La autenticación de mensajes (interfaces entre sistemas)
- La validación de datos de salida.

6.17.7 Validación de Datos de Entrada

Se definirá un procedimiento que durante la etapa de diseño, especifique controles que aseguren la validez de los datos ingresados, tan cerca del punto de origen como sea posible, controlando también datos permanentes y tablas de parámetros.

Este procedimiento considerará los siguientes controles:

- Control de secuencia.
- Control de monto límite por operación y tipo de usuario.
- Control del rango de valores posibles y de su validez, de acuerdo a criterios predeterminados.
- Control de paridad.
- Control contra valores cargados en las tablas de datos.
- Controles por oposición, de forma tal que quien ingrese un dato no pueda autorizarlo y viceversa.

Por otra parte, se llevarán a cabo las siguientes acciones:

- Se definirá un procedimiento para realizar revisiones periódicas de contenidos de campos claves o archivos de datos, definiendo quién lo realizará, en qué forma, con qué método, quiénes deberán ser informados del resultado, etc.
- Se definirá un procedimiento que explicite las alternativas a seguir para responder a errores de validación en un aplicativo.
- Se definirá un procedimiento que permita determinar las responsabilidades de todo el personal involucrado en el proceso de entrada de datos.

6.17.8 Controles de procesamiento Interno

Se definirá un procedimiento para que durante la etapa de diseño, se incorporen controles de validación a fin de eliminar o minimizar los riesgos de fallas de procesamiento y/o vicios por procesos de errores.

Para ello se implementarán:

- Procedimientos que permitan identificar el uso y localización en los aplicativos, de funciones de incorporación y eliminación que realizan cambios en los datos.
- Procedimientos que establezcan los controles y verificaciones necesarios para prevenir la ejecución de programas fuera de secuencia o cuando falle el procesamiento previo.
- Procedimientos que establezcan la revisión periódica de los registros de auditoría de forma de detectar cualquier anomalía en la ejecución de las transacciones.
- Procedimientos que realicen la validación de los datos generados por el sistema.
- Procedimientos que verifiquen la integridad de los datos y del software cargado o descargado entre computadoras.
- Procedimientos que controlen la integridad de registros y archivos.
- Procedimientos que verifiquen la ejecución de los aplicativos en el momento adecuado.
- Procedimientos que aseguren el orden correcto de ejecución de los aplicativos, la finalización programada en caso de falla, y la detención de las actividades de procesamiento hasta que el problema sea resuelto.

6.17.9 Seguridad de los Archivos del Sistema

Se garantizará que los desarrollos y actividades de soporte a los sistemas se lleven a cabo de manera segura, controlando el acceso a los archivos del mismo.

6.17.10 Control del Software Operativo

Se definen los siguientes controles a realizar durante la implementación del software en producción, a fin de minimizar el riesgo de alteración de los sistemas:

- Toda aplicación, desarrollada por la Institución o por un tercero tendrá un único Responsable designado formalmente por el Responsable de la Dirección de Tecnologías de la Información.
- Ningún programador o analista de desarrollo y mantenimiento de aplicaciones podrán acceder a los ambientes de producción.
- El Responsable de la Dirección de Tecnologías de la Información, propondrá para su aprobación por parte del superior jerárquico que corresponda, la asignación de la función de "implementador" al personal de su área que considere adecuado, quien tendrá como funciones principales:
    - Coordinar la implementación de modificaciones o nuevos programas en el ambiente de Producción.
    - Asegurar que los sistemas aplicativos en uso, en el ambiente de Producción, sean los autorizados y aprobados de acuerdo a las normas y procedimientos vigentes.
    - Instalar las modificaciones, controlando previamente la recepción de la prueba aprobada por parte del Analista Responsable, del sector encargado del testeo y del usuario final.
    - Rechazar la implementación en caso de encontrar defectos y/o si faltara la documentación estándar establecida.

Otros controles a realizar son:

- Guardar sólo los ejecutables en el ambiente de producción.
- Llevar un registro de auditoría de las actualizaciones realizadas.

- Retener las versiones previas del sistema, como medida de contingencia.
- Definir un procedimiento que establezca los pasos a seguir para implementar las autorizaciones y conformes pertinentes, las pruebas previas a realizarse, etc.
- Denegar permisos de modificación al implementador sobre los programas fuentes bajo su custodia.
- Evitar, que la función de implementador sea ejercida por personal que pertenezca al sector de desarrollo o mantenimiento.

6.17.11 Protección de los datos de prueba del Sistema

Las pruebas de los sistemas se efectuarán sobre datos extraídos del ambiente operativo. Para proteger los datos de prueba se establecerán normas y procedimientos que contemplen lo siguiente:

- Prohibir el uso de bases de datos operativas. En caso contrario se deben despersonalizar los datos antes de su uso. Aplicar idénticos procedimientos de control de acceso que en la base de producción.
- Solicitar autorización formal para realizar una copia de la base operativa como base de prueba, llevando registro de tal autorización.
- Eliminar inmediatamente, una vez completadas las pruebas, la información operativa utilizada.

6.17.12 Control de cambios a datos operativos

La modificación, actualización o eliminación de los datos operativos serán realizadas a través de los sistemas que procesan dichos datos y de acuerdo al esquema de control de accesos implementado en los mismos (Ver 6.14.7 Administración de Accesos de Usuarios). Una modificación por fuera de los sistemas a un dato, almacenado ya sea en un archivo o base de datos, podría poner en riesgo la integridad de la información.

Los casos en los que no fuera posible la aplicación de la precedente política, se considerarán como excepciones. El Oficial de Seguridad de la Información definirá procedimientos para la gestión de dichas excepciones que contemplarán lo siguiente:

- Se generará una solicitud formal para la realización de la modificación, actualización o eliminación del dato.
- El Propietario de la Información afectada y del Oficial de Seguridad de la Información aprobarán la ejecución del cambio evaluando las razones por las cuales se solicita.
- Se generarán cuentas de usuario de emergencia para ser utilizadas en la ejecución de excepciones. Las mismas serán protegidas mediante contraseñas, sujetas al procedimiento de administración de contraseñas críticas (Ver 6.14.11 Administración de Contraseñas Críticas) y habilitadas sólo ante un requerimiento de emergencia y por el lapso que ésta dure.
- Se designará un encargado de implementar los cambios, el cual no será personal del área de Desarrollo. En el caso de que esta función no pueda ser segregada, se aplicarán controles adicionales de acuerdo a lo establecido en 6.7.8. Separación de Funciones.
- Se registrarán todas las actividades realizadas con las cuentas de emergencia. Dicho registro será revisado posteriormente por el Oficial de Seguridad de la Información.

6.17.13 Control de acceso a las bibliotecas de programas fuentes

Para reducir la probabilidad de alteración de programas fuentes, el Responsable de la Dirección de Tecnologías de la Información, propondrá para su aprobación por parte del superior jerárquico que corresponda la función de “administrador de programas fuentes” al personal de su área que

considere adecuado, quien tendrá en custodia los programas fuentes y deberá aplicarán los siguientes controles:

- Proveer al Área de Desarrollo los programas fuentes solicitados para su modificación, manteniendo en todo momento la correlación programa fuente / ejecutable.
- Llevar un registro actualizado de todos los programas fuentes en uso, indicando nombre del programa, programador, Analista Responsable que autorizó, versión, fecha de última modificación y fecha / hora de compilación y estado (en modificación, en producción).
- Verificar que el Analista Responsable que autoriza la solicitud de un programa fuente sea el designado para la aplicación, rechazando el pedido en caso contrario. Registrar cada solicitud aprobada.
- Administrar las distintas versiones de una aplicación.
- Asegurar que un mismo programa fuente no sea modificado simultáneamente por más de un desarrollador.
- Denegar al "administrador de programas fuentes" permisos de modificación sobre los programas fuentes bajo su custodia.
- Establecer que todo programa objeto o ejecutable en producción tenga un único programa fuente asociado que garantice su origen.
- Establecer que el implementador de producción efectuará la generación del programa objeto o ejecutable que estará en producción (compilación), a fin de garantizar tal correspondencia.
- Desarrollar un procedimiento que garantice que toda vez que se migre a producción el módulo fuente, se cree el código ejecutable correspondiente en forma automática.
- Evitar que la función de "administrador de programas fuentes" sea ejercida por personal que pertenezca al sector de desarrollo y/o mantenimiento.
- Prohibir la guarda de programas fuentes históricos (que no sean los correspondientes a los programas operativos) en el ambiente de producción.
- Prohibir el acceso a todo operador y/o usuario de aplicaciones a los ambientes y a las herramientas que permitan la generación y/o manipulación de los programas fuentes.
- Realizar las copias de respaldo de los programas fuentes cumpliendo los requisitos de seguridad establecidos por la Institución en los procedimientos que surgen de la presente política.

6.17.14 Seguridad de los procesos de Desarrollo y Soporte

Esta Política provee seguridad al software y a la información del sistema de aplicación, por lo tanto se controlarán los entornos y el soporte dado a los mismos.

6.17.15 Procedimiento de Control de Cambios

A fin de minimizar los riesgos de alteración de los sistemas de información, se implementarán controles estrictos durante la implementación de cambios imponiendo el cumplimiento de procedimientos formales. Éstos garantizarán que se cumplan los procedimientos de seguridad y control, respetando la división de funciones.

Para ello se establecerá un procedimiento que incluya las siguientes consideraciones:

- Verificar que los cambios sean propuestos por usuarios autorizados y respete los términos y condiciones que surjan de la licencia de uso.
- Mantener un registro de los niveles de autorización acordados.
- Solicitar la autorización del propietario de la Información, en caso de tratarse de cambios a sistemas de procesamiento de la misma.
- Identificar todos los elementos que requieren modificaciones (software, bases de datos, hardware).

