MINISTERIO DE LA MUJER Y POBLACIONES VULNERABLES
ES COPIA FIEL DEL ORIGINAL
Que he tenido a la vista
MARIELA JUAREZ BALDERA
SECRETARIA
Fecha: 25/05/18 Registro 212

REPÚBLICA DEL PERÚ

Resolución Ministerial

N°...165-2018-MIMP

Lima, 25 MAYO 2018

Vistos, el Informe Técnico N° 035-2018-MIMP/OGA.OTI/HEH y la Nota N° 128-2018-MIMP/OGA-OTI de la Oficina de Tecnologías de la Información de la Oficina General de Administración del Ministerio de la Mujer y Poblaciones Vulnerables;

CONSIDERANDO:

Que, mediante Resolución Ministerial N° 004-2016-PCM se aprobó el uso obligatorio de la Norma Técnica Peruana "NTP ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 2ª Edición", en todas las entidades integrantes del Sistema Nacional de Informática;

Que, la Norma Técnica Peruana señala que la Alta Dirección debe establecer una política de seguridad de la información que: sea apropiada al propósito de la organización; incluya objetivos de seguridad de la información o proporcione el marco de referencia para fijar los objetivos de seguridad de la información; incluya un compromiso de satisfacer requisitos aplicables relacionados a la seguridad de la información; e, incluya un compromiso de mejora continua del sistema de gestión de seguridad de la información;

Que, la Resolución Ministerial N° 004-2016-PCM, dispone que cada entidad debe designar un Comité de Gestión de Seguridad de la Información, cuyas funciones serán establecidas por cada entidad;

Que, con Resolución Ministerial N° 143-2016-MIMP, modificada por Resolución Ministerial N° 006-2018-MIMP, se constituyó el Comité de Gestión de Seguridad de la Información del Ministerio de la Mujer y Poblaciones Vulnerables - MIMP, que tiene entre sus funciones, proponer la política y objetivos de seguridad de la información alineados con el Plan Estratégico Institucional, con la Política Nacional de Gobierno Electrónico y regulación en el ámbito de seguridad de la información; así como revisar periódicamente la Política de Seguridad de la Información o, si ocurren cambios significativos, asegurar su conveniencia, adecuación y efectividad continua;

Que, en el marco de sus funciones, el Comité de Gestión de Seguridad de la Información mediante Acta N° 03-2018 de fecha 24 de abril de 2018 ha aprobado la propuesta de Política de Seguridad de la Información del Ministerio de la Mujer y Poblaciones Vulnerables, cuyo objetivo es proteger los recursos de la información del MIMP y la tecnología utilizada para su procesamiento, frente a amenazas, internas o externas, deliberadas o accidentales, con el fin de minimizar los riesgos de daño y asegurar la confidencialidad, integridad y disponibilidad de la información; así como también garantizar la continuidad de los sistemas de información que la soportan;

MINISTERIO DE LA MUJER Y POBLACIONES VULNERABLES
ES COPIA FIEL DEL ORIGINAL
que he tenido a la vista
MARIELA VALDEZ BALDERA
SECRETARIA
Fecha: 25/05/18 Registro: 212

Que, mediante el Informe Técnico N° 035-2018-MIMP/OGA.OTI/HEH, que hace suyo a través de la Nota N° 128-2018-MIMP/OGA-OTI, el Director II de la Oficina de Tecnologías de la Información de la Oficina General de Administración, señala que la propuesta cumple con lo dispuesto en la mencionada Norma Técnica Peruana;

Que, resulta necesario aprobar la "Política de Seguridad de la Información del Ministerio de la Mujer y Poblaciones Vulnerables – MIMP";

Con las visaciones de la Secretaría General, de la Oficina General de Administración, de la Oficina General de Planeamiento y Presupuesto, de la Oficina General de Asesoría Jurídica y de la Oficina de Tecnologías de la Información;

De conformidad con lo dispuesto en la Ley N° 29158, Ley Orgánica del Poder Ejecutivo; el Decreto Legislativo N° 1098, Ley de Organización y Funciones del Ministerio de la Mujer y Poblaciones Vulnerables; su Reglamento de Organización y Funciones, aprobado por Decreto Supremo N° 003-2012-MIMP y modificatorias; y la Resolución Ministerial N° 004-2016-PCM que aprueba el uso obligatorio de la Norma Técnica Peruana "NTP ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 2ª Edición", en todas las entidades integrantes del Sistema Nacional de Informática;

SE RESUELVE:

Artículo 1.- Aprobar la "Política de Seguridad de la Información del Ministerio de la Mujer y Poblaciones Vulnerables – MIMP", que como Anexo forma parte de la presente Resolución.

Artículo 2.- Disponer la publicación de la presente Resolución y su Anexo en el portal institucional del Ministerio de la Mujer y Poblaciones Vulnerables (www.mimp.gob.pe).

Regístrese y comuníquese.

ANA MARÍA MENDIETA TREFOGLI
Ministra de la Mujer y Poblaciones Vulnerables
MIMP

PERÚ | Ministerio de la Mujer y Poblaciones Vulnerables

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN DEL MINISTERIO DE LA MUJER Y POBLACIONES VULNERABLES

INDICE

DECLARACIÓN DE LA POLÍTICA GENERAL DE LA SEGURIDAD DE LA INFORMACIÓN

El Ministerio de la Mujer y Poblaciones Vulnerables – MIMP gestiona en forma responsable, la seguridad de la información relacionada con sus actividades, metas y programas, en concordancia con la normatividad vigente y los siguientes lineamientos:

- La implementación de mecanismos para conservar la integridad, confidencialidad y disponibilidad de la información de la institución.
- La identificación de los riesgos de seguridad de la información que son relevantes para la institución, así como su adecuado manejo y mitigación.
- La solución efectiva y adopción de medidas correctivas ante los incidentes relacionados con la seguridad de la información.
- La comunicación y difusión oportuna de la política, y de los procedimientos de seguridad definidos, asegurando que sean asumidos y se encuentren disponibles para todos los interesados.
- El afianzamiento de los valores y el compromiso de todo el personal, a fin de velar por el cumplimiento de la presente política.

