Resolución Ministerial

Lima, 18 DIC. 2013

Nº 274-2013-MIDIS

VISTO:

El Memorando N° 575-2013-MIDIS/SG/OGTI, emitido por la Oficina General de Tecnologías de la Información del Ministerio de Desarrollo e Inclusión Social;

CONSIDERANDO:

Que, mediante Ley N° 29792, se creó el Ministerio de Desarrollo e Inclusión Social, determinándose su ámbito, competencias, funciones y estructura orgánica básica;

Que, mediante Resolución N° 042-2008-INDECOPI-CNB, se aprobó la Norma Técnica Peruana "NTP-ISO/IEC 27001:2008 EDI Tecnología de la Información. Técnicas de seguridad. Sistemas de gestión de seguridad de la información. Requisitos", la cual tiene por objeto establecer, implementar, operar, monitorear, mantener y mejorar un efectivo Sistema de Gestión de Seguridad de la Información en las organizaciones, lo cual incluye la aprobación de una Política de Seguridad de la Información que dirija y brinde soporte a la gestión de la seguridad de la información, en concordancia con los requerimientos de la organización y la normativa vigente;

Que, mediante Resolución Ministerial N° 129-2012-PCM, se aprobó el uso obligatorio de la Norma Técnica Peruana "NTP-ISO/IEC 27001:2008 EDI Tecnología de la Información. Técnicas de seguridad. Sistemas de gestión de seguridad de la información. Requisitos", en todas las entidades públicas integrantes del Sistema Nacional de Informática;

Que, mediante el documento de Visto, la Oficina General de Tecnologías de la Información, de acuerdo con las funciones y competencias establecidas en el artículo 33 del Reglamento de Organización y Funciones del Ministerio de Desarrollo e Inclusión Social, aprobado por Decreto Supremo N° 011-2012-MIDIS, propone la aprobación de las Políticas de Seguridad de la Información del Ministerio de Desarrollo e Inclusión Social, para su aplicación por parte de todas las unidades ejecutoras que conforman el Pliego 040: Ministerio de Desarrollo e Inclusión Social;

Que, según lo indicado por la precitada oficina general, las referidas políticas tienen por objetivo lograr un nivel razonable de seguridad de la información del Ministerio, garantizando su confidencialidad, integridad y disponibilidad, en forma eficiente y eficaz;

Que, en mérito a las consideraciones expuestas, se estima procedente aprobar las Políticas de Seguridad de la Información del Ministerio de Desarrollo e Inclusión Social propuestas por la Oficina General de Tecnologías de la Información, según los fundamentos expresados en el documento de Visto; y,

De conformidad con lo dispuesto por la Resolución Ministerial N° 129-2012-PCM; la Norma Técnica Peruana "NTP-ISO/IEC 27001:2008 EDI Tecnología de la Información. Técnicas de seguridad. Sistemas de gestión de seguridad de la información. Requisitos", aprobada por Resolución N° 042-2008-INDECOPI-CNB; la Ley N° 29158, Ley Orgánica del Poder Ejecutivo; la Ley Nº 29792, Ley de Creación, Organización y Funciones del Ministerio de Desarrollo e Inclusión Social; y su Reglamento de Organización y Funciones, aprobado por Decreto Supremo Nº 011-2012-MIDIS;

SE RESUELVE:

Artículo 1.- Aprobación de las Políticas de Seguridad de la Información del Ministerio de Desarrollo e Inclusión Social

Aprobar las Políticas de Seguridad de la Información del Ministerio de Desarrollo e Inclusión Social, conforme al anexo que forma parte integrante de la presente resolución.

Artículo 2.- Difusión

Disponer la publicación de la presente resolución y su anexo en el Portal Institucional del Ministerio de Desarrollo e Inclusión Social (www.midis.gob.pe).

Artículo 3.- Vigencia

Las Políticas de Seguridad de la Información del Ministerio de Desarrollo e Inclusión Social aprobadas por la presente resolución entrarán en vigencia a partir del día siguiente de su publicación en el Portal Institucional del Ministerio de Desarrollo e Inclusión Social.

Regístrese y comuníquese.

Mónica Rubio García
MINISTRA DE DESARROLLO E INCLUSIÓN SOCIAL

PERÚ | Ministerio de Desarrollo e Inclusión Social

POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN DEL MINISTERIO DE DESARROLLO E INCLUSIÓN SOCIAL

MIDIS
Oficina General de Tecnologías de la Información

Noviembre, 2013.

POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN DEL MINISTERIO DE DESARROLLO E INCLUSIÓN SOCIAL

CONTENIDO

MIDIS Oficina General de Tecnologías de la Información

ENUNCIADO DE LAS POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

El Ministerio de Desarrollo e Inclusión Social - MIDIS es un organismo del Poder Ejecutivo cuyo objetivo principal es mejorar la calidad de vida de la población en situación de vulnerabilidad y pobreza, promover el ejercicio de sus derechos, el acceso a oportunidades y el desarrollo de sus propias capacidades. A tal efecto, gestiona, en forma responsable, la seguridad de la información relacionada con sus actividades, metas y programas, en concordancia con la normatividad vigente[1] y los siguientes lineamientos:

- El establecimiento de mecanismos para preservar la confidencialidad, integridad y disponibilidad de la información de la institución, garantizando su transparencia.
- La continua identificación, manejo y mitigación de los riesgos de seguridad de la información que son relevantes para la institución.
- La respuesta efectiva y adopción de acciones correctivas ante incidentes relacionados con la seguridad de la información.
- La comunicación oportuna de las políticas y procedimientos de seguridad definidos, asegurando que sean comprendidos y se encuentren disponibles para todos los interesados.
- El fortalecimiento de los valores y el compromiso de todo el personal de velar por el cumplimiento de las presentes políticas.

