Resolución Directoral Ejecutiva

Nº020-2019 -MINEDU/VMGI-PRONIED

Lima, 28 FEB. 2019

VISTOS:

El Informe N° 113-2018-MINEDU/VMGI/PRONIED-OTI y los Memorando N°s 676-2018-MINEDU/VMGI/PRONIED-OTI, 702-2018-MINEDU/VMGI/PRONIED-OTI y 060-2019-MINEDU/VMGI/PRONIED-OTI emitidos por la Oficina de Tecnologías de la Información, el Acta de Reunión N° 001-2018 emitida por el Comité de Gestión de Seguridad de la Información, el Informe N° 568-2018-MINEDU/VMGI-PRONIED-OPP emitido por la Oficina de Planeamiento y Presupuesto y los Memorándum N°s 2462-2018-MINEDU/VMGI-PRONIED-OAJ y 140-2019-MINEDU/VMGI-PRONIED-OAJ y el Informe N° 182-2019-MINEDU/VMGI-PRONIED-OAJ emitidos por la Oficina de Asesoría Jurídica, y;

CONSIDERANDO:

Que, con Decreto Supremo N° 004-2014-MINEDU se creó el Programa Nacional de Infraestructura Educativa – PRONIED, con el objeto de ampliar, mejorar, sustituir, rehabilitar y/o construir infraestructura educativa pública de Educación Básica y de Educación Superior Pedagógica, Tecnológica y técnico – Productiva, incluyendo el mantenimiento y/o equipamiento de la misma, cuando corresponda, de manera concertada y coordinada con los otros niveles de gobierno, y en forma planificada, articulada y regulada, en el marco de las políticas sectoriales de educación en materia de infraestructura educativa, a fin de contribuir a la mejora en la calidad de la educación del país;

Que, con 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, y su modificatoria mediante Resolución Ministerial N° 166-2017-PCM;

Que, con Resolución Directoral Ejecutiva N° 091-2017-MINEDU/VMGI-PRONIED se aprobó la Política de Seguridad de Información del Programa Nacional de Infraestructura Educativa – PRONIED, la cual tenía por finalidad establecer un marco general de seguridad de la información que permita proteger los activos de información de la institución, asegurando la confidencialidad, integridad y disponibilidad de la información del PRONIED;

Que, el PRONIED cuenta con un Comité de Gestión de Seguridad de la Información (CGSI), conformado mediante Resolución Directoral Ejecutiva N° 068-2017-MNEDU/VMGI-PRONIED y modificado por Resolución Directoral Ejecutiva N° 090-2018-MINEDU/VMGI-PRONIED;

Que, el Manual de Operaciones del Programa Nacional de Infraestructura Educativa – PRONIED aprobado mediante la Resolución Ministerial N° 034-2016-MINEDU, establece en los artículos 26 y 27 que la Oficina de Tecnologías de la Información es responsable del desarrollo, implementación y mantenimiento del Software, Redes y Comunicaciones, así como del Soporte Técnico y Seguridad de la Información en el ámbito del PRONIED, y que –entre otras funciones– tiene las de dirigir, coordinar y supervisar las actividades de seguridad de la información que sirvan de apoyo a las actividades operativas y de gestión del PRONIED;

Que, con Informe N° 113-2018-MINEDU/VMGI/PRONIED-OTI, la Oficina de Tecnologías de Información informó a la Dirección Ejecutiva sobre la propuesta de actualización de la Política de Seguridad de Información del Programa Nacional de Infraestructura Educativa – PRONIED, en cumplimiento de la Resolución Ministerial N° 004-2016-PCM con la cual Aprueban 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", propuesta de actualización que fue puesta en conocimiento del Comité de Seguridad de la Información, el cual recomendó su aprobación por parte de la Dirección Ejecutiva del PRONIED, según consta en el Acta de Reunión N° 001-2018; y solicitó derogar la Resolución Directoral Ejecutiva N° 091-2017-MINEDU/VMGI-PRONIED;

Que, mediante Informe N° 568-2018-MINEDU/VMGI-PRONIED-OPP, la Oficina de Planeamiento y Presupuesto procedió a revisar la propuesta de actualización de la Política de Seguridad de la Información del PRONIED, encontrándola conforme, ya que la misma considera mejoras respecto a la Política vigente y ha sido elaborada en el marco de la Norma Técnica Peruana NTP ISO/IEC 27001:2014, emitiendo opinión favorable y recomendando su aprobación;

Que, mediante Informe N° 182-2019-MINEDU/VMGI-PRONIED-OAJ, la Oficina de Asesoría Jurídica sobre la base de lo propuesto e informado técnicamente por la Oficina de Tecnologías de la Información, respecto a la actualización de la Política de Seguridad de la Información del Programa Nacional de Infraestructura Educativa – PRONIED, la opinión técnica favorable de la Oficina de Planeamiento y Presupuesto, esta Oficina de Asesoría Jurídica, opina que es viable legalmente continuar con el trámite para la emisión del acto resolutivo de aprobación correspondiente, en cumplimiento de las disposiciones contenidas en la Resolución Ministerial N° 004-2016-PCM con la cual Aprueban 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" y su modificatoria aprobada con Resolución Ministerial N° 166-2017-PCM.