CAPÍTULO 1

GENERALIDADES

1.1. Introducción

La Política de Seguridad de la Información del Ministerio de la Mujer y Poblaciones Vulnerables ha sido elaborada en el marco de la Norma Internacional ISO/IEC 27001:2013, y la Norma Técnica Peruana "NTP-ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 2ª Edición", cuyo uso obligatorio ha sido aprobado por la Resolución Ministerial N° 004-2016-PCM, cuya finalidad principal es asegurar la confidencialidad, integridad y disponibilidad de la información gestionada en la Institución.

Las Políticas de Seguridad identifican responsabilidades y establecen los objetivos para una protección apropiada y consistente de los activos de información del Ministerio de la Mujer y Poblaciones Vulnerables, en adelante MIMP.

1.2. Alcance

1.2.1 La Política de Seguridad de la Información tiene alcance a las unidades ejecutoras que conforman el Pliego 039 MIMP, comprometiendo a todas aquellas personas que prestan servicios al MIMP que tengan acceso o que desarrollen, adquieran o usen sistemas de información, aplicaciones informáticas y/o datos del MIMP.

1.2.2 Comprende toda la información generada, administrada, transmitida y almacenada en el MIMP, y todos los sistemas y datos asociados con el almacenamiento, procesamiento y transmisión de la información generada por y a favor del MIMP.

1.2.3 Estas políticas aplican a todas las personas que prestan servicios en los órganos y/o unidades orgánicas de la sede central del MIMP independientemente de su régimen laboral y/o modalidad contractual; así como de aquellas que lo hacen en los programas nacionales del MIMP.

1.2.4 El presente documento comprende las siguientes políticas específicas:

- Política de Gestión de Seguridad de la Información.
- Política de Gestión de Acceso a la Información.
- Política de Seguridad Física.
- Política de Gestión de Operaciones y Comunicaciones.
- Política de Adquisición, Desarrollo y Mantenimiento de Aplicaciones Informáticas.
- Política de Gestión de Incidentes de Seguridad de la Información.

1.3. Objetivos

La Política de Seguridad de la Información tiene como objetivo establecer el marco general de gestión para proteger adecuadamente la información del MIMP, definiendo las directrices generales de actuación que aseguran el tratamiento adecuado de los riesgos y que conduzcan al fortalecimiento de una cultura organizacional en el MIMP, para lo cual se debe asegurar un

compromiso manifiesto de los Directivos Públicos del MIMP, para la difusión, consolidación y cumplimiento de la presente Política.

1.4. Definiciones

Para los fines de la esta Política se establecen las siguientes definiciones:

a) **Activo** (Seguridad de la información): Es cualquier información o sistema relacionado con la captura, generación, tratamiento, almacenamiento y presentación de la misma, el cual tiene un valor para la organización. Estos pueden ser:

- **Activo de información.-** Archivos, bases de datos, manuales procedimientos operativos o de soporte, contratos y acuerdos, material de formación, información financiera, documentos con información de investigación y desarrollo, correo electrónico, libros revistas, etc.
- **Activos de software.-** Software de aplicación, herramientas y programas de desarrollo.
- **Activos físicos.-** Instalaciones (cuarto de servidores, ciosets de cableado y LAN, sistemas de alarma ubicación de proveedor terremark), equipos de cómputo, de comunicaciones, medios magnéticos, u otro equipo técnico.
- **Activos de servicios.-** Servicios de comunicaciones, informáticos, documentarios, de información y informáticos (VPN, FTP,web, proxy, mail, seguridad firewall, iDS, IPS, anti-spam/virus/spyware, servicio de wireless y protocolo de autenticación) y generales (energía eléctrica, telefonía iluminación).
- **Personas.-** Colaboradores del MIMP, sus calificaciones, habilidades y experiencia y conocimientos.
- **Intangibles.-** Reputación e imagen institucional, secretos comerciales, patentes, registros de marca, confianza de los clientes, ventaja competitiva, ética, productividad, relación de negocios (proveedores, clientes, sociedad) logros e imagen corporativa.

b) **Aplicación informática:** Es un tipo de software que permite al usuario realizar uno o más tipos de trabajo. Son aquellos programas que permiten la interacción entre un usuario y una computadora (comunicación), brindándole a aquel la opción de elegir entre varias opciones y ejecutar acciones que el programa le ofrece. Las aplicaciones pueden desarrollarse a medida (para satisfacer las necesidades específicas de un usuario) o formar parte de un paquete integrado.

c) **Confidencialidad:** Garantizar que la información sea accesible únicamente a las personas que cuenten con acceso autorizado.

d) **Disponibilidad:** Conseguir que la información esté disponible para los trabajadores del MIMP, dentro de los parámetros de eficacia normales de los sistemas correspondientes, incluidos los Sistemas de Procesamiento de la Información.

e) **Estación de Trabajo:** Equipo de cómputo, también llamado computadora personal que generalmente está conectada a la red informática y es usada por el colaborador como herramienta de trabajo para conectarse a sistemas de información, aplicaciones informáticas, u otros servicios, tales como correo electrónico, internet, etc.

f) **Incidente de Seguridad de la Información:** Evento no deseado que tiene una probabilidad significativa de comprometer las operaciones de la institución y que genera amenazas a la seguridad de la información.

g) **Información:** Conjunto de datos contenidos en documentos físicos (papel, microfichas, libros, etc.) y medios electrónicos (discos duros, cintas, memorias de tipo USB, disquetes, CD, DVD, discos portátiles, entre otros).