MIDIS Oficina General de Tecnologías de la Información

[1] Resolución Ministerial N° 129-2012-PCM, que dispuso el uso obligatorio de la Norma Técnica Peruana "NTP-ISO/IEC 27001:2008 EDI Tecnología de Información. Técnicas de seguridad. Sistemas de gestión de seguridad de la información. Requisitos" en todas las entidades integrantes del Sistema Nacional de Informática.

CAPÍTULO 1
GENERALIDADES

1.1 Introducción

Las Políticas de Seguridad de la Información del Ministerio de Desarrollo e Inclusión Social han sido elaboradas tomando como marco de referencia la Norma Internacional ISO 27001:2005, y la Norma Técnica Peruana NTP-ISO/IEC 27001:2008 "EDI Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos", aprobada por Resolución N° 042-2008-INDECOPI-CNB, cuya finalidad principal es asegurar la confidencialidad, integridad y disponibilidad de la información gestionada en la Institución.

Las Políticas de Seguridad de la Información identifican responsabilidades y establecen los objetivos para una protección apropiada y consistente de los activos de información del Ministerio de Desarrollo e Inclusión Social, en adelante MIDIS.

1.2 Alcance

1.2.1 Las presentes políticas tienen alcance a todas las unidades ejecutoras que conforman el Pliego MIDIS, involucrando a todos los funcionarios, trabajadores y terceros que tengan acceso o que desarrollen, adquieran o usen sistemas de información, aplicaciones informáticas y/o datos del MIDIS.

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

1.2.3 En cuanto a las relaciones jurídicas que el MIDIS mantenga con terceros, el presente documento y las disposiciones que en materia de seguridad de la información apruebe el MIDIS, comprenden la información creada por ellos (los terceros), así como la información propia del Ministerio que se les haya otorgado en el marco de dichas relaciones jurídicas.

1.2.4 El presente documento comprende las siguientes políticas específicas:

- Política de seguridad de la información.
- Política de gestión de comunicaciones y operaciones.
- Política de control de accesos.
- Política de adquisición, desarrollo y mantenimiento de aplicaciones informáticas.
- Política de gestión de incidentes.

1.3 Objetivo

Las Políticas de Seguridad de la Información tienen por objetivo proteger los recursos de información del MIDIS 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 el cumplimiento de la confidencialidad, integridad y disponibilidad de la información, así como garantizar la continuidad de los sistemas de información. Asimismo, las Políticas de Seguridad de la Información deben constituirse en parte de la cultura organizacional del MIDIS, para lo cual se debe asegurar un compromiso manifiesto de los funcionarios del Ministerio, para la difusión, consolidación y cumplimiento de las presentes Políticas.

1.4 Definiciones

Para los fines de las presentes Políticas, se establecen las siguientes definiciones:

a) **Activo:** Todo aquello que presenta valor para la institución, tal como:

- Información;
- Software, como un programa de computadora;
- Físicos, como una computadora;
- Servicios;
- Personas y sus calificaciones, habilidades y experiencia;
- Intangibles, como reputación o imagen.

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 aquél 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 Ministerio, 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 intencionadas. Ello incluye los elementos que garantizan su procedencia o autenticidad. También se aplica a los equipos y a las personas.

i) **MIDIS:** Comprende todas las unidades ejecutoras que conforman el Pliego Ministerio de Desarrollo e Inclusión Social.

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:** Trabajador del MIDIS, con prescindencia de su nivel o jerarquía, autorizado a utilizar un sistema de información determinado, bajo un nivel de acceso pre-establecido.

n) **Política de Seguridad de la Información en el MIDIS:** Conjunto de principios o lineamientos generales, cuya implementación está orientada a asegurar la confiabilidad, integridad y disponibilidad de la información del Ministerio. Como documento dinámico del MIDIS, debe seguir un proceso de actualización periódica sujeto a los cambios organizacionales relevantes, tales como cambio en la infraestructura tecnológica, alta rotación del personal, desarrollo de nuevos servicios, etc.

Los principales beneficios de la implementación de la referida Política son:

- Contribuir a efectivizar el manejo del riesgo.
- Priorizar el valor de la Información.
- Estandarizar los controles y revisiones de los sistemas de información y aplicaciones informáticas.
- Establecer bases referenciales para el desarrollo de estrategias y planes referidos a la seguridad de la información.
- Brindar un entorno de trabajo seguro a los usuarios.
- Cumplir con los requerimientos regulatorios y legales pertinentes.

1.5. Responsabilidades Generales

1.5.1 Comité de Gestión de Seguridad de la Información del MIDIS:

El Comité de Gestión de Seguridad de la Información del MIDIS vela por la existencia y cumplimiento de las medidas de seguridad de la información del Ministerio, salvo en materia informática, en concordancia con el rol de la Institución y los recursos disponibles.