- Revisar los controles y los procedimientos de integridad para garantizar que no serán comprometidos por los cambios.
- Obtener aprobación formal por parte del Responsable de la Dirección de Tecnologías de la Información para las tareas detalladas, antes que comiencen las tareas.
- Solicitar la revisión del Oficial de Seguridad de la Información para garantizar que no se violen los requerimientos de seguridad que debe cumplir el software.
- Efectuar las actividades relativas al cambio en el ambiente de desarrollo.
- Obtener la aprobación por parte del usuario autorizado y del área de pruebas mediante pruebas en el ambiente correspondiente.
- Actualizar la documentación para cada cambio implementado, tanto de los manuales de usuario como de la documentación operativa.
- Mantener un control de versiones para todas las actualizaciones de software.
- Garantizar que la implementación se llevará a cabo minimizando la discontinuidad de las actividades y sin alterar los procesos involucrados.
- Informar a las áreas usuarias antes de la implementación de un cambio que pueda afectar su operatoria.
- Garantizar que sea el implementador quien efectúe el pasaje de los objetos modificados al ambiente operativo, de acuerdo a lo establecido en 6.17.10 “Control del Software Operativo”.

En el **ANEXO 3** al presente capítulo se presenta un esquema modelo de segregación de ambientes de procesamiento.

6.17.16 Revisión Técnica de los cambios en el Sistema Operativo

Toda vez que sea necesario realizar un cambio en el Sistema Operativo, los sistemas serán revisados para asegurar que no se produzca un impacto en su funcionamiento o seguridad.

Para ello, se definirá un procedimiento que incluya:
- Revisar los procedimientos de integridad y control de aplicaciones para garantizar que no hayan sido comprometidas por el cambio.
- Garantizar que los cambios en el sistema operativo sean informados con anterioridad a la implementación.
- Asegurar la actualización del Plan de Continuidad de las Actividades de la Institución.

6.17.17 Restricción del cambio de Paquetes de Software

En caso de considerarlo necesario la modificación de paquetes de software suministrados por proveedores, y previa autorización del Responsable de la Dirección de Tecnologías de la Información, se deberá:
- Analizar los términos y condiciones de la licencia a fin de determinar si las modificaciones se encuentran autorizadas.
- Determinar la conveniencia de que la modificación sea efectuada por la Institución, por el proveedor o por un tercero.
- Evaluar el impacto que se produce si la Institución se hace cargo del mantenimiento.
- Retener el software original realizando los cambios sobre una copia perfectamente identificada, documentando exhaustivamente por si fuera necesario aplicarlo a nuevas versiones.

6.17.18 Canales Ocultos y Código Malicioso

Un canal oculto puede exponer información utilizando algunos medios indirectos y desconocidos. El código malicioso está diseñado para afectar a un sistema en forma no autorizada y no requerida por el usuario.

En este sentido, se redactarán normas y procedimientos que incluyan:
- Adquirir programas a proveedores acreditados o productos ya evaluados.
- Examinar los códigos fuentes (cuando sea posible) antes de utilizar los programas.
- Controlar el acceso y las modificaciones al código instalado.
- Utilizar herramientas para la protección contra la infección del software con código malicioso.

6.17.19 Desarrollo Externo de Software

Para el caso que se considere la tercerización del desarrollo de software, se establecerán normas y procedimientos que contemplen los siguientes puntos:
- Acuerdos de licencias, propiedad de código y derechos conferidos.
- Requerimientos contractuales con respecto a la calidad del código y la existencia de garantías.
- Procedimientos de certificación de la calidad y precisión del trabajo llevado a cabo por el proveedor, que incluyan auditorías, revisión de código para detectar código malicioso, verificación del cumplimiento de los requerimientos de seguridad del software establecidos, etc.
- Verificación del cumplimiento de las condiciones de seguridad contempladas en el punto 6.3.1. Requerimientos de Seguridad en Contratos de Tercerización.
- Acuerdos de custodia de las fuentes del software (y cualquier otra información requerida) en caso de quiebra de la tercera parte.

6.18 Administración de la continuidad de las Actividades de la Institución

6.18.1 Generalidades

La administración de la continuidad de las actividades es un proceso crítico que debe involucrar a todos los niveles de la Institución.

El desarrollo e implementación de planes de contingencia es una herramienta básica para garantizar que las actividades de la Institución puedan restablecerse dentro de los plazos requeridos.

Dichos planes deben mantenerse actualizados y transformarse en una parte integral del resto de los procesos de administración y gestión, debiendo incluir necesariamente controles destinados a identificar y reducir riesgos, atenuar las consecuencias de eventuales interrupciones de las actividades de la institución y asegurar la reanudación oportuna de las operaciones indispensables.

6.18.2 Objetivo

- Minimizar los efectos de las posibles interrupciones de las actividades normales de la Institución (sean éstas resultado de desastres naturales, accidentes, fallas en el equipamiento, acciones deliberadas u otros hechos) y proteger los procesos críticos mediante una combinación de controles preventivos y acciones de recuperación.

- Analizar las consecuencias de la interrupción del servicio y tomar las medidas correspondientes para la prevención de hechos similares en el futuro.
- Maximizar la efectividad de las operaciones de contingencia de la Institución con el establecimiento de planes que incluyan al menos las siguientes etapas:
  - Notificación / Activación: Consistente en la detección y determinación del daño y la activación del plan.
  - Reanudación: Consistente en la restauración temporal de las operaciones y recuperación del daño producido al sistema original.
  - Recuperación: Consistente en la restauración de las capacidades de proceso del sistema a las condiciones de operación normales.
- Asegurar la coordinación con el personal de la Institución y los contactos externos que participarán en las estrategias de planificación de contingencias. Asignar funciones para cada actividad definida.

6.18.3 Alcance

Esta Política se aplica a todos los procesos críticos identificados de la Institución.

6.18.4 Responsabilidad

El Oficial de Seguridad de la Información participará activamente en la definición, documentación, prueba y actualización de los planes de contingencia.

Los Propietarios de la Información (Ver 6.1.2. Asignación de Responsabilidades en Materia de Seguridad de la Información) y el Oficial de Seguridad de la Información cumplirán las siguientes funciones:

- Identificar las amenazas que puedan ocasionar interrupciones de los procesos y/o las actividades de la Institución.
- Evaluar los riesgos para determinar el impacto de dichas interrupciones.
- Identificar los controles preventivos.
- Desarrollar un plan estratégico para determinar el enfoque global con el que se abordará la continuidad de las actividades de la Institución.
- Elaborar los planes de contingencia necesarios para garantizar la continuidad de las actividades de la Institución.

Los responsables de Procesos revisarán periódicamente los planes bajo su incumbencia, como así también identificar cambios en las disposiciones relativas a las actividades de la Institución aún no reflejadas en los planes de continuidad.

Los administradores de cada plan verificarán el cumplimiento de los procedimientos implementados para llevar a cabo las acciones contempladas en cada plan de continuidad.

6.18.5 Política del proceso de la Administración de la Continuidad de la Institución

El Comité de Seguridad de la Información , será el responsable de la coordinación del desarrollo de los procesos que garanticen la continuidad de las actividades de la Institución.

Este Comité tendrá a cargo la coordinación del proceso de administración de la continuidad de la operatoria de los sistemas de tratamiento de información de la Institución frente a interrupciones imprevistas, lo cual incluye las siguientes funciones:

- Identificar y priorizar los procesos críticos de las actividades de la Institución.

- Asegurar que todos los integrantes de la Institución comprendan los riesgos que la misma enfrenta, en términos de probabilidad de ocurrencia e impacto de posibles amenazas, así como los efectos que una interrupción puede tener en la actividad de la Institución.
- Elaborar y documentar una estrategia de continuidad de las actividades de la Institución consecuente con los objetivos y prioridades acordados.
- Proponer planes de continuidad de las actividades de la Institución de conformidad con la estrategia de continuidad acordada.
- Establecer un cronograma de pruebas periódicas de cada uno de los planes de contingencia, proponiendo una asignación de funciones para su cumplimiento.
- Coordinar actualizaciones periódicas de los planes y procesos implementados.
- Considerar la contratación de seguros que podrían formar parte del proceso de continuidad de las actividades de la Institución.
- Proponer las modificaciones a los planes de contingencia.

6.18.6 Continuidad de las actividades y análisis de los Impactos

Con el fin de establecer un Plan de Continuidad de las actividades de la Institución se deben contemplar los siguientes puntos:

- Identificar los eventos (amenazas) que puedan ocasionar interrupciones en los procesos de las actividades, por ejemplo, fallas en el equipamiento, comisión de ilícitos, interrupción del suministro de energía eléctrica, inundación e incendio, desastres naturales, destrucción edilicia, atentados, etc.
- Evaluar los riesgos para determinar el impacto de dichas interrupciones, tanto en términos de magnitud de daño como del período de recuperación. Dicha evaluación debe identificar los recursos críticos, los impactos producidos por una interrupción, los tiempos de interrupción aceptables o permitidos, y debe especificar las prioridades de recuperación.
- Identificar los controles preventivos, como por ejemplo sistemas de supresión de fuego, detectores de humo y fuego, contenedores resistentes al calor y a prueba de agua para los medios de backup, los registros no electrónicos vitales, etc.