h) **Integridad:** Asegurar que la información no sea manipulada, destruida o corrompida por accidentes o acciones intencionales. Ello incluye los elementos que garantizan su procedencia o autenticidad.

i) **MIMP:** Comprende todas las unidades ejecutoras que conforman el Pliego Ministerio de la Mujer y Poblaciones Vulnerables.

j) **Seguridad de la Información:** Es la preservación de la confidencialidad, integridad y disponibilidad de la información.

k) **Sistema de Información:** Es un conjunto de elementos orientados al tratamiento y administración de datos e información, organizados y listos para su uso posterior, generados para cubrir una necesidad u objetivo. Tales elementos se clasifican principalmente en: Personas, datos, actividades o técnicas de trabajo, y recursos materiales en general (como por ejemplo los recursos informáticos y de comunicación).

l) **Sistema de Gestión de Seguridad de la Información:** Considera los riesgos de la Institución para establecer, implementar, operar, monitorear, revisar, mantener y mejorar la Seguridad de la Información.

m) **Usuario:** Colaborador del MIMP con prescindencia de su nivel o jerarquía autorizado a utilizar un sistema de información determinado, bajo un nivel de acceso preestablecido.

1.5. Responsabilidades Generales

1.5.1 Cumplimiento por parte de los colaboradores del MIMP

En relación con el alcance de la presente Política, se precisa que ésta comprende a todas aquellas personas que prestan servicios al MIMP, independientemente de su régimen laboral o contractual.

Los colaboradores del MIMP tienen la responsabilidad de cumplir con lo establecido en este documento y de aplicarlo en el entorno en el que desempeñan sus funciones. Además, tienen la obligación de alertar de manera oportuna y adecuada al titular del órgano o unidad orgánica en donde o para quien presta sus servicios, sobre cualquier situación que atente contra lo establecido en la presente Política o pueda poner en riesgo la seguridad de la información del MIMP.

1.5.1.1 Funcionarios y Directivos Públicos

Se refiere a quienes ostentan la titularidad de los programas nacionales, Directivos de Alta Dirección y Directores Generales del MIMP, independientemente de su régimen laboral o contractual.

Los Funcionarios y Directivos Públicos del MIMP deberán garantizar e implementar la seguridad de la información y de los sistemas de información dentro del programa, órgano o unidad orgánica a su cargo. Ello implica:

a) Difundir entre el personal a su cargo acerca de la regulación en materia de seguridad de la información que se encuentre en vigencia, y que haya sido puesta en su conocimiento conforme a la normativa vigente.
b) Formular al Comité de Gestión de Seguridad de Información[1] las recomendaciones que considere pertinentes.
c) Asegurar los niveles de confidencialidad de la información bajo su ámbito, verificando que los reglamentos internos sean debidamente cumplidos.
d) Definir al personal bajo su cargo que tendrá acceso a la información, a los sistemas de información y aplicaciones informáticas del MIMP, cuando corresponda.
e) Designar a los trabajadores que se encargarán de apoyar en la difusión de la presente política.
f) Difundir entre el personal a su cargo acerca de la regulación en materia de seguridad de la información que se encuentre en vigencia, y que haya sido puesta en su conocimiento conforme a la normativa vigente.
g) Supervisar periódicamente su ámbito de acción a fin de detectar posibles deficiencias en materia de seguridad de la información.
h) Iniciar rápidamente medidas correctivas e informar al Comité de Gestión de Seguridad de la Información y/u a la Oficina de Tecnologías de la Información, o a la dependencia competente de los programas nacionales, según corresponda, acerca de las deficiencias y demás incidentes de carácter relevante.

1.5.1.2 Servidores del MIMP

Comprende a todos los colaboradores del MIMP, distintos de los Funcionarios y Directivos Públicos, independientemente de su régimen laboral o contractual.

Todos los Servidores del MIMP deberán garantizar activamente la protección de la información. Ello implica:

a) La utilización de la información, de los sistemas de información y de las aplicaciones informáticas solo para el cumplimiento de sus funciones.
b) El cuidado en el manejo de la información y de los sistemas de información, especialmente si se trata de información confidencial, asegurando su no divulgación.
c) Observar los reglamentos internos y cumplir cabalmente los procedimientos y estándares en cuanto a la seguridad en materia de información.
d) Informar a los titulares de los programas nacionales, órganos y unidades orgánicas en donde prestan servicios acerca de las deficiencias e incidentes advertidos en materia de seguridad de la información.
e) Participar en las pruebas e implementación de los planes de contingencia, ante eventuales fallas de los sistemas de información y aplicaciones informáticas.

[1] Resolución Ministerial N° 143-2016-MIMP, que dispuso constituir el Comité de Gestión de Seguridad de la Información del Ministerio de la Mujer y Poblaciones Vulnerables.

1.5.2 Propietario de la Información

Los titulares de los distintos órganos del MIMP son responsables de generar y hacer uso de dicha información. El propietario de la información es quien define la clasificación de la data y es responsable del mantenimiento y actualización de dicha clasificación, sin perjuicio de la responsabilidad por las funciones que por delegación le sean asignadas al personal subalterno.

Esta responsabilidad no puede ser delegada a terceros, con excepción de la custodia de la información que puede darse a un colaborador perteneciente al órgano en particular, quien apoya en las tareas operativas de administración y control de seguridad correspondiente a la información.

El propietario de la información debe participar activamente en la definición del valor de la información para el MIMP, de manera que se puedan determinar los controles apropiados para protegerla.

1.6. Segregación de tareas

Los responsables de las Unidades Orgánicas deben separar las funciones críticas y áreas de responsabilidad con la finalidad de reducir el riesgo de una modificación no autorizada o accidental o el mal uso de los activos de información del MIMP.