1.5.1.1 Conformación del Comité de Gestión de Seguridad de la Información del MIDIS:

El Comité de Gestión de Seguridad de la Información del MIDIS está conformado de la siguiente manera:

- El (la) Secretario(a) General o su representante, quien lo presidirá;
- El (la) Jefe(a) de la Oficina General de Tecnologías de la Información, quien será el (la) Secretario(a) Técnico(a) del Comité;
- El (la) Jefe(a) de la Oficina General de Planeamiento y Presupuesto;
- El (la) Jefe(a) de la Oficina General de Administración;
- Un representante del Despacho Viceministerial de Políticas y Evaluación Social;
- Un representante del Despacho Viceministerial de Prestaciones Sociales; y,
- El Oficial de Seguridad de la Información.

MIDIS Oficina General de Tecnologías de la Información

1.5.1.2 Funciones y responsabilidades del Comité de Gestión de Seguridad de la Información del MIDIS:

a) Asegurar que las metas sobre seguridad de la información sean identificadas, relacionarlas con las exigencias institucionales y que sean integradas en procesos relevantes.
b) Revisar periódicamente las Políticas de Seguridad de la Información, para su adecuación a la normatividad vigente y aprobación por el Titular del MIDIS.
c) Supervisar la implementación y efectividad de las Políticas de Seguridad de la Información.
d) Proveer lineamientos claros y un visible apoyo en la gestión para iniciativas de seguridad de la información.

e) Proponer planes y programas de capacitación para sensibilizar al personal del MIDIS en materia de seguridad de la información.
f) Adoptar acciones administrativas orientadas a garantizar la seguridad de la información del MIDIS, en coordinación con las dependencias competentes.
g) Aprobar los roles y responsabilidades específicas para la seguridad de la información en toda la organización.
h) Proponer directivas sectoriales sobre la gestión y uso de los recursos informáticos; sobre el uso del internet y del correo electrónico institucional; y acerca del almacenamiento y respaldo de la información; para su aplicación por parte de todas las unidades ejecutoras que conforman el Pliego MIDIS.

1.5.1.3 Funciones Específicas del Presidente del Comité de Gestión de Seguridad de la Información del MIDIS:

El Presidente del Comité de Gestión de Seguridad de la Información del MIDIS asume las siguientes funciones:

a) Mantener una agenda actualizada sobre los temas de seguridad de la información que deba abordar el Comité de Gestión de Seguridad de la Información del MIDIS.
b) Coordinar y fijar las fechas para las sesiones del Comité.
c) Revisar y aprobar las Actas del Comité, previa rúbrica de sus integrantes.
d) Conducir y moderar las sesiones del Comité.

1.5.1.4 Funciones Específicas del Secretario Técnico del Comité de Gestión de Seguridad de la Información del MIDIS:

El Secretario Técnico del Comité de Gestión de Seguridad de la información del MIDIS asume las siguientes funciones:

a) Realizar las convocatorias para las sesiones del Comité (ordinarias y extraordinarias) conforme al calendario que disponga el Presidente.
b) Redactar las Actas de las sesiones y dar lectura de las mismas ante los integrantes del Comité.
c) Conservar las Actas y la documentación de todas las actuaciones del Comité.

1.5.1.5 Funcionamiento del Comité de Gestión de Seguridad de la Información del MIDIS:

a) Acerca de las sesiones del Comité:

a.1) Las fechas para las sesiones del Comité serán fijadas por el Presidente del Comité, ya sean de carácter ordinario o extraordinario. Se aplicará la siguiente pauta de convocatoria:

- Para las sesiones ordinarias: Se celebrarán en forma bimensual, previa convocatoria del Presidente con siete (7) días de anticipación. Esta reunión se celebra en forma rutinaria, por lo que la convocatoria sólo constituye una confirmación de fecha, lugar y hora.
- Para las sesiones extraordinarias: Se celebrarán por libre decisión del Presidente del Comité o a solicitud de uno o más de sus integrantes. Las convocatorias para las sesiones extraordinarias deberán realizarse con el mayor tiempo de anticipación posible, según la urgencia del asunto a tratar.

a.2) Las convocatorias para las sesiones ordinarias y extraordinarias podrán realizarse por escrito o por correo electrónico, debiendo indicarse el lugar, día y hora de la sesión, y el asunto a tratar en ella.

a.3) Por cada sesión se levantará un Acta, la cual será elaborada por el Secretario Técnico del Comité.

b) Acerca de los acuerdos del Comité:
Los acuerdos adoptados en cada sesión quedarán reflejados en las respectivas Actas. Para adoptar el carácter de acuerdos válidos, las actas serán leídas por el Secretario Técnico al final de la sesión y se considerarán aprobadas con su suscripción por parte de todos los integrantes del Comité, creándose el registro necesario. En caso que un integrante del Comité haya sido reemplazado por inasistencia, la persona que lo representó en la sesión deberá informarle sobre los acuerdos adoptados.