Resolución Directoral Ejecutiva

Nº 020 - 2019 -MINEDU/VMGI-PRONIED

Que, a través de la Resolución Ministerial N° 034-2016-MINEDU de fecha 13 de enero de 2016, se aprobó el Manual de Operaciones del Programa Nacional de Infraestructura Educativa – PRONIED, modificado por Resolución Ministerial N° 341-2017-MINEDU, el cual en su artículo 8 establece que la Dirección Ejecutiva es la máxima autoridad administrativa del PRONIED; responsable de su dirección y administración general. Ejerciendo su representación ante entidades públicas y privadas, la misma que está a cargo de un Director Ejecutivo;

Que, el literal b) del artículo 9 del Manual de Operaciones del Programa Nacional de Infraestructura Educativa – PRONIED, aprobado mediante Resolución Ministerial N° 034-2016-MINEDU, señala que la Directora Ejecutiva expide resoluciones directorales ejecutivas, entre otros; y,

Con la visación de la Oficina de Tecnologías de la Información, de la Oficina de Planeamiento y Presupuesto y de la Oficina de Asesoría Jurídica;

SE RESUELVE:

Artículo 1.- Dejar sin efecto, a partir de la emisión de la presente resolución, la Resolución Directoral N° 091-2018-MINEDU/VMGI-PRONIED con la cual se aprobó la "Política de Seguridad de la Información del Programa Nacional de Infraestructura – PRONIED".

Artículo 2.- Aprobar la "Política de Seguridad de la Información – Sistema de Gestión de Seguridad de la Información" del Programa Nacional de Infraestructura Educativa – PRONIED, la misma que como Anexo forma parte integrante de la presente resolución.

Artículo 3.- Encargar a la Oficina de Comunicaciones del Programa Nacional de Infraestructura Educativa – PRONIED la publicación de la presente resolución en el Portal Institucional del Programa Nacional de Infraestructura Educativa – PRONIED.

REGÍSTRESE, COMUNÍQUESE Y PUBLÍQUESE

Arq. Elizabeth Milagros Añaños Vega
Directora Ejecutiva
Programa Nacional de Infraestructura Educativa
PRONIED

020-2019

"MINISTERIO DE EDUCACIÓN"

VICEMINISTERIO DE GESTIÓN INSTITUCIONAL

PROGRAMA NACIONAL DE INFRAESTRUCTURA EDUCATIVA

POLÍTICA:

"POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN - SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN"

PERÚ

020-2019

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN – SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACION

Registro de Modificaciones			
Versión	**Fecha**	**Descripción de la modificación**	**Autor de la modificación**
1	02/05/2017	Elaboración de la Política de Seguridad de la Información	No procede
2	19/10/2018	Actualización de la Política de Seguridad de la Información	Programa Nacional de Infraestructura Educativa

020-2019

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN – SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACION

ÍNDICE

020-2019

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN – SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACION

1. FINALIDAD

Establecer los lineamientos generales, que sirvan de guía para la implementación de medidas de seguridad de la información, a partir de las cuales se busca mantener la integridad, confidencialidad y disponibilidad de los activos de información del PRONIED.

2. ALCANCE

La Política de Seguridad de la Información es de cumplimiento obligatorio del personal del PRONIED y de terceros, independientemente de su régimen laboral o contractual.

La presente política incluye la seguridad de la información aplicada a los distintos procesos que ejecuta el PRONIED.

3. BASE NORMATIVA

- Ley N° 28716, del 18 de abril del 2006, Ley de Control Interno de las Entidades del Estado.
- Ley N° 27444 – Ley del Procedimiento Administrativo General.
- Ley N° 27806 – Ley de Transparencia y Acceso a la Información Pública.
- Ley N° 29733 – Ley de Protección de Datos Personales y su reglamento.
- Decreto Supremo N° 004-2014-MINEDU, Crea el Programa Nacional de Infraestructura Educativa – PRONIED.
- Resolución Ministerial N° 034-2016-MINEDU, que aprueba el Manual de Operaciones del Programa Nacional de Infraestructura Educativa – PRONIED y modificado por Resolución Ministerial 341-2017-MINEDU, de fecha 12 de junio 2017
- Resolución Comisión de Normalización y de Fiscalización de Barreras Comerciales No Arancelarias N° 129-2014/CNB-INDECOPI, de fecha 20 de noviembre de 2014, que aprueba la Norma Técnica Peruana "NTP-ISO/IEC 27001:2014 EDI. Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de seguridad de la información. Requisitos. 2ª Edición.
- Resolución Ministerial N° 004-2016-PCM, de fecha 08 de enero de 2016, 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.
- Resolución Ministerial N° 166-2017- PCM, de fecha 20 de junio de 2017, que modifica el artículo 5 de a R.M. N° 001-2016-PCM referente al Comité de Gestión de Seguridad de la información.
- Resolución de Contraloría General N° 004-2017-CG, del 20 de enero del 2017, que aprueba la "Guía para la Implementación y fortalecimiento del Sistema de Control Interno de las entidades del Estado".
- Resolución Directoral Ejecutiva N° 060-2017-MINEDU/VMGI-PRONIED, que aprueba la designación del Oficial de Seguridad de la Información del PRONIED.