1.7. Sanciones por incumplimiento

El MIMP aplicará las medidas disciplinarias a los colaboradores que incumplan con lo dispuesto en la Política de Seguridad de la Información conforme a las disposiciones señaladas en los documentos normativos de la institución, sin prejuicio de las acciones civiles y/o penales que pudieran corresponder.

CAPÍTULO 2

POLÍTICA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

2.1. Objetivos

a) Establecer los lineamientos que faciliten la adecuada toma de decisiones en aspectos relacionados con la Seguridad de la Información.
b) Establecer las disposiciones con respecto al uso de los activos de información del MIMP y de las medidas que se deben adoptar para su protección.
c) Establecer las responsabilidades para la sensibilización y capacitación de los colaboradores del MIMP en relación con la importancia y la comprensión de su rol a efectos de mantener la seguridad de la información.
d) Crear un marco normativo de obligatorio cumplimiento, orientado a gestionar de manera apropiada la seguridad de la información en el MIMP.

2.2. Adhesión a la Política

a) La presente política y procedimientos asociados deben ser cumplidos por todos los colaboradores del MIMP sin excepción.
b) El Comité de Gestión de Seguridad de la Información debe monitorear el cumplimiento de la presente política al menos una vez al año.

2.3. Gestión de Riesgos

a) El Oficial de Seguridad de la Información del MIMP realizará las siguientes actividades, con respecto a la gestión de riesgos:
   - Apoya a las dependencias del MIMP en la identificación, cuantificación y priorización de los riesgos de seguridad de la información, de acuerdo con los objetivos de la Institución.
   - Propone una metodología de análisis y evaluación de riesgos de seguridad que provea un enfoque sistemático adecuado para identificar, cuantificar y priorizar los riesgos de seguridad de la información.
   - Con la colaboración de los propietarios de la información y el Director de la Oficina de Tecnologías de la Información o de la dependencia competente de los programas nacionales, cuando corresponda, utiliza la metodología adoptada para efectuar el análisis de riesgos, a fin de poder establecer los controles apropiados para el tratamiento de cada uno de los riesgos identificados. La evaluación de riesgos debe realizarse como mínimo una vez al año y cada vez que se identifiquen cambios en la estructura, organización y normativa del MIMP.
b) El Comité de Gestión de Seguridad de la Información del MIMP aprueba la metodología y los resultados de la evaluación de riesgos.

2.4. Protección de la información

a) El MIMP reconoce que la seguridad de la información es un objetivo institucional que debe ser impulsado y apoyado por todo sus colaboradores.

b) No es posible eliminar el riesgo, sino sólo mitigarlo, por lo que los controles que se definan para proteger la información deben ser determinados en base a un análisis de riesgos previo, que considere el costo beneficio de aplicarlos.

2.5. Clasificación de la información

Toda información se considera pública, a excepción de aquella que se encuentre clasificada como secreta, confidencial o reservada, de conformidad con lo establecido en el Texto Único Ordenado de la Ley N° 27806, Ley de Transparencia y Acceso a la Información Pública, aprobado mediante Decreto Supremo N° 043-2003-PCM, y su Reglamento, aprobado por Decreto Supremo N° 072-2003-PCM y su modificatoria, y de aquella que se encuentre protegida de conformidad con lo establecido en la Ley N° 29733, Ley de Protección de Datos Personales y su Reglamento aprobado mediante Decreto Supremo N° 003-2013-JUS.

2.6. Uso de activos de información

a) Los activos de información deben ser usados para los fines y objetivos del MIMP, de acuerdo con la política, directivas y procedimientos que se definan, y considerando criterios de buen uso.
b) En el marco de las relaciones que el MIMP establezca con terceros, los convenios, contratos y órdenes, según corresponda, consignarán cláusulas o disposiciones referidas a la confidencialidad de la información que se entregue o a la que tengan acceso, así como sobre la cesión de derechos, de corresponder.
c) Se debe cumplir con los requisitos legales, contractuales y normativos relativos al uso de activos de información, incluyendo la política de seguridad que deben mantenerse alineadas con la normatividad vigente.
d) Se deben guardar reserva y/o proteger los elementos de control de acceso, como contraseñas y tarjetas de identificación, según corresponda.

CAPÍTULO 3

POLÍTICA DE GESTIÓN DE ACCESO A LA INFORMACIÓN

3.1. Objetivos

a) Prevenir accesos no autorizados a los sistemas de información y a los servicios de red.
b) Garantizar que la autorización de acceso a la información se realice de acuerdo con las atribuciones, funciones y/o tareas a desarrollar por los colaboradores.
c) Mantener el acceso autorizado de los colaboradores.
d) Controlar los accesos a la información.

Para el acceso a los distintos activos de información del MIMP se establecen los siguientes lineamientos generales.

3.2. Requerimientos para el control de accesos

Todos los accesos a los recursos de información del MIMP deben basarse en la necesidad y rol del usuario, debiendo la Oficina de Tecnologías de la Información tomar en cuenta los siguientes aspectos:

- Los requerimientos de seguridad de cada una de las aplicaciones.
- Identificación de toda la información relacionada a las aplicaciones y los riesgos a la que está expuesta.
- Uso de perfiles de usuarios estandarizados definidos según roles.
- Revisión periódica de los controles de acceso.
- Revocación de los derechos de acceso.