1.5.2 Responsable de Seguridad de la Información:

Es el representante designado como Oficial de Seguridad de la Información del MIDIS, de acuerdo con lo dispuesto por la Resolución Ministerial N° 129-2012-PCM. Se encuentra encargado de definir y aplicar los criterios de Seguridad de la Información en el Ministerio de Desarrollo e Inclusión Social, en base a la Norma Técnica Peruana NTP-ISO/IEC 27001:2008 "EDI Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos", aprobada por Resolución N° 042-2008-INDECOPI-CNB. Cumple las siguientes funciones:

a) Establecer y aplicar una metodología de análisis de riesgo, en función de los lineamientos establecidos por el Comité de Gestión de Seguridad de la Información.
b) Proponer ante el Comité de Gestión de Seguridad de la Información las modificaciones de las Políticas de Seguridad de la Información del MIDIS, de resultar necesarias.
c) Definir procedimientos para la aplicación de políticas de seguridad informática.
d) Coordinar con todas las Direcciones, Oficinas y Programas del MIDIS, en temas relacionados con la Seguridad de la Información.
e) Promover la aplicación de auditorías enfocadas en la seguridad, para evaluar las prácticas de Seguridad de la Información en el MIDIS.
f) Informar regularmente a los trabajadores/colaboradores del MIDIS acerca de los objetivos, medidas y reglamentaciones en materia de seguridad de la información que se encuentren en vigencia.

1.5.3 Personal del MIDIS:

A efectos de las presentes políticas, comprende a todas aquellas personas que prestan servicios al MIDIS, independientemente de su régimen laboral o contractual.
El personal del MIDIS tiene la responsabilidad de cumplir con lo establecido en este documento y de aplicarlo en el entorno en el que desempeña sus funciones. Además, tiene 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 esta política o pueda poner en riesgo la seguridad de la información del Ministerio.

1.5.3.1 Funcionarios:

Se refiere a quienes ostentan la titularidad de los programas sociales, órganos y unidades orgánicas del MIDIS, independientemente de su régimen laboral o contractual.
Los Funcionarios del MIDIS 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) Supervisar periódicamente su ámbito de acción a fin de detectar posibles deficiencias en materia de seguridad de la información.
b) Iniciar rápidamente medidas correctivas e informar al Comité de Gestión de Seguridad de Información y/u Oficina General de Tecnologías de la

Información, o la dependencia competente del programa, según corresponda, acerca de las deficiencias y demás incidentes de carácter relevante.

c) 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 hayan sido puesta en su conocimiento conforme a la normativa vigente.
d) Asegurar los niveles de confidencialidad de la información bajo su ámbito, verificando que las reglamentaciones operativas sean debidamente cumplidas.
e) Definir al personal bajo su cargo que tendrá acceso a la información, a los sistemas de información y aplicaciones informáticas del MIDIS, cuando corresponda.
f) Formular al Comité de Gestión de Seguridad de Información las recomendaciones que considere pertinentes.
g) Designar a los trabajadores que se encargarán de apoyar en la difusión de la presentes políticas y su regulación complementaria.
h) Coordinar la activación de planes de contingencia ante eventuales caídas de los sistemas de información, a efectos de asegurar la continuidad de las actividades a su cargo.

1.5.3.2 Empleados:

Comprende a todas las personas que prestan servicios al MIDIS, distintas de los funcionarios, independientemente de su régimen laboral o contractual.

Todos los empleados del MIDIS deberán garantizar activamente la protección de la información. Ello implica:

a) La utilización de la información y de los sistemas de información, aplicaciones informáticas, solo para el cumplimiento de sus funciones.
b) El cuidadoso manejo de la información y de los sistemas de información, especialmente si se trata de información confidencial, asegurando su no divulgación.
c) Observar las reglamentaciones y cumplir cabalmente los procedimientos y estándares en cuanto a la seguridad en materia de información.
d) Informar a los titulares de los programas sociales, 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 caídas de los sistemas de información y aplicaciones informáticas.

1.5.3.3 Propietario de la Información:

Para los fines de las presentes Políticas, es el responsable de la información y de los procesos que la manipulan, sean manuales, mecánicos o electrónicos. El término "propietario" no significa que la persona tiene algún derecho de propiedad real sobre el activo.

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

1.6. Sanciones por incumplimiento

El incumplimiento de las presentes Políticas, dará lugar a la aplicación de las sanciones correspondientes, de conformidad con la normativa vigente, sin perjuicio de las responsabilidades civiles y/o penales que pudieran corresponder.

CAPÍTULO 2
POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

2.1. Objetivos

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

2.2. Política

a) Adhesión a la Política:
   (i) La presente política y procedimientos asociados deben ser cumplidos por todo el personal del MIDIS, sin excepción.
   (ii) El Comité de Gestión de Seguridad de la Información debe monitorear el cumplimiento de la presente política, reportando los resultados al Titular del Ministerio, al menos trimestralmente.

b) Gestión de Riesgos:
   (i) El Oficial de Seguridad de la Información del MIDIS asume las siguientes funciones:
      - Apoya a las dependencias del MIDIS 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 Jefe de la Oficina General de Tecnologías de la Información, o de la dependencia competente del programa, 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 MIDIS.
   (ii) El Comité de Gestión de Seguridad de la Información del MIDIS aprueba la metodología y los resultados de la evaluación de riesgos.

c) Protección de la información:
   (i) El MIDIS reconoce que la seguridad de la información es un objetivo institucional que debe ser impulsado y apoyado por todo su personal.
   (ii) 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.

d) Clasificación de la información:
   (i) Los activos de información deben ser clasificados de acuerdo con el grado de importancia para la Institución, determinada según su sensibilidad y criticidad.