Esta actividad será llevada a cabo con la activa participación de los propietarios de los procesos y recursos de información de que se trate y el Oficial de Seguridad de la Información, considerando todos los procesos de las actividades de la Institución y no limitándose a las instalaciones de procesamiento de la información.
Según los resultados de la evaluación de esta actividad, se desarrollará un plan estratégico para determinar el enfoque global con el que se abordará la continuidad de las actividades de la Institución. Una vez que se ha creado este plan, el mismo debe ser propuesto por el Comité de Seguridad de la Información a la máxima autoridad de la Institución para su aprobación.

6.18.7 Elaboración e implementación de los Planes de Continuidad de las Actividades de la Institución

Los propietarios de procesos y recursos de información, con la asistencia del Oficial de Seguridad de la Información, elaborarán los planes de contingencia necesarios para garantizar la continuidad de las actividades de la Institución. Estos planes deberán ser solicitados por el Comité de Seguridad de la Información.

El proceso de planificación de la continuidad de las actividades considerará los siguientes puntos:

- Identificar y acordar respecto a todas las funciones y procedimientos de emergencia.

- Analizar los posibles escenarios de contingencia y definir las acciones correctivas a implementar en cada caso.
- Implementar procedimientos de emergencia para permitir la recuperación y restablecimiento en los plazos requeridos. Se debe dedicar especial atención a la evaluación de las dependencias de actividades externas y a los contratos vigentes.
- Documentar los procedimientos y procesos acordados.
- Instruir adecuadamente al personal, en materia de procedimientos y procesos de emergencia acordados, incluyendo el manejo de crisis.

Instruir al personal involucrado en los procedimientos de reanudación y recuperación en los siguientes temas:

- Objetivo del plan.
- Mecanismos de coordinación y comunicación entre equipos (personal involucrado).
- Procedimientos de divulgación.
- Requisitos de la seguridad.
- Procesos específicos para el personal involucrado.
- Responsabilidades individuales.
- Probar y actualizar los planes.

Además, el proceso de planificación debe concentrarse en los objetivos de las actividades de la Institución requeridos, por ejemplo, restablecimiento de los servicios a los usuarios en un plazo aceptable. Deben considerarse los servicios y recursos que permitirán que esto ocurra, incluyendo, dotación de personal, recursos que no procesan información, así como acuerdos para reanudación de emergencia en sitios alternativos de procesamiento de la información.

6.18.8 Marco para la planificación de la Continuidad de las actividades de la Institución

Se mantendrá un solo marco para los planes de continuidad de las actividades de la Institución, a fin de garantizar que los mismos sean uniformes e identificar prioridades de prueba y mantenimiento.
Cada plan de continuidad especificará claramente las condiciones para su puesta en marcha, así como las personas a cargo de ejecutar cada componente del mismo. Cuando se identifiquen nuevos requerimientos, se modificarán los procedimientos de emergencia establecidos, por ejemplo, los planes de evacuación o los recursos de emergencia existentes.
El administrador de cada plan de continuidad será el encargado de coordinar las tareas definidas en el mismo.
Estas modificaciones deberán ser aprobados por el Comité de Seguridad de la Información.

El marco para la planificación de la continuidad de las actividades de la Institución, tendrá en cuenta los siguientes puntos:

- Prever las condiciones de implementación de los planes que describan el proceso a seguir (cómo evaluar la situación, qué personas estarán involucradas, etc.) antes de poner en marcha los mismos.
- Definir los procedimientos de emergencia que describan las acciones a emprender una vez ocurrido un incidente que ponga en peligro las operaciones de la Institución y/o la vida humana. Esto debe incluir disposiciones con respecto a la gestión de las relaciones públicas y a vínculos eficaces a establecer con las autoridades públicas pertinentes, por ejemplo, la policía, bomberos y autoridades locales.
- Realizar los procedimientos de emergencia que describan las acciones a emprender para el traslado de actividades esenciales de la Institución o de servicios de soporte a ubicaciones transitorias alternativas, y para el restablecimiento de los procesos en los plazos requeridos.

- Redactar los procedimientos de recuperación que describan las acciones a emprender para restablecer las operaciones normales de la Institución.
- Definir un cronograma de mantenimiento que especifique cómo y cuándo será probado el plan, y el proceso para el mantenimiento del mismo.
- Efectuar actividades de concientización e instrucción al personal, diseñadas para propiciar la comprensión de los procesos de continuidad las actividades y garantizar que los procesos sigan siendo eficaces.
- Documentar las responsabilidades y funciones de las personas, describiendo los responsables de la ejecución de cada uno de los componentes del plan y las vías de contacto posibles. Se deben mencionar alternativas cuando corresponda. Es de suma importancia definir a un responsable de declarar el estado de contingencia, lo cual dará inicio al plan.

El cumplimiento de los procedimientos implementados para llevar a cabo las acciones contempladas en cada plan de continuidad, deben contarse entre las responsabilidades de los administradores de cada plan. Las disposiciones de emergencia para servicios técnicos alternativos, como instalaciones de comunicaciones o de procesamiento de información, normalmente se cuentan entre las responsabilidades de los proveedores de servicios.

6.18.9 Ensayo, mantenimiento y reevaluación de los Planes de Continuidad de la Institución.

Debido a que los planes de continuidad de las actividades de la Institución pueden fallar, por suposiciones incorrectas, errores o cambios en el equipamiento, se establecen las siguientes pautas de acción:

El Comité de Seguridad de la Información establecerá un cronograma de pruebas periódicas de cada uno de los planes de contingencia.

El cronograma indicará quienes son los responsables de llevar a cabo cada una de las pruebas y de elevar el resultado obtenido al citado Comité.

Se deberán utilizar diversas técnicas para garantizar que los planes de contingencia funcionarán ante un hecho real, y éstas incluirán por lo menos:
- Efectuar pruebas de discusión de diversos escenarios (discutiendo medidas para la recuperación las actividades utilizando ejemplos de interrupciones).
- Realizar simulaciones (especialmente para entrenar al personal en el desempeño de sus roles de gestión posterior a incidentes o crisis).
- Efectuar pruebas de recuperación técnica (garantizando que los sistemas de información puedan ser restablecidos con eficacia).
- Realizar ensayos completos probando que la Institución, el personal, el equipamiento, las instalaciones y los procesos pueden afrontar las interrupciones.

Para las operaciones críticas de la Institución se tomarán en cuenta, además, los siguientes mecanismos:
- Efectuar pruebas de recuperación en un sitio alternativo (ejecutando los procesos de las actividades de la Institución en paralelo, con operaciones de recuperación fuera del sitio principal).
- Realizar pruebas de instalaciones y servicios de proveedores (garantizando que los productos y servicios de proveedores externos cumplan con los compromisos contraídos).
- Los planes de continuidad de las actividades de la Institución serán revisados y actualizados periódicamente, para garantizar su eficacia permanente. Se incluirán procedimientos en el

programa de administración de cambios de la Institución para garantizar que se aborden adecuadamente los tópicos de continuidad de las actividades.

La Dirección de Tecnologías de la Información, con los responsables de cada Unidad o Proceso a su cargo deberá elaborar los planes correspondientes y nombrar el administrador; y establecer la periodicidad de evaluación y actualización de los planes.

Cada uno de los responsables de Procesos es el responsable de las revisiones periódicas de cada uno de los planes de continuidad de su incumbencia, como así también de la identificación de cambios en las disposiciones relativas a las actividades de la Institución aún no reflejadas en dichos planes.

Deberá prestarse atención, especialmente, a los cambios de:
- Personal.
- Direcciones o números telefónicos.
- Estrategia de la Institución.
- Ubicación, instalaciones y recursos.
- Legislación.
- Contratistas, proveedores y clientes críticos.
- Procesos, o procesos nuevos / eliminados.
- Tecnologías.
- Requisitos operacionales.
- Requisitos de seguridad.
- Hardware, software y otros equipos (tipos, especificaciones, y cantidad).
- Requerimientos de los sitios alternativos.
- Registros de datos vitales.

Todas las modificaciones efectuadas serán propuestas por el Comité de Seguridad de la Información para su aprobación por el superior jerárquico que corresponda.

Por otra parte, el resultado de este proceso será dado a conocer a fin de que todo el personal involucrado tenga conocimiento de los cambios incorporados.

6.19 CUMPLIMIENTO

6.19.1 Generalidades

El cumplimiento del EGSI considera la implementación de controles que garanticen el cumplimiento del esquema de seguridad de la información.

6.19.2 Objetivo

- Identificar de forma explícita los requisitos necesarios, legales, reglamentarios, contractuales y la visión de la institución para cumplir con estos requisitos, debe definirse claramente documentarse y mantenerse actualizados para cada sistema de información de la institución.

- Implementar procedimientos adecuados para garantizar el cumplimiento de los requisitos legales, normativos y contractuales relacionados con los derechos de propiedad intelectual y sobre el uso de productos de software original.

- Implementar el procedimiento adecuado para, proteger los registros contra pérdida, destrucción, falsificación, accesos y publicación no autorizados de acuerdo con la norma legal vigente.

- La institución debe desarrollar, implementar y socializar la política de protección y privacidad de la información, según dispone la norma legal vigente.

- La institución debe utilizar los controles de cifrado en cumplimiento con todos los acuerdos, leyes reglamentos de la legislación vigente.

- La gestión de seguridad de la información debe ser revisada al menos 1 vez al año, o cuando se produzcan cambios significativos en la institución.

- El Nivel Jerárquico Superior, debe revisar periódicamente de acuerdo a la criticidad de sus activos, el cumplimiento del procesamiento de la información y procedimientos en el área de su responsabilidad, que cumplan con las normas de seguridad de la información.