3.3. Gestión de usuario

a) La Oficina de Tecnologías de la Información o la dependencia competente de los programas nacionales deben asignar un identificador (cuenta) único y exclusivo a todo colaborador que haga uso de los recursos informáticos, ya sea de forma temporal o permanente.
b) Con el propósito de impedir accesos no autorizados a los recursos de información, deben establecerse procedimientos formales para asignar los derechos de acceso a los sistemas.
c) Deben definirse normas y procedimientos de control a nivel de sistema operativo de red, de manera que no se compartan identificadores entre diferentes usuarios ni pueda detectarse la duplicidad de sesiones de usuarios.
d) Los Funcionarios y Directivos Públicos son los encargados de autorizar y solicitar el acceso del personal a su cargo a los recursos de tecnología de información, conforme al procedimiento que se establezca para tal efecto. La Oficina General de Recursos Humanos o la que haga sus veces en los programas informará a la OTI o a la dependencia competente de los programas nacionales sobre los ceses de los colaboradores a efectos de la respectiva eliminación de accesos.
e) La Oficina de Tecnologías de la Información o la dependencia competente de los programas nacionales deben establecer en sus respectivos ámbitos, las normas y procedimientos para la asignación y cambio de contraseñas. Al respecto, se informará al usuario sobre lo siguiente:

- Debe seleccionar secuencias de caracteres o palabras claras y fáciles de recordar. Se debe considerar una longitud mínima de 10 caracteres.
- No debe considerar información relacionada directamente con el usuario (nombre, fecha de nacimiento, teléfono, etc.).
- Cada persona es responsable de la confidencialidad de la contraseña asignada, y de las consecuencias por las acciones que, mediante su uso, terceras personas puedan realizar.
- Las contraseñas deben ser cambiadas regularmente o cada vez que el sistema lo solicite. Está prohibido compartir las contraseñas asignadas.
- No se debe usar las contraseñas utilizadas en el MIMP para sistemas externos (por ejemplo, correo personal).

f) Los usuarios deben bloquear su estación de trabajo si por algún motivo se retiran de su puesto de labores.

g) Todas las estaciones de trabajo deben tener un protector de pantalla con clave y activación automática de bloqueo de usuario cuando no se estén utilizando.

h) Los colaboradores deberán mantener sus escritorios libres de documentos y/o medios de almacenamiento removibles, cuando no los utilicen, procurando guardarlos en gabinetes con llaves cuando se retiren del centro de labores.

3.4. Control de acceso a las redes informáticas

a) El acceso a los recursos de red debe ser controlado por la Oficina de Tecnologías de la Información o la dependencia competente de los programas nacionales, de manera que el personal no comprometa la seguridad de los activos de información.

b) Para la seguridad en las redes informáticas se deben tener en cuenta los siguientes aspectos:

- Lineamientos de uso de la red.
- Segmentación de redes.
- Control de conexiones a redes en base a la política.
- Controles de enrutamiento de redes.

3.5. Control de acceso a los sistemas operativos

a) El acceso a los sistemas operativos de las estaciones de trabajo del MIMP debe ser debidamente controlado por la Oficina de Tecnologías de la Información o por la dependencia competente de los programas nacionales a fin de evitar accesos no autorizados a recursos o información.

b) Dentro de los aspectos que deben ser tomados en consideración para definir los controles, se incluyen:

- Identificación automática de estación de trabajo.
- Procedimientos de inicio de sesión seguros.
- Identificación y autenticación de usuarios.
- Sistema de gestión de contraseñas.
- Restricción del uso de herramientas utilitarias del sistema operativo con capacidades de eludir y/o sobrescribir los controles de seguridad.

3.6. Control de acceso a las aplicaciones

La Oficina de Tecnologías de la Información o la dependencia competente de los programas nacionales deben establecer los lineamientos de control de accesos a la información y a las aplicaciones, restringiéndolas solo para el personal debidamente autorizado; asimismo, revisar periódicamente los accesos concedidos, revocando los derechos cuya vigencia de autorización haya caducado.

3.7. Conexiones externas

En cualquier caso, para el acceso remoto (todo acceso a la información del MIMP fuera del centro de trabajo) se debe utilizar la tecnología y acceso seguro (SSL-VPN) y su uso debe ser autorizado solo en caso de ser necesario por el responsable de la unidad orgánica y la Oficina de Tecnologías de la Información, con el conocimiento del Oficial de Seguridad de la Información del MIMP.

3.8. Seguridad de la Información en la Gestión de Proyectos

Se debe integrar la Seguridad de la Información en los métodos de gestión de proyectos de la organización para asegurar la identificación y tratamiento de los riesgos de seguridad de la información como parte de los proyectos, es decir, los riesgos asociados a la ausencia de Confidencialidad, Integridad y Disponibilidad. Esto se aplica a cualquier proyecto, sin importar su carácter. Para la gestión de riesgos se utilizará la Metodología aprobada dentro de la institución.

CAPÍTULO 4

POLÍTICA DE SEGURIDAD FÍSICA

4.1. Objetivo

Tomar las medidas necesarias para impedir el acceso físico no autorizado, los daños e interferencia a la información y a las instalaciones de procesamiento de la información de la institución.

4.2. Controles de seguridad física perimetral

a) El personal del MIMP que atienda a personas externas a la institución (incluyendo proveedores) deberá asegurar que los datos de todas las visitas de personas externas a la institución quedan anotados en el registro de visitas.
b) Los visitantes a las instalaciones deben portar su pase de visita.
c) Para el ingreso o salida de cualquier equipo de propiedad del MIMP se deberá utilizar el formato de autorización correspondiente con el registro completo de toda la información que allí se solicita.
d) Los colaboradores del MIMP deben portar en todo momento su fotocheck.

4.3. Protección contra amenazas externas y ambientales

a) Las medidas de protección contra amenazas externas y ambientales deben incluir:
   - Detectores de humo.
   - Extintores.
   - Sistema de alimentación ininterrumpida (UPS).
   - Sistema de puesta a Tierra.
   - Sensores de aniego.
   - Grupo Electrógeno.

b) Se deben proteger los equipos de tecnología de la información de fallas por falta de suministro de energía y otras anomalías eléctricas.
c) El cableado de la red de comunicaciones y suministro de energía deben protegerse para evitar intercepción o daño.
d) El cableado de suministro de energía eléctrica y telecomunicaciones en las zonas de tratamiento de información debe contar con un sistema de pozo a tierra, el que debe ser revisado periódicamente para garantizar su adecuado funcionamiento.
e) Se debe considerar un programa de mantenimiento de los equipos de tecnología de información y de los sistemas de acondicionamiento de temperatura, humedad y filtrado de aire, sistemas de energía ininterrumpida (UPS) y sistemas de detección y extinción de fuego, según las especificaciones del fabricante.