(ii) Toda información se considera pública, con 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.

e) Uso de activos de información:

(i) Los activos de información debe ser usados para los fines y objetivos del MIDIS, de acuerdo con las políticas, directivas y procedimientos que se definan, y considerando criterios de buen uso.

(ii) En el marco de las relaciones que el MIDIS 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.

(iii) Se debe cumplir con los requisitos legales, contractuales y normativos relativos al uso de activos de información, incluyendo las políticas de seguridad que deben mantenerse alineadas con la normatividad vigente.

(iv) Se deben guardar reserva y/o proteger los elementos de control de acceso, como contraseñas y tarjetas de identificación, según corresponda.

MIDIS Oficina General de Tecnologías de la Información

CAPÍTULO 3
POLÍTICA DE GESTIÓN DE COMUNICACIONES Y OPERACIONES

3.1. Objetivo

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

3.2. Política

Las actividades de gestión sobre los recursos de tecnología de información del MIDIS son esenciales para el buen funcionamiento de los servicios de la Institución. Para tales efectos, deben considerarse los siguientes lineamientos:

a) Responsabilidades de operación:
La Jefatura de la Oficina General de Tecnologías de la Información, o de la dependencia competente del programa, deberá asegurar la existencia de documentación formal de sus procedimientos operativos, estableciendo las responsabilidades y los recursos utilizados para su ejecución eficiente.

b) Gestión de cambios:
(i) La Oficina General de Tecnologías de la Información, o la dependencia competente del programa, deberá 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.
(ii) Todos los cambios deben ser solicitados a la Jefatura de la Oficina General de Tecnologías de la Información, o de la dependencia competente del programa, 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.

c) Segregación de tareas:
Se 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 del MIDIS.

d) Separación de los recursos para desarrollo y producción:
(i) Se deben separar los recursos de prueba, desarrollo y producción, implementando los controles necesarios. Asimismo, se debe definir y documentar el procedimiento para pases de desarrollo a producción.
(ii) El entorno de pruebas debe ser, en lo posible, igual al ambiente de producción, en lo referido a recursos de tecnología de información.
(iii) No se deben utilizar datos que contengan información personal u otra de carácter sensible en el ambiente de pruebas.

e) Gestión y niveles de servicios externos:
   (i) Se debe 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.
   (ii) Todos los servicios provistos por terceros deben ser monitoreados, revisados y auditados regularmente.
   (iii) Los cambios en los servicios que proveen terceros deben ser planificados y autorizados, considerando los riesgos que podrían generar, en el marco de la normativa aplicable.

f) Planificación y aceptación de los sistemas de información y aplicaciones informáticas:
   (i) La Oficina General de Tecnologías de la Información, o la dependencia competente del programa, debe supervisar la planificación de capacidades de los sistemas en operación y proyectará las futuras demandas, a fin de garantizar un procesamiento y almacenamiento adecuado.
   (ii) La Oficina General de Tecnologías de la Información, o la dependencia competente del programa, debe 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.

g) Protección contra software malicioso:
   (i) La Oficina General de Tecnologías de la Información, o la dependencia competente del programa, deberá adoptar las medidas necesarias para la prevención, detección y eliminación de código malicioso (malware) a nivel de servidores de red, computadores portátiles, estaciones de trabajo, tabletas y smartphones.
   (ii) La Oficina General de Tecnologías de la Información, o la dependencia competente del programa, debe 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).
   (iii) La Oficina General de Tecnologías de la Información, o la dependencia competente del programa, es responsable de la renovación de licencias de software, y deberá definir su cronograma de renovación, para evitar que se produzca incumplimiento de uso legal de software.
   (iv) El software utilizado por el MIDIS debe ser autorizado en forma expresa por la Oficina General de Tecnologías de la Información, o la dependencia competente del programa, de corresponder.
   (v) El usuario final no debe ser facultado para deshabilitar los sistemas de control y prevención de malware.
   (vi) Los equipos portátiles (laptops y/o tabletas) que, por motivos laborales o en razón del servicio contratado, según corresponda, sean autorizados a ingresar en la red del MIDIS, deben ser revisados por el personal de soporte técnico de la Oficina General de Tecnologías de la Información, o la dependencia competente del programa, verificando que tengan instalado software antivirus actualizado, sistema operativo actualizado y que no exista algún software instalado que implique un riesgo de seguridad.
   (vii) El personal de soporte técnico de la Oficina General de Tecnologías de la Información, o de la dependencia competente del programa, como medida de prevención, si detecta que algún servidor de red, estación de trabajo o computadora portátil está infectada con algún tipo de malware, deberá de aislarla inmediatamente, desconectándola de la red del MIDIS.