- Implementar el procedimiento adecuado, para comprobar regularmente que los sistemas de información cumplen con las políticas y normas de seguridad de la información de la institución.

6.19.3 Alcance

Esta Política se aplica a todos los procesos identificados referentes a seguridad de la información de la Institución.

6.19.4 Responsabilidad

El Oficial de Seguridad de la Información coordinará las actividades del Comité de Seguridad de la Información, para lograr el cumplimiento de la implementación del EGSI.

6.19.5 Cumplimiento de los requisitos legales y contractuales.

Se deberá considerar las normas y leyes más generales relacionadas a la gestión de los datos e información electrónica en el gobierno. A saber:

- Constitución de la República del Ecuador
- Ley de Comercio Electrónico. Firmas Electrónicas y Mensajes de Datos
- Ley Orgánica de Transparencia y Acceso a la Información Pública
- Ley del Sistema Nacional de Registro de Datos Públicos
- Estatuto del Régimen Jurídico Administrativo de la Función Ejecutiva
- Ley Orgánica y Normas de Control de la Contraloría General del Estado
- Leyes y normas de control del sistema financiero
- Leyes y normas de control de empresas públicas
- Ley del Sistema Nacional de Archivos
- Código orgánico de la economía social de los conocimientos, creatividad e innovación
- Otras normas cuya materia trate sobre la gestión de los activos de información en las instituciones de la Administración Pública

6.19.6 Derechos de propiedad Intelectual

Se deberá realizar las siguientes actividades:

- Implementar mecanismos para concienciar sobre las políticas para proteger derechos de propiedad intelectual y las acciones disciplinarias para el personal que las viole. Se aplica tanto al software libre como al privativo.
- Verificar que se instale únicamente software autorizado y con las respectivas licencias en el caso de utilizar software privativo.
- Definir y aplicar una licencia pública general al software desarrollado por la institución o contratado a terceros como desarrollo, para proteger la propiedad intelectual.

6.19.7 Protección de los registros Control.

Para cumplir los objetivos de salvaguardar los registros, la institución debe clasificar los registros electrónicos y físicos por tipos, especificando los periodos de retención y los medios de almacenamiento, como discos, cintas, entre otros. Se deberá crear bitácoras de registro. Se deberá establecer un procedimiento para garantizar el acceso a los datos e información.

6.19.8 Protección y privacidad de la información de carácter personal

El Oficial de Seguridad de la Información deberá controlar la aplicación de la política de protección de datos y privacidad de la información personal. Se deberá implementar una política de uso e intercambio de datos personales de personas o ciudadanos en custodia de las instituciones públicas.

6.19.9 Revisiones de seguridad de la información

El Comité de Seguridad de la Información, deberá revisar la Política de Seguridad de la Información al menos 1 vez al año, o cuando se produzcan cambios significativos en la institución.
El Comité de Seguridad de la Información, deberá auditar periódicamente el cumplimiento la Política de Seguridad. Si se determina algún incumplimiento o no conformidad como resultado de la revisión, la dirección deberá:

- Determinar la causa del incumplimiento
- Evaluar la necesidad de acciones para garantizar que no se repitan estos incumplimientos
- Determinar e implementar la acción correctiva apropiada
- Revisar la acción correctiva que se ejecutó

El Comité de Seguridad de la Información, deberá ejecutar o contratar pruebas de penetración y evaluaciones de la vulnerabilidad, las cuales pueden ser realizadas por expertos independientes especialmente contratados

ANEXO 1

ACUERDO DE CONFIDENCIALIDAD Y NO DIVULGACIÓN DE INFORMACIÓN PARA USO DE UNA RED PRIVADA VIRTUAL - VPN

Acuerdo de confidencialidad y no divulgación de información que celebran por una parte el Ministerio de Desarrollo Urbano y Vivienda – MIDUVI a través de **(Nombre del funcionario que entrega la información/administrador del contrato o proyecto)**, a quién se lo reconocerá como el INFORMANTE y por otro lado **(Responsable oficial por parte del proveedor, consultor externo o funcionario)** a quien se lo reconocerá como RECEPTOR en la ciudad de Quito el día _____.

CLAUSULAS:

PRIMERA.- El presente Acuerdo se refiere a la información que EL INFORMANTE proporcione al RECEPTOR, ya sea de forma oral, gráfica o a través de archivos y/o scripts de configuración que contengan la información necesaria como contraseñas para la obtención de accesos vía VPN a equipos de comunicaciones y servidores que actualmente se encuentran en producción en el MIDUVI a fin de **(detallar el motivo por el cual se entrega la información……)**.

SEGUNDA.-

1.- EL RECEPTOR únicamente utilizará la información facilitada por EL INFORMANTE para el fin mencionado en la estipulación anterior, comprometiéndose EL RECEPTOR a mantener la más estricta confidencialidad respecto de dicha información, advirtiendo de dicho deber de confidencialidad y secreto a sus funcionarios y servidores públicos, asociados y a cualquier persona que, por su relación con EL INFORMANTE, deba tener acceso a dicha información para el correcto cumplimiento de las obligaciones del RECEPTOR para con EL INFORMATE.
2.- EL RECEPTOR o las personas mencionadas en el párrafo anterior no podrán reproducir, modificar, hacer pública o divulgar a terceros la información objeto del presente acuerdo sin previa autorización escrita y expresa del INFORMANTE.
3.- De igual forma, EL RECEPTOR adoptará respecto de la información objeto de este acuerdo las mismas medidas de seguridad que adoptaría normalmente respecto a la información confidencial de su propia empresa u organización, evitando su pérdida, robo o sustracción.
4.- Es de exclusiva responsabilidad por parte del RECEPTOR el buen uso del enlace entregado por el INFORMANTE, así como también cada una de las actividades que el RECEPTOR realice en equipos o servidores que estén al alcance del mismo, cualquier problema técnico sea este de acceso, daño o degradación en la configuración de equipos de comunicaciones, virus en servidores de producción, etc.; deberá ser penalizado, siendo el RECEPTOR quien afronte las consecuencias.

TERCERA.- Sin perjuicio de lo estipulado en el presente acuerdo, ambas partes aceptan que la obligación de confidencialidad no se aplicará en los siguientes casos:

a) Cuando la información se encontrara en el dominio público en el momento de su suministro al RECEPTOR o, una vez suministrada la información, ésta acceda al dominio público sin infracción de ninguna de las Estipulaciones del presente Acuerdo.
b) Cuando la información ya estuviera en el conocimiento del RECEPTOR con anterioridad a la firma del presente acuerdo y sin obligación de guardar confidencialidad.

c) Cuando la legislación vigente o un mandato judicial exija su divulgación. En ese caso, EL RECEPTOR notificará al INFORMANTE tal eventualidad y hará todo lo posible por garantizar que se dé un tratamiento confidencial a la información.

En caso de que EL RECEPTOR pueda probar que la información fue desarrollada o recibida legítimamente de terceros, de forma totalmente independiente a su relación con EL INFORMANTE.

CUARTA.- Los derechos de propiedad intelectual de la información objeto de este Acuerdo pertenecen al INFORMANTE y el hecho de revelarla al RECEPTOR para el fin mencionado en la Estipulación Primera no cambiará tal situación.
En caso de que la información resulte revelada o divulgada o utilizada por EL RECEPTOR de cualquier forma distinta al objeto de este acuerdo, ya sea de forma dolosa o por mera negligencia, habrá de indemnizar al INFORMANTE los daños y perjuicios ocasionados, sin perjuicio de las acciones civiles o penales que puedan corresponder a este último ***(si se requiere, se puede fijar la cantidad determinada como indemnización)***.

QUINTA.- Las partes se obligan a devolver cualquier documentación, antecedentes facilitados en cualquier tipo de soporte y, en su caso, las copias obtenidas de los mismos, que constituyan información amparada por el deber de confidencialidad objeto del presente acuerdo, en el supuesto de que cese la relación entre las partes por cualquier motivo.

SEXTA.- El presente Acuerdo entrará en vigor en el momento de la firma del mismo por ambas partes, extendiéndose su vigencia hasta un plazo de **(puede ser indefinido o válido cada año)** después de finalizada la relación entre las partes o, en su caso, la prestación del servicio.
Y en señal de expresa conformidad y aceptación de los términos recogidos en el presente Acuerdo, lo firman las partes por triplicado.