CAPÍTULO 5

POLÍTICA DE GESTIÓN DE OPERACIONES Y COMUNICACIONES

5.1. Objetivos

a) Proteger la integridad de software y de la información.
b) Resguardar la información de las redes y la infraestructura que la soporta.
c) Asegurar la operación correcta y segura de los recursos de tecnología de información del MIMP.
d) Implementar y mantener un nivel apropiado de seguridad y de entrega de servicio en línea con los acuerdos celebrados con terceros.
e) Minimizar el riesgo de falla de los sistemas.
f) Monitorear las actividades de procesamiento de información no autorizadas.

Las actividades de gestión sobre los recursos de tecnología de información del MIMP son esenciales para el buen funcionamiento de los servicios de la Institución.

5.2. Responsabilidades de operación

La Oficina de Tecnologías de la Información o de la dependencia competente de los programas nacionales debe asegurar la existencia de documentación formal de sus procedimientos operativos, estableciendo las responsabilidades y los recursos utilizados para su ejecución eficiente.

5.3. Gestión de Cambios

a) La Oficina de Tecnologías de la Información o de la dependencia competente de los programas nacionales deben mantener un registro de control de cambios de los sistemas de información, aplicaciones informáticas, equipos de comunicación, bases de datos, equipos de cómputo y perfiles de acceso, a través de la implementación de acciones y procedimientos orientados a asegurar que todo cambio siga un proceso planificado que incluya responsabilidades y canales de comunicación, identificación de los recursos comprometidos, pruebas de comprobación y estrés, controles de seguridad, reversión en caso de fallas y análisis de impacto.
b) Todos los cambios deben ser solicitados a la Oficina de Tecnologías de la Información o de la dependencia competente de los programas nacionales, por el propietario de la Información, y se llevará un registro sobre cada solicitud de cambio. En caso existiera algún problema con el cambio realizado, se revertirá al estado anterior al cambio.

5.4. Separación de los entornos de desarrollo, prueba y producción

La Oficina de Tecnologías de la Información o de la dependencia competente de los programas nacionales, realizan la separación de los recursos para desarrollo, prueba y producción:

a) Debe separar los recursos de prueba, desarrollo y producción implementando los controles necesarios. Asimismo, se debe definir y documentar el procedimiento para el pase de desarrollo a producción.
b) Asegurar que el entorno de pruebas sea, en lo posible, igual al ambiente de producción en lo referido a recursos de tecnología de información.

c) No debe utilizar datos que contengan información personal u otra de carácter sensible en el ambiente de pruebas.

5.5. Gestión y niveles de servicios externos

a) Los Responsables de las Unidades Orgánicas deben asegurar que todos los controles de seguridad y los Acuerdos de Niveles de Servicio (SLA, por sus siglas en inglés) suscritos con terceros sean implementados y cumplidos.
b) Todos los servicios provistos por terceros deben ser planificados y autorizados por los Responsables de las Unidades Orgánicas, considerando los riesgos.
c) Los Responsables de las Unidades Orgánicas que tengan relaciones con proveedores deben establecer mecanismos de control con el objetivo de asegurar que la información a la que tengan acceso o los servicios que sean provistos por ellos, cumplan con los lineamientos de acuerdo a la política de seguridad de la información. Asimismo, cualquier cambio en los servicios que preste un proveedor debe ser comunicado, acordado y planificado antes de realizarse.

5.6. Planificación y aceptación de los sistemas de información y aplicaciones informáticas

a) La Oficina de Tecnologías de la Información o la dependencia competente de los programas nacionales deben supervisar la planificación de capacidades de los sistemas en operación y proyectar las futuras demandas, a fin de garantizar un procesamiento y almacenamiento adecuado.
b) La Oficina de Tecnologías de la Información o la dependencia competente de los programas nacionales deben establecer los criterios y las pruebas a realizar a los sistemas existentes o nuevos que permitan al área usuaria su evaluación y aceptación formal previa a su puesta en ambiente de producción.

5.7. Protección contra software malicioso

a) La Oficina de Tecnologías de la Información o la dependencia competente de los programas nacionales deben adoptar las medidas necesarias para la prevención, detección y eliminación de código malicioso (malware) a nivel de servidores de red, computadoras portátiles, estaciones de trabajo, tabletas y Smart Phones.
b) La Oficina de Tecnologías de la Información o la dependencia competente de los programas nacionales deben asegurar que todas las estaciones de trabajo estén protegidas con el antivirus corporativo y que éste se encuentre actualizado. Asimismo, debe garantizar que el sistema operativo y los aplicativos de oficina cuenten con las últimas actualizaciones de seguridad (parches).
c) La Oficina de Tecnologías de la Información o la dependencia competente de los programas nacionales son responsables de la renovación de licencias de software, y deberán definir su cronograma de renovación para evitar que se produzca incumplimiento de uso legal de software.
d) El Software utilizado por el MIMP debe ser autorizado en forma expresa por la Oficina de Tecnologías de la Información o la dependencia competente de los programas nacionales de corresponder.

e) El usuario final no debe ser facultado para deshabilitar los sistemas de control y prevención de malware.
f) El personal de soporte técnico de la Oficina de Tecnologías de la Información o de la dependencia competente de los programas nacionales, como medida de prevención, si detecta que algún servidor de red, estación de trabajo o computadora portátil se encuentra infectada con algún tipo de malware, deberá de aislarla inmediatamente, desconectándola de la red del MIMP.