h) Gestión interna de respaldo y recuperación:
   (i) La Oficina General de Tecnologías de la Información, o la dependencia competente del programa, deberá 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.
   (ii) Las copias de seguridad deben resguardarse en un ambiente distinto al de la institución (es decir, fuera de las instalaciones de la entidad), que reúna las condiciones adecuadas de acondicionamiento, temperatura y humedad. Asimismo, los equipos y los medios de respaldo deben estar a una distancia de seguridad conveniente para evitar que se dañen por un desastre en el Data Center.
   (iii) Los equipos y los medios de respaldo deben contar con un programa de mantenimiento preventivo y correctivo para asegurar su correcto funcionamiento.
   (iv) La Oficina General de Tecnologías de la Información, o la dependencia competente del programa, debe 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.
   (v) El personal de soporte técnico debe 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.
   (vi) Se deben programar y realizar pruebas de recuperación de las copias de respaldo.
   (vii) Se debe revisar periódicamente la vigencia tecnológica de los equipos y software utilizados para el respaldo y recuperación de la información.

i) Diseño de la infraestructura de seguridad:
   La Oficina General de Tecnologías de la Información, o la dependencia competente del programa, debe implantar 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:

   (i) Implementación de un esquema de segmentación de redes.
   (ii) El desarrollo de procedimientos para la gestión remota de los recursos de tecnología de información de manera segura.
   (iii) Registro y monitoreo de las acciones de seguridad relevantes.
   (iv) Coordinación de las actividades de gestión para optimizar el servicio y para asegurar que los controles se apliquen adecuadamente a través de toda la infraestructura de procesamiento de la información.
   (v) Se deben establecer controles y medidas especiales para salvaguardar la confidencialidad e integridad de los datos que se transfieran a través de redes públicas, así como para proteger los sistemas conectados, tales como firewall, utm, filtro de contenidos, antispam, entre otros.

j) Buen uso de los medios de almacenamiento:
   (i) Con la finalidad de prevenir daños a los recursos e interrupciones a las actividades del MIDIS, se deberá contar con mecanismos de seguridad que garanticen que los medios sean controlados y físicamente protegidos.
   (ii) Se deben implementar controles que aseguren que todos los medios de almacenamiento que contengan información sensible sean almacenados, protegidos contra el acceso no autorizado y eliminados de manera segura y efectiva.

k) Uso adecuado de los recursos y servicios informáticos:
   (i) Los recursos y servicios informáticos asignados al personal del MIDIS son de uso exclusivo para las funciones encomendadas. Está prohibido su uso para actividades que no formen parte de sus labores.
   (ii) El personal que haga uso de los servicios y recursos de tecnología de información del MIDIS, debe cumplir los reglamentos, directivas, procedimientos e instructivos aprobados sobre la materia.

l) Seguridad del correo electrónico:
   (i) El MIDIS se reserva el derecho de deshabilitar una cuenta de correo electrónico por algún uso indebido que transgreda lo establecido en el presente documento.
   (ii) Cada persona es responsable por la información que se transmita desde la cuenta de correo electrónico que le haya asignado la institución.
   (iii) En caso de recibir mensajes con asuntos sospechosos y/o de origen desconocido, estos deben ser eliminados sin abrir el contenido, y comunicados a la Oficina General de Tecnologías de Información o a la dependencia competente del programa, según corresponda, así como al Oficial de Seguridad de la Información, para los fines correspondientes.
   (iv) El personal debe usar firmas estandarizadas, de conformidad con el Manual de Identidad Corporativa del MIDIS.
   (v) El envío de mensajes masivos de correo electrónico está permitido solo para el personal o dependencias del MIDIS que lo requieran como parte de sus funciones. Debe ser autorizado por el superior inmediato y habilitado por la Oficina General de Tecnologías de la Información, o la dependencia competente del programa.
   (vi) Solo por mandato judicial o con autorización expresa de la persona a la que se hubiera asignado una cuenta de correo institucional, el MIDIS podrá acceder al contenido de los mensajes enviados y/o recibidos desde dicha cuenta, y por motivos debidamente justificados.

m) Registros de auditoría y monitoreo:
   (i) Todos los servicios informáticos se encuentran sujetos a monitoreo por parte de la Oficina General de Tecnologías de la Información, o la dependencia competente del programa.
   (ii) Deben generarse registros de auditoría sobre el uso de los recursos de tecnología de información.
   (iii) Las actividades de operadores y administradores de los sistemas deben ser monitoreadas, registradas y verificadas regularmente.
   (iv) Se debe contar con registro de fallas en los sistemas, para asegurar que han sido corregidas oportunamente.
   (v) Los registros de auditoría y monitoreo deben ser respaldados.
   (vi) Cada persona es responsable de todas las actividades realizadas a través de sus cuentas de acceso a red, correo electrónico, sistemas de información asociados y aplicaciones informáticas.

MIDIS Oficina General de Tecnologías de la Información

CAPÍTULO 4
POLÍTICA DE CONTROL DE ACCESOS

4.1. Objetivos

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

4.2. Política

Para el acceso a los distintos activos de información del MIDIS, se establecen los siguientes lineamientos generales:

a) Requerimientos para el control de accesos:
Todos los accesos a los recursos de información del MIDIS deben basarse en la necesidad y rol del usuario, debiendo tomarse 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.
- Coherencia entre las políticas de control de accesos y las políticas de clasificación de la información.
- Uso de perfiles de usuarios estandarizados definidos según roles.
- Revisión periódica de los controles de acceso.
- Revocación de los derechos de acceso.

b) Gestión de acceso del personal:
(i) 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.
(ii) Los funcionarios 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 de Recursos Humanos, o la que haga sus veces en los programas, informará a la OGTI, o a la dependencia competente del programa, sobre los ceses de los trabajadores a efectos de la respectiva eliminación de accesos.
(iii) La Oficina General de Tecnologías de la Información, o la dependencia competente del programa, debe asignar un identificador (cuenta) único y exclusivo a toda persona que haga uso de los recursos informáticos, ya sea de forma temporal o permanente.
(iv) 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.
(v) La Oficina General de Tecnologías de la Información, o la dependencia competente del programa, debe 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 8 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 debe usar las contraseñas usadas en el MIDIS para sistemas externos (por ejemplo, correo personal).