_____	_____
EL INFORMANTE	EL RECEPTOR
C.C./RUC:	C.C./RUC:

(*Para la Impresión del acuerdo eliminar esta nota aclaratoria y los datos/ comentarios entre paréntesis)

ANEXO 2

Ministerio de Desarrollo Urbano y Vivienda

SOLICITUD DE INGRESO DE EQUIPOS PARA MANTENIMIENTO

Dirección de Tecnologías de la Información y Comunicación

Gestión de Soporte Técnico

DATOS DE RECEPCIÓN DE EQUIPOS

RECIBIDO POR (Nombres y apellidos): _____

FECHA DE RECEPCIÓN DE EQUIPO: _____

NRO DE INCIDENCIA: _____

DATOS DEL EQUIPO

TIPO DE EQUIPO: _____ MARCA: _____

MODELO: _____ NRO. DE SERIE: _____

CÓDIGO MIDUVI: _____ MARCA DE ADAPTADOR: _____

NÚMERO DE SERIE DE ADAPTADOR: _____

DATOS DE USUARIO DE EQUIPO

NOMBRES Y APELLIDOS DEL USUARIO: _____

EDIFICIO/DIRECCIÓN PROVINCIAL: _____

UNIDAD ADMINISTRATIVA/PROYECTO: _____

CORREO ELECTRÓNICO: _____

EXTENSIÓN: _____

SELECCIONE EL MOTIVO DE LA SOLICITUD SEÑALANDO LAS SIGUIENTES OPCIONES:

ASISTENCIA TÉCNICA Indicar el problema que presenta el equipo				REVISIÓN Y/O MANTENIMIENTO Señale el/los dispositivo/s que requieren mantenimiento				INSTALAR/REINSTALAR PROGRAMAS Seleccione el/los programas a instalar			
	No enciende		Lentitud		Teclado		Monitor		Formateo disco		Antivirus
	Se reinicia		Mensaje de error		Unidad de CD/DVD		Teléfono		Normalización		Token
	Archivos perdidos		Virus		Mouse		Puerto USB		Ofimática		Sistema Operativo
	Otros				Sonido		Otro		Drivers		Otros

OBSERVACIONES

DATOS DEL TÉCNICO ASIGNADO	
NOMBRES Y APELLIDOS DE TÉCNICO ASIGNADO	FECHA DE RECEPCIÓN
BREVE DESCRIPCIÓN DE LA SOLUCIÓN	FECHA DE ENTREGA

FIRMA DE USUARIO	FIRMA DE TÉCNICO	ACEPTADO CONFORME

Mantenimiento Preventivo

Equipo	Frecuencia de Mantenimiento	Responsable	Personal Autorizado

ANEXO 3

Para cumplir con esta Política, en lo referente a los puntos “Seguridad de los Archivos del Sistema” y “Seguridad de los Procesos de Desarrollo y Soporte”, se sugiere implementar un modelo de separación de funciones entre los distintos ambientes involucrados. Toda aplicación generada en el sector de desarrollo o adquirida a un proveedor es, en algún momento, implementada en un ambiente de producción. Los controles de esta transferencia deben ser rigurosos a fin de asegurar que no se instalen programas fraudulentos. Es conveniente implementar algún software para la administración de versiones y para la transmisión de programas entre los ambientes definidos, con un registro asociado para su control.

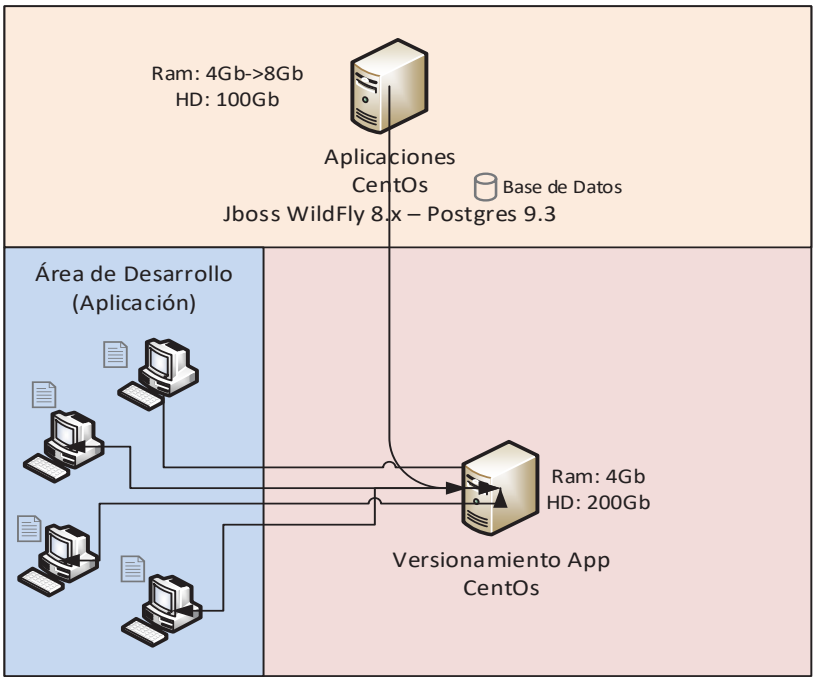
A continuación se presenta un modelo formado por tres ambientes que debe ser adaptado al MIDUVI, teniendo en cuenta las capacidades instaladas, los recursos y el equipamiento existente.

Ambiente de Desarrollo

Es donde se desarrollan los programas fuentes y donde se almacena toda la información relacionada con el análisis y diseño de los sistemas. El analista o programador (desarrollador) tiene total dominio sobre el ambiente. Puede recibir algún fuente para modificar, quedando registrado en el sistema de control de versiones que administra el “administrador de programas fuentes”.

El desarrollador realiza las pruebas con los datos de la base de desarrollo (la base de datos se encontrara local o en el servidor de desarrollo). Cuando considera que el programa está terminado, lo pasa al ambiente de pruebas junto con la documentación requerida que le entregará al implementador de ese ambiente.

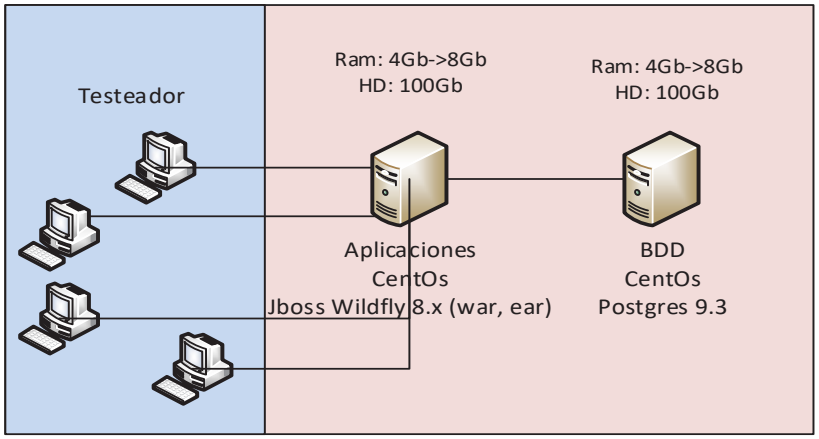
DIAGRAMA AMBIENTE DE DESARROLLO



Ambiente de Pruebas

El implementador de este ambiente recibe el programa y la documentación respectiva y realiza una prueba general con un lote de datos para tal efecto, junto con el usuario de ser posible.
El testeador realiza las pruebas con los datos de la base de pruebas. El ambiente de pruebas será una copia exacta del ambiente de producción (base de datos y configuración del servidor de aplicaciones). Si no detectan errores de ejecución, los resultados de las rutinas de seguridad son correctos de acuerdo a las especificaciones y considera que la documentación presentada es completa, entonces remite el programa fuente al implementador de producción, se remitirá formalmente la versión del programa con las autorizaciones respectivas. Caso contrario, vuelve atrás el ciclo devolviendo el programa al desarrollador, junto con un detalle de las observaciones.

DIAGRAMA AMBIENTE DE PRUEBAS
(PREPRODUCCIÓN)



Ambiente de Producción

Es donde se ejecutan los sistemas y se encuentran los datos registrados por los usuarios finales del sistema, los cuales ya serán utilizados para la gestión del Ministerio. Los programas fuentes certificados se guardan en un repositorio de fuentes de producción, almacenándolos mediante un sistema de control de versiones que maneja el "administrador de programas fuentes" y donde se dejan los datos del programador que hizo la modificación, fecha, hora y tamaño de los programas fuentes y objetos o ejecutables. El "implementador" compila el programa fuente dentro del ambiente de producción en el momento de realizar el pase, para asegurar de esta forma que hay una correspondencia biunívoca con el ejecutable en producción y luego se elimina, dejándolo en el repositorio productivo de programas fuentes.
Deberían aplicarse procedimientos de la misma naturaleza y alcance para las modificaciones de cualquier otro elemento que forme parte del sistema, por ejemplo: modelo de datos de la base de datos o cambios en los parámetros, etc. Las modificaciones realizadas al software de base (Sistemas Operativos, motores de bases de datos, productos middleware) deberían cumplir idénticos pasos, sólo que las implementaciones las realizarán los propios administradores.
Cabe aclarar que tanto el personal de desarrollo, como el proveedor de los aplicativos, no deben tener acceso al ambiente de producción, así como tampoco a los datos reales para la realización de las pruebas en el Ambiente de Prueba. Para casos excepcionales, se debe documentar adecuadamente la autorización, los trabajos realizados y monitorearlos en todo momento.

Se aplicara este procedimiento para el desarrollo de los nuevos requerimientos y para el mantenimiento de los módulos existentes en los sistemas del Ministerio.