5.8. Gestión interna de respaldo y recuperación

a) Mantener el registro actualizado de las operaciones de gestión de respaldo y recuperación, así como de las fallas que pudieran presentarse y las soluciones realizadas a través del personal de soporte técnico.
b) Establecer procedimientos rutinarios para el respaldo de la información, de acuerdo con su criticidad, realizando copias de seguridad y pruebas de recuperación conforme a un cronograma definido.
c) Asegurar que los equipos y los medios de respaldo cuenten con un programa de mantenimiento preventivo y correctivo para asegurar su correcto funcionamiento.
d) Resguardar las copias de seguridad en un ambiente distinto al de la institución (fuera de las instalaciones del MIMP) que reúna las condiciones adecuadas de acondicionamiento, temperatura y humedad.
e) Estimar anticipadamente la cantidad necesaria de medios magnéticos requeridos para realizar las copias de respaldo y, en caso de no contar con ello, solicitar su oportuna adquisición.
f) Realizar pruebas de restauración a las copias de seguridad a fin de asegurar que se pueda obtener correctamente la información almacenada al momento de ser necesaria.
g) Revisar periódicamente la vigencia tecnológica de los equipos y software utilizados para el respaldo y recuperación de la información.

5.9. Gestión de Seguridad de Red

La Oficina de Tecnologías de la Información o la dependencia competente de los programas nacionales deben implementar los controles y medidas requeridas para proteger y conservar la seguridad de los datos en las redes y la protección de los servicios conectados contra accesos no autorizados. Estos controles deben incluir:

a) Implementación de un esquema de segmentación de redes.
b) El desarrollo de procedimientos para la gestión remota de los recursos de tecnología de información de manera segura.
c) Registro y monitoreo de acciones de seguridad relevantes.
d) Asegurar que los controles de seguridad de la información se apliquen adecuadamente a través de toda la infraestructura de procesamiento de la información.
e) Establecer controles y medidas específicas para salvaguardar la confidencialidad, integridad y disponibilidad de la información que se transfiera a través de redes públicas, así como proteger los sistemas conectados, implementando controles tales como: firewall, utm, filtro de contenidos, antispam, entre otros.

5.10. Registros de auditoría y monitoreo

a) Todos los servicios informáticos se encuentran sujetos a monitoreo por parte de la Oficina de Tecnologías de la Información o la dependencia competente de los programas nacionales.
b) Deben generarse registros de auditoría sobre el uso de los recursos de tecnología de la información.
c) Las actividades de los operadores y administradores de los sistemas deben ser monitoreadas, registradas y verificadas regularmente.
d) Se debe contar con registro de fallas en los sistemas para asegurar que han sido corregidas oportunamente.
e) Los registros de auditoría y monitoreo deben ser respaldados.
f) Cada persona es responsable de todas las actividades realizadas a través de sus cuentas de acceso de red, correo electrónico, sistemas de información asociados y aplicaciones informáticas.

CAPÍTULO 6

POLÍTICA DE ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE APLICACIONES INFORMÁTICAS

6.1. Objetivos

a) Proteger la confidencialidad, autenticidad e integridad de las aplicaciones informáticas del MIMP.
b) Asegurar que las aplicaciones informáticas cumplan con los requisitos de seguridad del MIMP.
c) Evitar pérdidas, modificaciones o mal uso de la información que se encuentra dentro de las aplicaciones.

6.2. Metodología para la adquisición, desarrollo y mantenimiento de las aplicaciones informáticas

a) El MIMP debe aprobar una metodología para la adquisición, desarrollo y mantenimiento de las aplicaciones informáticas.
b) Todo desarrollo y/o mantenimiento de aplicaciones informáticas debe ser documentado con la finalidad de que personas del MIMP no familiarizadas con estas aplicaciones ejecuten las actividades con facilidad.

6.3. Requisitos de seguridad de las aplicaciones informáticas

a) La Oficina de Tecnologías de la Información o la dependencia competente de los programas definen un procedimiento que incluya controles de seguridad durante las etapas de análisis y diseño de las aplicaciones informáticas.
b) Toda aplicación informática desarrollada por el personal de la Oficina de Tecnologías de la Información o de la que haga sus veces en los programas, o por terceros, deben satisfacer los requisitos de seguridad definidos para el desarrollo y mantenimiento de las aplicaciones informáticas. En el caso de los terceros, el desarrollo de las aplicaciones debe constar en el respectivo contrato de prestación de servicios.
c) El personal debe cumplir los controles, estándares y metodologías en relación al desarrollo de las aplicaciones informáticas que se hayan implementado.
d) La Oficina de Tecnologías de la Información o la dependencia competente de los programas deben verificar que los acuerdos sobre materia informática a suscribir con terceros incluyan cláusulas relativas a la cesión de derechos y confidencialidad de la información para el resguardo de la propiedad intelectual del MIMP.
e) Los acuerdos que involucran el acceso, procesamiento, comunicación o manejo de terceros de las instalaciones de procesamiento de información deben cubrir los requisitos de seguridad necesarios.
f) Toda aplicación informática desarrollada por los colaboradores es de propiedad del MIMP.

6.4. Seguridad de los archivos de las aplicaciones informáticas

La implementación de controles sobre lo siguiente:

a) Control de la aplicación informática en Producción: Comprende la formulación y puesta en práctica de procedimientos orientados a controlar la instalación de la aplicación en los sistemas en producción.
b) Protección de Datos de Prueba: Los datos de prueba de las aplicaciones informáticas deben ser cuidadosamente seleccionados, protegidos y controlados.

6.5. Control de acceso al Código Fuente de la aplicación informática

a) Se debe limitar y controlar el acceso al código fuente de las aplicaciones informáticas o programas.
b) Se debe contar con un responsable del acceso al código fuente de las aplicaciones informáticas, quien deberá implementar un registro de uso, si es que el código es requerido.