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

(vii) 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.

(viii) El personal debe 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.

c) Control de acceso a las redes informáticas:

(i) El acceso a los recursos de red, internos y externos, debe ser controlado por la Oficina General de Tecnologías de la Información, o la dependencia competente del programa, de manera que el personal no comprometa la seguridad de los activos de información.

(ii) 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 políticas.
- Controles de enrutamiento de redes.
- Seguridad en los servicios de red.

d) Control de acceso a los sistemas operativos:

(i) El acceso a los sistemas operativos de las estaciones de trabajo del MIDIS debe ser debidamente controlado por la Oficina General de Tecnologías de la Información, o por la dependencia competente del programa, a fin de evitar accesos no autorizados a recursos o información.

(ii) 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.
- Desconexión automática de computadoras por tiempo de inactividad.
- Limitación de horarios y tiempo de conexión.

e) Control de acceso a las aplicaciones:

(i) La Oficina General de Tecnologías de la Información, o la dependencia competente del programa, debe establecer los lineamientos de control de accesos a la información y a las aplicaciones, restringiéndolas solo para el personal debidamente autorizado; asimismo, revisa periódicamente los accesos concedidos, revocando los derechos cuya vigencia de autorización haya caducado.

(ii) Se deben aislar los sistemas identificados con información sensible, asignándoles un entorno de procesamiento dedicado, creado a partir de métodos físicos o lógicos.

f) Conexiones externas:

(i) Las unidades ejecutoras del MIDIS deben establecer e implementar normas y procedimientos relativos a las actividades de teletrabajo o trabajo remoto, en concordancia con lo establecido en la Ley N° 30036, Ley que regula el teletrabajo, y normas complementarias, previa opinión favorable del Comité de Gestión de Seguridad de la Información. Las referidas normas deberán definir las horas de acceso, el tipo de información que el teletrabajador podrá utilizar, los sistemas y servicios internos a los que estará autorizado a acceder, y el periodo de autorización de los accesos, entre otros.

(ii) Las actividades de teletrabajo deben ser autorizadas por la Oficina General de Administración, o la dependencia competente de los programas, con sujeción a la normativa aplicable.

(iii) En cualquier caso, para el acceso remoto (todo acceso a la información del MIDIS fuera del centro de trabajo) se debe utilizar la tecnología y acceso seguro (SSL-VPN) y su uso debe ser autorizado por el Comité de Gestión de Seguridad de la Información.

CAPÍTULO 5
POLÍTICA DE ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE APLICACIONES INFORMÁTICAS

5.1. Objetivos

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

5.2. Política

a) Metodología para la adquisición, desarrollo y mantenimiento de las aplicaciones informáticas:
   (i) El MIDIS debe aprobar una metodología sectorial estandarizada para la adquisición, desarrollo y mantenimiento de las aplicaciones informáticas.
   (ii) Todo desarrollo y/o mantenimiento de aplicaciones informáticas deberá ser documentado, con la finalidad de que personas no familiarizadas con ellas en el MIDIS, ejecuten las actividades con facilidad.

b) Requisitos de seguridad de las aplicaciones informáticas:
   (i) La Oficina General de Tecnologías de la Información, o la dependencia competente de los programas, define un procedimiento que incluya controles de seguridad durante las etapas de análisis y diseño de las aplicaciones informáticas.
   (ii) Toda aplicación informática desarrollada por el personal de la Oficina General de Tecnologías de la Información, o de la que haga sus veces en los programas, o por terceros, debe 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 deben constar en el respectivo contrato de prestación de servicios.
   (iii) El personal debe cumplir los controles, estándares y metodologías referidas al desarrollo de las aplicaciones informáticas que se hayan implementado.
   (iv) La Oficina General de Tecnologías de la Información, o la dependencia competente de los programas, debe verificar que los acuerdos sobre materia informática a suscribir con terceros, incluyan cláusulas relativas a la cesión de derechos y la confidencialidad de la información, para el resguardo de la propiedad intelectual del MIDIS.
   (v) 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.
   (vi) Toda aplicación informática desarrollada por el personal es de propiedad del MIDIS.

c) Procesamiento correcto de las aplicaciones:
   (i) Se deben implementar controles de seguridad apropiados en las aplicaciones utilizadas por el MIDIS, para validar los datos de entrada, el procesamiento interno y los datos de salida.
   (ii) La validación de los datos de entrada debe tener un procedimiento que permita determinar las responsabilidades de todo el personal involucrado en el proceso de entrada de datos.