ACUERDO MINISTERIAL Nro. 025-20

Arq. Guido Esteban Macchiavello Almeida
MINISTRO DE DESARROLLO URBANO Y VIVIENDA

CONSIDERANDO:

Que, la Constitución de la República del Ecuador en el artículo 30, dispone: *"Las personas tienen derecho a un hábitat seguro y saludable, y a una vivienda adecuada y digna, con independencia de su situación social y económica."*

Que, la Constitución de la República del Ecuador en el numeral 2 del artículo 66 indica que se reconoce y garantiza a las personas: *"El derecho a una vida digna, que asegure la salud, alimentación y nutrición, agua potable, vivienda, saneamiento ambiental, educación, trabajo, empleo, descanso y ocio, cultura física, vestido, seguridad social y otros servicios sociales necesarios."*

Que, el artículo 154 número 1 de la Constitución de la República, señala que dentro de las atribuciones de los Ministros de Estado les corresponde: *"(...) Ejercer la rectoría de las políticas públicas del área a su cargo y expedir los acuerdos y resoluciones administrativas que requiera."*

Que, el artículo 226 de la Constitución de la República, dispone que: *"Las instituciones del Estado, sus organismos, dependencias, las servidoras o servidores públicos y las personas que actúen en virtud de una potestad estatal ejercerán solamente las competencias y facultades que les sean atribuidas en la Constitución y la ley. Tendrán el deber de coordinar acciones para el cumplimiento de sus fines y hacer efectivo el goce y ejercicio de los derechos reconocidos en la Constitución."*

Que, el artículo 375 de la Constitución de la República del Ecuador, determina: *"El Estado, en todos sus niveles de gobierno, garantizará el derecho al hábitat y a la vivienda digna, para lo cual: (...) El Estado ejercerá la rectoría para la planificación, regulación, control, financiamiento y elaboración de políticas de hábitat y vivienda".*

Que, el artículo 85 de la Ley Orgánica de Ordenamiento Territorial, Uso y Gestión de Suelo, establece: *"La vivienda de interés social es la vivienda adecuada y digna destinada a los grupos de atención prioritaria y a la población en situación de pobreza o vulnerabilidad, en especial la que pertenece a los pueblos indígenas, afroecuatorianos y montubios. La definición de la población beneficiaria de vivienda de interés social así como los parámetros y procedimientos que regulen su acceso, financiamiento y construcción serán determinados en base a lo establecido por el órgano rector nacional en materia de hábitat y vivienda en coordinación con el ente rector de inclusión económica y social."*

Que, el artículo 147 del Código Orgánico de Organización Territorial, Autonomía y Descentralización, señala: *"El Estado en todos los niveles de gobierno garantizará el derecho a un hábitat seguro y saludable y una vivienda adecuada*

y digna, con independencia de la situación social y económica de las familias y las personas.

El gobierno central a través del ministerio responsable dictará las políticas nacionales para garantizar el acceso universal a este derecho y mantendrá, en coordinación con los gobiernos autónomos descentralizados municipales, un catastro nacional integrado georeferenciado de hábitat y vivienda, como información necesaria para que todos los niveles de gobierno diseñen estrategias y programas que integren las relaciones entre vivienda, servicios, espacio y transporte públicos, equipamiento, gestión del suelo y de riegos, a partir de los principios de universalidad, equidad, solidaridad e interculturalidad.

Los planes y programas desarrollarán además proyectos de financiamiento para vivienda de interés social y mejoramiento de la vivienda precaria, a través de la banca pública y de las instituciones de finanzas populares, con énfasis para las personas de escasos recursos económicos y las mujeres jefas de hogar".

Que, el artículo 47 del Código Orgánico Administrativo COA, sobre la representación legal de las administraciones públicas y señala que: *"(...) la máxima autoridad administrativa de la correspondiente entidad pública ejerce su representación para intervenir en todos los actos y contratos y relaciones jurídicas sujetas a su competencia. Esta autoridad no requiere delegación o autorización alguna de un órgano o entidad superior, salvo en los casos expresamente previstos en la Ley."*

Que, el Estatuto del Régimen Jurídico y Administrativo de la Función Ejecutiva, en su artículo 17 determina que: *"(...) Los Ministros de Estado son competentes para el despacho de todos los asuntos inherentes a sus ministerios sin necesidad de autorización alguna del Presidente de la República, salvo los casos expresamente señalados en leyes especiales (...)."*

Que, con Decreto Ejecutivo Nro. 3 publicado en el Registro Oficial Nro.1 del 11 de agosto de 1992, se crea el Ministerio de Desarrollo Urbano y Vivienda.

Que, las Políticas contenidas en el Plan Nacional de Desarrollo para el Buen Vivir 2010-2013, conllevan a que el Estado deba establecer mecanismos financieros y no financieros para adquisición de vivienda, a favor de los sectores más vulnerables, ampliando la cobertura del subsidio público para la construcción, adquisición y mejoramiento de ella;

Que, el Directorio del Banco del Estado, a través de Resolución Nro. 2012-DIR-012, de 25 de abril de 2012, resolvió calificar los programas y proyectos de financiamiento para vivienda urbana y rural de interés social, como necesarios e indispensables para el desarrollo socio-económico nacional, debiendo la Administración implementarlos y ejecutarlos;

Que, mediante Resolución Nro. CSPE-2012-003, de 17 de mayo de 2012, publicada en el Registro Oficial Nro. 844, de 4 de diciembre de 2012, el Concejo Sectorial de la Política Económica resolvió implementar la política financiera pública y la

reforma de la banca pública de desarrollo, aprobadas por el señor Presidente Constitucional de la República y formalizadas a través del Compromiso Presidencial denominado "*Implementación de medidas propuestas de Banca Pública"*, y; conforme consta en el artículo 2, entre otros, requirió a la dirección y administración de las entidades que conforman el sector financiero público que adopten todas las acciones de carácter legal, operativo, administrativo, de recursos humanos, de comunicación y tecnológica, necesarias para llevar a cabo dicha implementación;

Que, mediante resolución Nro. 2013-DIR-004, de 22 de enero de 2013, publicada en el Registro Oficial Nro. 885, del 4 de febrero del 2013, el Director del Banco del Estado aprobó el programa PROHABITAT VIVIENDA, el mismo que deberá observar y cumplir la política pública y sus actualizaciones, que para el efecto dicte el Ministerio de Desarrollo Urbano y Vivienda, donde queda autorizada la Gerente General del Banco del Estado, para la suscripción de los actos administrativos convenios y contratos necesarios para la implementación y operatividad del Programa, dentro de los cuales se encuentra la suscripción de Convenios de Cooperación Interinstitucional como el presente, una vez cumplidos los requisitos legales previos, establecidos para estas operaciones;

Que, el Banco del Estado otorgó financiamiento para la construcción de vivienda de interés social a los sujetos de crédito establecidos en las *"Políticas de Crédito del Banco del Estado para el Financiamiento de Vivienda de Interés Social",* con la entrega oportuna y efectiva de Bonos de Vivienda que el Estado proyectó para los próximos 10 años, con el fin de garantizar la liquidez de sus programas y proyectos.

Que, mediante Decreto Ejecutivo Nro. 1419 de 22 de enero de 2013, se modificó el Sistema de Incentivos a la Vivienda Social; y, se estableció que para acceder a los bonos de vivienda, el valor de la vivienda será hasta de USD. $30.000 Dólares de los Estados Unidos de América;

Que, el MIDUVI con Acuerdo Ministerial Nro. 0161 de 28 de febrero de 2013, emitió las Normas transitorias para el funcionamiento del *"Sistema de Incentivos a la Vivienda",* mientras se expiden los reglamentos de aplicación a las modificaciones de los diferentes programas y modalidades, al amparo del Decreto Ejecutivo Nro. 1419 de 22 de enero de 2013, reformado con Acuerdo Ministerial Nro. 175**,** de 19 de abril de 2013 que en el numeral 3.2 del Artículo 3 establece el esquema de pago anticipado de bono en la oferta de vivienda social y establece que: *"El promotor podrá solicitar el pago anticipado de bonos correspondiente al 30% de la oferta de vivienda social disponible en el proyecto, previo la presentación de las garantías respectivas. Se podrá efectuar un segundo pago de bonos anticipados de hasta el 30% de la oferta de vivienda social disponible en el proyecto, una vez que se haya justificado el 30% inicialmente pagado de acuerdo con las postulaciones respectivas, y el 40%, se desembolsará una vez que el promotor haya presentado las postulaciones en su totalidad".*

Que, mediante Acuerdo Ministerial Nro. 179, de 15 de mayo de 2013, el MIDUVI expidió el *"Reglamento que establece las condiciones técnicas para la*

calificación de proyectos inmobiliarios de vivienda social que apliquen al bono de vivienda entregado por el MIDUVI y/o a la línea de crédito al Promotor canalizada por el Banco del Estado", posteriormente reformado con Acuerdos Ministeriales Nos. 200 de 12 de julio de 2013; 220 de 14 de octubre de 2013 y, 0013 de 23 de junio de 2014.

Que, el 24 de junio de 2013, el MIDUVI suscribió el Convenio Nro. 271 de Cooperación Interinstitucional, Transferencia y Administración entre el Ministerio de Desarrollo Urbano y Vivienda y Banco del Estado. En la Cláusula Tercera estipula que el Convenio tiene como objeto: *"(...) el MIDUVI y el BdE convienen en cooperar con la ejecución del "Sistema de Incentivos a la Vivienda", en beneficio de la población del sector urbano, constituyendo para el efecto un Fondo en Administración en el BdE, (...)*; y, que el Convenio tiene una vigencia hasta que los recursos, sean entregados y justificados en su totalidad, como así lo establece en la Cláusula Séptima.