6.6. Uso de controles criptográficos

Se debe implementar el uso de controles para cifrar la información y proteger la confidencialidad, autenticidad e integridad de la misma, cuando sea requerido, y de acuerdo al nivel de exposición al riesgo.

6.7. Seguridad en los procesos de desarrollo y pase a producción

a) Procedimiento para el desarrollo de las aplicaciones informáticas:

Todo el desarrollo y mantenimiento de las aplicaciones informáticas en el MIMP debe ser ejecutado en el marco de los procedimientos establecidos, debiendo considerarse como mínimo las siguientes etapas:

1. Fase de análisis.
2. Fase de diseño.
3. Fase construcción.
4. Fase de implantación y aceptación.
5. Fase de elaboración de documentación técnica y de usuario.

b) Procedimiento para pase a producción:

1. El personal encargado del desarrollo y mantenimiento de las aplicaciones informáticas, así como los terceros, no tendrán acceso a los datos de producción. Los datos sensibles con los que trabajen deben ser diferentes a los datos del ambiente de producción.
2. Los ambientes de desarrollo y producción deben ser configurados en servidores diferentes, limitando el acceso solo al personal autorizado.
3. El pase a producción debe ser realizado exclusivamente por la persona autorizada por la Dirección de la Oficina de Tecnologías de la Información o la dependencia competente de los programas nacionales, quien llevará un control de los pases efectuados y/o actualizaciones de las aplicaciones informáticas en un registro o bitácora.

4. Todo desarrollo, previo a su pase a producción, debe ser revisado por la Oficina de Tecnologías de la Información o la dependencia competente de los programas nacionales, para asegurar que se cumplan los estándares establecidos por la citada oficina.

c) Análisis de requerimientos de aplicaciones:
Se deben establecer los requerimientos referidos a arquitectura, tecnología necesaria, seguridad y otros requerimientos especiales.

6.8. Control de cambios de las aplicaciones

a) El control, registro y monitoreo de los cambios de las aplicaciones informáticas del MIMP debe ser supervisado y registrado por la Oficina de Tecnologías de la Información o la dependencia competente de los programas nacionales.
b) El proceso de control de cambios debe considerar:
    1. Planificación del cambio.
    2. Responsabilidades y canales de comunicación.
    3. Identificación de los recursos comprometidos.
    4. Pruebas de comprobación y estrés, controles de seguridad y reversión en ambiente de desarrollo.
    5. Análisis de impacto.
    6. Registro documentado de los cambios.
    7. Acta de conformidad de puesta en producción.
c) Todo acceso a la librería de los programas fuente será controlado por la Oficina de Tecnologías de la Información o la dependencia competente de los programas nacionales para evitar accesos y/o cambios no autorizados.
d) Todo cambio efectuado en las aplicaciones informáticas del MIMP deberá ser documentado, contar con un registro de los cambios efectuados y ser archivado por la Oficina de Tecnologías de la Información o la dependencia competente de los programas nacionales, según corresponda.

6.9. Gestión de vulnerabilidades técnicas

a) La Oficina de Tecnologías de la Información o la dependencia competente de los programas nacionales deben programar la realización de pruebas de comprobación técnica a cargo de especialistas externos para verificar que se han implementado correctamente los controles de seguridad definidos para el hardware y software.
b) Identificadas las vulnerabilidades técnicas se deben determinar los riesgos asociados e implementar los controles necesarios para mitigarlos. Las aplicaciones informáticas críticas y en alto riesgo deben ser tratadas primero.
c) Para la aplicación de una actualización de seguridad (parches) se debe probar y evaluar su efectividad en un ambiente de pruebas; asimismo, se deben considerar los riesgos asociados a su aplicación y, en todos los casos, se deben cumplir los controles establecidos para la gestión de cambios.

CAPÍTULO 7

POLÍTICA DE GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

7.1. Objetivos

Garantizar que los eventos y debilidades en la seguridad de la información del MIMP asociados con los sistemas de información y aplicaciones informáticas sean comunicados oportunamente a las instancias correspondientes con la finalidad de adoptar las acciones correctivas a tiempo.

7.2. Reporte de eventos y debilidades de la Seguridad de la Información

a) El colaborador del MIMP debe conocer el procedimiento de comunicación de incidentes de seguridad e informar de su ocurrencia tan pronto tome conocimiento de ellos.
b) Los incidentes relativos a la seguridad de la información deben comunicarse a la Oficina de Tecnologías de la Información o la dependencia competente de los programas nacionales y al Oficial de Seguridad de la Información, conforme al procedimiento que se establezca para tal efecto.
c) Son considerados incidentes de seguridad para el MIMP:
    1. Pérdida de disponibilidad del servicio, equipos o instalaciones (disponibilidad del servicio de TI).
    2. Sobrecargas en los sistemas (software y hardware).
    3. Errores humanos en uso de los sistemas y aplicaciones informáticas.
    4. Incumplimientos de política, normas y/o procedimientos sobre seguridad de la información.
    5. Cambios no controlados en los sistemas (software y hardware) y servicios.
    6. Fallas en software y/o hardware.
    7. Violaciones de acceso a los sistemas y aplicaciones informáticas.
    8. Ataques por software de tipo malicioso (malware).
    9. Correos fraudulentos (phishing) solicitando información del usuario.
    10. Pérdida o fuga de Información.
    11. Uso indebido del correo electrónico.
    12. Detección o explotación de vulnerabilidades de la seguridad.

7.3. Evaluación y respuesta a incidentes de seguridad de la información

Los eventos de Seguridad de la Información deben ser evaluados y decidirse si son clasificados como incidentes de Seguridad de la Información.

7.4. Aprendizaje de los incidentes de seguridad de la información

El Oficial de Seguridad de la Información debe analizar exhaustivamente los incidentes de Seguridad de la Información y adoptar las acciones para reducir la probabilidad o el impacto de incidentes futuros.