(iii) Para el control del proceso interno, se deben realizar comprobaciones del correcto funcionamiento del proceso (validación de los datos generados por la aplicación, tiempos de respuesta, funciones para cambio de datos, alertas para el procesamiento).
(iv) Deben identificarse los requerimientos para asegurar la autenticidad y la integridad de los mensajes en las aplicaciones, debiendo definirse e implementarse los controles apropiados.
(v) La validación de datos de salida debe realizarse a fin de asegurar el correcto procesamiento de la información. Asimismo, deben definirse las responsabilidades de todos los involucrados en el proceso de salida de datos.

d) Seguridad de los archivos de las aplicaciones informáticas:
Se deben implementar controles sobre lo siguiente:
(i) 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.
(ii) Protección de Datos de Prueba: Los datos de prueba de las aplicaciones informáticas deben ser cuidadosamente seleccionados, protegidos y controlados.

e) Control de acceso al Código Fuente de la aplicación informática:
(i) Se debe restringir y controlar el acceso al código fuente de las aplicaciones informáticas o programas.
(ii) 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.

f) 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.

g) Seguridad en los procesos de desarrollo y pase a producción:
(i) Procedimiento para el desarrollo de las aplicaciones informáticas:
Todo desarrollo y mantenimiento de las aplicaciones informáticas en el MIDIS debe ser realizado conforme a los procedimientos establecidos, debiendo considerarse como mínimo las siguientes etapas:
1) Fase de análisis.
2) Fase de diseño.
3) Fase de construcción.
4) Fase de implantación y aceptación.
5) Fase de elaboración de documentación técnico y de usuario.
(ii) 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 Jefatura de la Oficina General de Tecnologías de la Información, o la dependencia competente del programa, quien llevará un control de los pases efectuados y/o actualizaciones de las aplicaciones informáticas en un registro o bitácora.
4) Todo desarrollo, antes de su pase a producción, debe ser revisado por la Oficina General de Tecnologías de la Información, o la dependencia

competente del programa, para asegurar que se cumplan los estándares establecidos por dicha oficina.

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

h) Control de cambios de las aplicaciones:

(i) El control, registro y monitoreo de los cambios de las aplicaciones informáticas del MIDIS debe ser supervisado y registrado por la Oficina General de Tecnologías de la Información, o la dependencia competente del programa.

(ii) 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.

(iii) Todo acceso a la librería de los programas fuente será controlado por la Oficina General de Tecnologías de la Información, o la dependencia competente del programa, para evitar accesos y/o cambios no autorizados.

(iv) Todo cambio efectuado en las aplicaciones informáticas del MIDIS deberá ser documentado, contar con un registro de los cambios efectuados, y ser archivado por la Oficina General de Tecnologías de la Información, o la dependencia competente del programa, según corresponda.

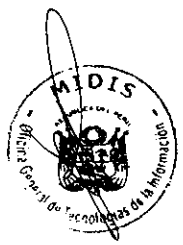
(v) La Jefatura de la Oficina General de Tecnologías de la Información, o de la dependencia competente del programa, debe efectuar revisiones periódicas de las aplicaciones informáticas en el ambiente de producción, a fin de asegurar que sólo se hayan efectuado los cambios autorizados.

i) Gestión de vulnerabilidades técnicas:

(i) La Oficina General de Tecnologías de la Información, o la dependencia competente del programa, debe 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.

(ii) 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.

(iii) 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 6
POLÍTICA DE GESTIÓN DE INCIDENTES

6.1. Objetivo

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

6.2. Política

a) Reporte de eventos y debilidades de la Seguridad de la Información:
   (i) Los incidentes relativos a la seguridad de la información deben comunicarse a la Oficina General de Tecnologías de la Información, o la dependencia competente del programa, y al Oficial de Seguridad de la Información, conforme al procedimiento que se establezca para tal efecto.
   (ii) El personal del MIDIS debe conocer el procedimiento de comunicación de incidentes de seguridad, e informar de su ocurrencia tan pronto tome conocimiento de ellos.
   (iii) Son considerados incidentes de seguridad para el MIDIS:
      1) Pérdida de 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 políticas, normas y/o procedimientos sobre seguridad de la información.
      5) ambios 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 de vulnerabilidades de la seguridad.

b) Gestión de las mejoras e incidentes en la seguridad de información:
   (i) El personal del MIDIS debe conocer su responsabilidad respecto a la comunicación de los incidentes de seguridad que tome conocimiento, debiendo ser notificados de los resultados una vez que el incidente haya sido resuelto.
   (ii) Reportados los incidentes de seguridad a la Oficina General de Tecnologías de la Información o a la dependencia competente del programa, y al Oficial de Seguridad de la Información, se debe proceder a su exhaustivo análisis por parte del personal que designe la referida oficina o dependencia del programa, a efectos de adoptar las acciones que correspondan.
   (iii) Los incidentes de seguridad serán evaluados por el Comité de Gestión de Seguridad de la Información, a efectos de proponer las acciones preventivas que correspondan, para lo sucesivo.
   (iv) El personal comprendido en el incidente de seguridad podrá ser sancionado, conforme a la normatividad vigente.
   (v) Periódicamente, la Oficina General de Tecnologías de la Información, o la dependencia competente del programa, deberá analizar las actividades realizadas y estudiar posibles mejoras o cambios que puedan proponerse al

Comité de Gestión de Seguridad de Información para prevenir la ocurrencia de futuros incidentes.