Que, el Convenio Nro. 271, suscrito el 24 de junio de 2013, en el primer párrafo de la Cláusula Octava -Administración del Convenio; establece: *"Serán responsables de la administración del presente convenio por parte del MIDUVI, el Subsecretario/a de Vivienda, y; por parte del BdE, el Gerente de Desarrollo Local, quienes tendrán la responsabilidad de efectuar el continuo y oportuno seguimiento y control a la adecuada ejecución del mismo; establecerán la coordinación interinstitucional requerida para el adecuado desarrollo de las obligaciones contraídas, documentarán y custodiarán la información producida a lo largo de la cooperación interinstitucional; reportarán oportunamente a las autoridades sobre eventos y casualidades que pudieren afectar el desarrollo del convenio y propondrán a dichas instancias las acciones y correctivos respectivos."*

Que, mediante Acuerdo Ministerial Nro. 201 de 12 de julio de 2013, el MIDUVI expidió el Sistema de Incentivos para Vivienda Urbana SIV, que el numeral 2 del artículo 66 prevé: *"Los proyectos que ya se encuentren registrados en el MIDUVI hasta el 31 de diciembre del 2012, si requieren financiamiento para construcción de vivienda social a través del BdE, deberán dirigir un oficio al Subsecretario de Vivienda solicitando la actualización de registro del proyecto, para el efecto, actualizarán la documentación del proyecto en base al formulario de actualización de proyectos, con la documentación estipulada en el Reglamento de calificación de proyectos de vivienda social (...)"; "3. En ambos casos el pago de los valores correspondientes a bonos de vivienda serán canalizados al promotor a través del Banco del estado, en función del flujo de caja que se haya aprobado en esta institución, y conforme lo establecido en el contrato de crédito otorgado por el BdE".*

Que, mediante Acuerdo Ministerial Nro. 229 de 18 de noviembre de 2013, se expide las reformas a las Normas de procedimiento aplicables al Sistema de Incentivos para Vivienda Urbana, expedido con Acuerdo Ministerial Nro. 201 de 12 de julio de 2013.

Que, el señor Presidente Constitucional de la República del Ecuador, mediante Decreto Ejecutivo Nro. 724, publicado en el Registro Oficial No. 561 de 7 de

agosto de 2015, delega a la Ministra de Desarrollo Urbano y Vivienda *"(...) para que, mediante acuerdo ministerial, implemente, en adelante, las reformas necesarias para actualizar el Texto Unificado de Legislación del Ministerio de Desarrollo Urbano y Vivienda"*.

Que, la Ministra de Desarrollo Urbano y Vivienda, con sustento en el Decreto Ejecutivo No. 724 antes citado, mediante Acuerdo Ministerial No. 0023-15, publicado en el Registro Oficial No. 572 de 25 de agosto de 2015, expide la "Codificación del Texto Unificado de Legislación del Ministerio de Desarrollo Urbano y Vivienda".

Que, la Ministra de Desarrollo Urbano y Vivienda, con sustento en el Decreto Ejecutivo No. 724 y Segunda Disposición Final del Acuerdo Ministerial No. 0023-15, entre otras disposiciones, con Acuerdo Ministerial No. 027-15 expidió el "Reglamento para la Operación del Sistema de Incentivos para la vivienda – SIV", publicado en el Registro Oficial No. 597, de 29 de septiembre de 2015, con el objeto de establecer las condiciones, requisitos, procedimientos y sanciones del Sistema de Incentivos para la Vivienda (SIV) a fin de facilitar a los diferentes grupos poblacionales especificados el acceso a una vivienda y hábitat digno como parte de los beneficios implementados por el Gobierno Nacional, el mismo que estuvo vigente hasta el 15 de mayo de 2018.

Que, el Ministerio de Desarrollo Urbano y Vivienda, mediante Acuerdo Ministerial No. 027-15, expidió el "Reglamento para la Operación del Sistema de Incentivos para la Vivienda SIV", en la Disposición Transitoria Décima, dispone: *"Los Promotores Inmobiliarios que cuenten con bonos pagados; y que por motivos comprobados no hayan podido justificar con la entrega de vivienda a sus beneficiarios, dentro de los plazos contemplados en el reglamento con el cual fueron pagados; podrán solicitar a la Dirección Provincial correspondiente, se les otorgue un plazo extraordinario, para lo cual deberán adjuntar el cronograma de entrega de viviendas para el análisis, validación y aprobación correspondiente*".

Que, el Estatuto Orgánico de Gestión Organizacional por Procesos del Ministerio de Desarrollo Urbano y Vivienda expedido mediante Acuerdo Nro. 051-15 de 27 de noviembre del 2015, publicado en la Edición Especial No.515 del Registro Oficial del 25 de Febrero del 2016, en el artículo 10 atribuciones y responsabilidades del Ministro dispone: *"Literal c) definir y emitir las políticas y el marco normativo regulador del desarrollo urbano y vivienda que garantice un adecuado desarrollo del sector y controlar su cumplimiento. (...) d) Definir y emitir las políticas y el Marco Normativo regulador para el desarrollo del Sistema Nacional de Catastros. (...) g) Expedir conforme la ley acuerdos, resoluciones, reglamentos y más disposiciones requeridas para la adecuada conducción de la gestión institucional. (...) w) Dirigir la gestión de los modelos integrales: Técnicos, económicos, financieros y de calidad que permitan el fortalecimiento institucional, garantizando el mejoramiento continuo del sector de hábitat, vivienda y asentamientos humanos."*

Que, el 25 de febrero de 2019, el Presidente Constitucional de la República del Ecuador, expidió el Decreto Ejecutivo Nro. 681, publicado en el Segundo

Suplemento del Registro Oficial Nro. 460 de 3 de abril de 2019, contentivo del "REGLAMENTO PARA EL ACCESO A SUBSIDIOS E INCENTIVOS DEL PROGAMA DE VIVIENDAD E INTERÉS SOCIAL Y PÚBLICO EN EL MARCO DE LA INTERVENCIÓN EMBLEMÁTICA "CASA PARA TODOS", que tiene como objeto facilitar el otorgamiento de facilidades e incentivos dirigidos a favorecer el acceso a vivienda, digna, y adecuada a los ciudadanos ecuatorianos, con énfasis en la población en situación de pobreza y vulnerabilidad, así como a los núcleos familiares de ingresos medios y bajos, que presentan necesidad de vivienda propia, asegurando un hábitat seguro e inclusivo; y en la Disposición General Séptima, faculta al Ministerio de Desarrollo Urbano y Vivienda emitir la normativa necesaria que regule la aplicación de subsidios e incentivos para las viviendas de interés social.

Que, mediante Decreto Ejecutivo Nro. 918, de 29 de octubre de 2019, el señor Presidente Constitucional de la República del Ecuador, expidió las Reformas al Decreto Ejecutivo Nro. 681 de 25 de febrero del 2019, contentivo del Reglamento para el Acceso a Subsidios e Incentivos del Programa de Vivienda de Interés Social y Público en el marco de la intervención emblemática "Casa Para Todos", y en su artículo 6 sustituye el texto de la Disposición Transitoria Segunda por la siguiente: *"SEGUNDA.- Aquellos programas o proyectos de vivienda implementados y ejecutados por el Ministerio de Desarrollo Urbano y Vivienda, como bonos, subsidios, incentivos o cualquier otra denominación a los aportes estatales no reembolsables para viviendas de interés social, deberán concluir su gestión, liquidación y cierre, conforme la normativa bajo los cuales se originaron, aprobaron, contrataron, implementaron y ejecutaron. Excepcionalmente previa justificación técnica, económica y legal del ente rector de hábitat y vivienda, podrán sujetarse a normas que deberán generarse para una adecuada liquidación y cierre en favor de recursos del Estado y menor impacto a los beneficiarios".*

Que, en aplicación la Disposición Transitoria Segunda del Decreto Ejecutivo Nro. 918 de 29 de octubre de 2019, el MIDUVI, el Ministerio de Desarrollo Urbano y Vivienda, está facultado en forma excepcional a emitir normas que deberán generarse para una adecuada liquidación y cierre de los proyectos previa justificación técnica, económica y legal.

Que, el Ministerio de Desarrollo Urbano y Vivienda en aplicación al Decreto Ejecutivo No. 681 y su reforma, expidió el Acuerdo Ministerial No. 035-19 del 18 de diciembre de 2019, contentivo de *"LOS LINEAMIENTOS TÉCNICOS PARA EL CIERRE, ACTUALIZACIÓN, REEMPLAZOS Y FIN DE GESTIÓN CON LOS RECURSOS COMPROMETIDOS DEL CONVENIO NRO. 271 DEL 24 DE JUNIO DE 2013, SUSCRITO ENTRE EL MDIUVI Y EL BANCO DEL ESTADO; Y LA ASIGNACIÓN DE SUBSIDIOS EN NUEVOS PROYECTOS".*

Que, el Acuerdo Ministerial No. 035-19 del 18 de diciembre de 2019, expedido por el Ministerio de Desarrollo Urbano y Vivienda, tiene como objeto: "*Emitir los lineamientos técnicos y establecer el procedimiento para la liquidación y cierre de los proyectos de promoción inmobiliaria, previa justificación, técnica, económica y legal, sujeta a la normativa regulatoria y reglamentaria expedida por el MIDUVI, con los cuales fueron calificados o actualizados como*

"proyectos de vivienda de interés social"; y, para concluir la gestión de justificación o devolución de bonos, de los proyectos que tienen crédito liquidado, reestructurado, refinanciado y/o vigente con el Banco de Desarrollo del Ecuador. PB, (BDE) y que no han podido justificar los bonos pagados con la presentación de postulaciones, viviendas terminadas o con escrituras a favor de los beneficiarios, en el marco del Convenio 271, de Cooperación Interinstitucional Transferencia y Administración suscrito el 24 de junio de 2013, entre el Banco del Estado, actual Banco de Desarrollo del Ecuador B.P, y el MIDUVI".

Que, el 11 de marzo de 2020, la Organización Mundial de la Salud ha declarado el brote de coronavirus como pandemia global, pidiendo a los países intensificar las acciones para mitigar su propagación, proteger a las personas y trabajadores de salud y salvar vidas;

Que, el 12 de marzo de 2020, el Ministerio de Salud Pública mediante el Acuerdo Ministerial No. 00126-2020 publicado en el Registro oficial Suplemento No. 160 declaró el estado de emergencia sanitaria en todos los establecimientos del Sistema Nacional de Salud, como consecuencia de la pandemia del coronavirus, en los siguientes términos:

***"Art. 1**.- Declarar el Estado de Emergencia Sanitaria en todos los establecimientos del Sistema Nacional de Salud, en los servicios de laboratorio, unidades de epidemiología y control, ambulancias aéreas, servicios de médicos y paramédicos, hospitalización y consulta externa por la inminente posibilidad del efecto provocado por el coronavirus COVID-19, y prevenir un posible contagio masivo en la población".*

Que, mediante Decreto Ejecutivo No. 1017, de 16 de marzo de 2020, el señor Presidente de la República del Ecuador, declaró estado de excepción durante 60 días por calamidad pública en todo el territorio nacional, por los casos de coronavirus confirmados y la declaratoria de pandemia de COVID-19 por parte de la Organización Mundial de la Salud, que representa un alto riesgo de contagio para toda la ciudadanía y generan afectación a los derechos a la salud y convivencia pacífica del Estado, a fin de controlar la situación de emergencia sanitaria para garantizar los derechos de las personas ante la inminente presencia del virus COVID -19 en Ecuador;

Que, el artículo 6 del Decreto Ejecutivo No. 1017, respecto al desarrollo de la jornada laboral, dispone lo siguiente: "*Se SUSPENDE la jornada presencial de trabajo comprendida entre el 17 al 24 de marzo 2020, para todos los trabajadores y empleados del sector público y del sector privado. El Comité de Operaciones de Emergencia Nacional, una vez evaluado el estado de la situación podrá prorrogar los días de suspensión de la jornada presencial de trabajo"*;

Que, el artículo 8 del Decreto Ejecutivo No. 1017, dispone: *"EMITASE por parte de todas las funciones del Estado y otros organismos establecidos en la Constitución de la República del Ecuador, las resoluciones que se consideren necesarias para que proceda a la suspensión de términos y plazos a las que haya lugar, en procesos judiciales y administrativos , y de igual forma, en*

procesos alternativos de solución de conflictos; a fin de precautelar la salud pública, el orden y la seguridad, en el marco de las garantías del debido proceso, ante la presente calamidad pública";

Que, el Ministerio de Desarrollo Urbano y Vivienda, mediante Resolución 056-20 del 24 de marzo de 2020, suspendió los términos y plazos para la sustanciación y tramitación de reclamos y recursos administrativos; y, los procedimientos de reversión de viviendas que se encuentren en trámite en el Ministerio de Desarrollo Urbano y Vivienda.

Que, el señor Presidente Constitucional de la República, mediante Decreto Ejecutivo No. 1704 del 15 de junio de 2020, declaró el estado de excepción por calamidad pública en todo el territorio nacional por la presencia del COVID-19 en el Ecuador; y que el estado de excepción regirá durante 60 días, a partir de la expedición del referido Decreto.

Que, en virtud de la declaratoria de excepción dispuesta mediante Decreto Ejecutivo Nro.1017 de fecha 16 de marzo de 2020 y Decreto Ejecutivo No. 1704 del 15 de junio de 2020, es necesario la modificación del Acuerdo Ministerial No. 035-19 del 18 de diciembre de 2019, expedido por el Ministerio de Desarrollo Urbano y Vivienda, en aplicación a lo dispuesto en el Decreto Ejecutivo No. 681 y la reforma, que facultan al Ministerio de Desarrollo Urbano y Vivienda, a la expedición de lineamientos para un adecuado cierre y liquidación de los proyectos;

Que, la Subsecretaría de Vivienda, mediante memorando No. MIDUVI-SV-2020-0993-M de 17 de junio de 2020, remitió el Informe Técnico, mediante el cual se justifica técnicamente la expedición de la reforma del Acuerdo Ministerial Nro. 035-19 de 18 de diciembre de 2019, publicado en el Registro Oficial No. 134 de 3 de febrero de 2020, contentivo de "**LOS LINEAMIENTOS TÉCNICOS PARA EL CIERRE, ACTUALIZACIÓN, REEMPLAZOS Y FIN DE GESTIÓN CON LOS RECURSOS COMPROMETIDOS DEL CONVENIO NRO. 271 DEL 24 DE JUNIO DE 2013, SUSCRITO ENTRE EL MIDUVI Y EL BANCO DEL ESTADO; Y LA ASIGNACIÓN DE SUBSIDIOS EN NUEVOS PROYECTOS**".

En uso de las facultades previstas en el número 1 del artículo 154 de la Constitución de la República del Ecuador, artículo 47 del Código Orgánico Administrativo COA; y, artículo 17 del Estatuto del Régimen Jurídico y Administrativo de la Función Ejecutiva ERJAFE;

ACUERDA:

Artículo 1.- Expedir las siguientes reformas al Acuerdo Ministerial Nro. 035-19 de 18 de diciembre de 2019, publicado en el Registro Oficial No. 134 de 3 de febrero de 2020, contentivo de "**LOS LINEAMIENTOS TÉCNICOS PARA EL CIERRE, ACTUALIZACIÓN, REEMPLAZOS Y FIN DE GESTIÓN CON LOS RECURSOS COMPROMETIDOS DEL CONVENIO NRO. 271 DEL 24 DE JUNIO DE 2013, SUSCRITO ENTRE EL MIDUVI Y EL BANCO DEL**

ESTADO; Y LA ASIGNACIÓN DE SUBSIDIOS EN NUEVOS PROYECTOS", expedido por el Ministerio de Desarrollo Urbano y Vivienda.

Artículo 2.- Sustitúyanse el numeral 7.4.2 del artículo 7**,** por lo siguiente:

"**7.4.2. Plazo para justificar postulaciones calificadas y bonos endosados a favor de beneficiarios (valores pagados anticipadamente):**

Los bonos pagados anticipadamente serán justificados en un plazo máximo de tres (3) meses, contados a partir de la vigencia del presente Acuerdo Ministerial.

Los Promotores Inmobiliarios, que no justifiquen en este plazo los bonos cancelados con las postulaciones calificadas y bonos endosados a favor de los beneficiarios, tendrán la obligación de devolver al Banco de Desarrollo del Ecuador B.P., el valor de los bonos más los intereses respectivos, sin que procedan más ampliaciones o prórrogas de plazo".

Artículo 3.- Sustitúyase el texto del numeral **9.3** del artículo 9, por el siguiente:

"El plazo máximo para la presentación de postulantes y justificación con la entrega de viviendas terminadas y escrituras de compraventa a nombre de los beneficiarios que formarán parte de las nuevas etapas del proyecto actualizado será de hasta trece (13) meses, contados a partir de la vigencia del presente Acuerdo Ministerial".

Artículo 4.- Sustitúyase el texto del Artículo 17, por el siguiente:

"El Banco de Desarrollo del Ecuador B.P., se comprometerá a utilizar los recursos remanentes en el plazo de trece (13) meses, contados a partir de la vigencia del presente Acuerdo Ministerial, si cumplido el plazo aún existiesen recursos remanentes, estos serán reembolsados al Ministerio de Desarrollo Urbano y Vivienda y procederán con el cierre y liquidación del Convenio No 271".

Artículo 5.- Elimínese el texto de la Disposición General Quinta del Acuerdo Ministerial No. 035-19.

Artículo 6.- Reenumérese la Disposición General Sexta, por Disposición General Quinta.

Artículo 7.- Añádase a continuación de la Disposición General Quinta renumerada las siguientes Disposiciones:

"**SEXTA**.- Por la Declaratoria del Estado de Excepción y la Declaratoria de Emergencia Sanitaria a consecuencia de la pandemia por el Coronavirus COVID-19, se establece el plazo máximo de tres (3) meses, contados a partir de la vigencia del presente Acuerdo Ministerial, para que el Promotor Inmobiliario justifique todos los recursos recibidos en el marco del Convenio Nro. 271 de 24 de junio de 2013, suscrito entre el MIDUVI y el Banco del Estado (actual Banco de Desarrollo del Ecuador B.P.).

En caso de incumplimiento por parte de los Promotores Inmobiliarios, en la justificación de los bonos en el plazo establecido en el presente Acuerdo Ministerial, el

Banco de Desarrollo del Ecuador B.P., realizará las acciones legales respectivas para la recuperación de los valores no justificados incluidos los intereses legales."

"SÉPTIMA.- En la ejecución e implementación de proyectos de vivienda y justificación de bonos con financiamiento del Banco de Desarrollo del Ecuador B.P., se observará lo estipulado en el Convenio Nro. 271 de 24 de junio de 2013, de Cooperación Interinstitucional, Transferencia y Administración entre el Ministerio de Desarrollo Urbano y Vivienda y Banco del Estado (actual Banco de Desarrollo del Ecuador B.P.), sus modificaciones; y, el presente Acuerdo Ministerial".

DISPOSICIÓN FINAL

PRIMERA.- De la ejecución del presente Acuerdo Ministerial, encárguese a la Subsecretaría de Vivienda, Dirección de Control de Vivienda, Dirección de Regulación, Direcciones de Oficina Técnica y de Prestación de Servicios / Coordinaciones Generales Regionales del MIDUVI, a nivel nacional.

El presente Acuerdo Ministerial, se encontrará vigente desde su suscripción, sin perjuicio de su publicación en el Registro Oficial.

Dado en el Distrito Metropolitano de Quito a los, 2020 JUN 17

firmado electrónicamente por:
GUIDO ESTEBAN MACCHIAVELLO ALMEIDA

Arq. Guido Esteban Macchiavello Almeida
MINISTRO DE DESARROLLO URBANO Y VIVIENDA