- Resolución Directoral Ejecutiva N° 068-2017-MINEDU/VMGI-PRONIED, que aprueba la conformación del Comité de Gestión de Seguridad de la Información del PRONIED.
- Resolución Directoral Ejecutiva N° 080-2018-MINEDU/VMGI-PRONIED, que deja sin efecto la Resolución Directoral Ejecutiva N° 060-2017-MINEDU/VMGI-PRONIED y designa como Oficial de Seguridad de la Información al Ingeniero Luis Pérez Pichis.
- Resolución Directoral Ejecutiva N° 090-2018-MINEDU/VMGI-PRONIED, que modifica la Resolución Directoral Ejecutiva N° 068-2017-MINEDU/VMGI-PRONIED.

4. ABREVIATURAS Y DEFINICIONES

4.1. Abreviaturas

- CGSI: Comité de Gestión de Seguridad de la Información.
- CISO: Oficial de Seguridad de la Información.
- PRONIED: Programa Nacional de Infraestructura Educativa
- SGSI: Sistema de Gestión de Seguridad de la Información.

4.2. Definiciones

- Activo
  Son los bienes que tienen valor para el PRONIED, siendo tangibles o intangibles.
- Comité de Seguridad de la Información
  Directivos del PRONIED designados en base a los lineamientos mencionados en las Resoluciones N° 004-2016-PCM y N° 166-2017- PCM.
- Confidencialidad
  Evitar que las personas no autorizadas puedan acceder a la información.
- Control
  Herramienta de gestión de riesgo, incluidas políticas, pautas, estructuras organizacionales, que pueden ser de naturaleza administrativa, técnica, gerencial o legal.
- Disponibilidad
  La información y los recursos relacionados se encuentren disponibles para el personal autorizado.
- Integridad
  Guardar la totalidad de la información, cuyo contenido debe permanecer inalterado a menos que sea modificado por personal autorizado.
- Política de Seguridad de la Información.
  Documento de contenido genérico que establece el compromiso de la Dirección Ejecutiva y el enfoque de la institución en la Gestión de la Seguridad de la Información, dentro del marco normativo que se rige en las entidades del estado.
- Procedimiento

Documento donde se encuentra un conjunto de pasos que se realizan para una tarea específica, incluye un flujograma.

- Registro
  Documento que indique los resultados obtenidos o proporcione evidencia de las actividades desempeñadas.
- Sistema de Gestión de Seguridad de la Información
  Proporciona un modelo para establecer, implementar, operar, monitorear, revisar, mantener y mejorar la protección de los activos de información para lograr los objetivos de negocio, ayuda a establecer políticas, procedimientos y controles de seguridad de la información.

5. POLITICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN

El PRONIED considera que la información que utiliza, procesa, genera o comparte durante el desarrollo de sus actividades, es un recurso estratégico y un activo crítico, y que el aseguramiento de los principios de confidencialidad, disponibilidad e integridad son primordiales para realizar con normalidad sus operaciones y actividades institucionales.

Es compromiso del PRONIED desarrollar, implantar, mantener y mejorar continuamente el Sistema de Gestión de Seguridad de la Información (SGSI)

6. POLITICAS ESPECÍFICAS DE SEGURIDAD DE LA INFORMACIÓN

6.1. Seguridad de la Información

Evitar la destrucción, divulgación, modificación y uso no autorizado de toda información relacionada con empleados, documentos físicos y digitales, manuales, código fuente, estrategias y otros conceptos asociados a activos de información.

6.2. Organización de la Seguridad de la Información

El PRONIED ha designado un CISO para velar y garantizar el cumplimiento de la presente política y establecer el marco de gestión de seguridad de información para su implementación en la institución.

La Oficina de Tecnologías de la Información es la encargada de administrar e implementar los mecanismos y salvaguardas relacionadas a la seguridad de la información dentro de la Institución.

El PRONIED cuenta con un Comité de Gestión de Seguridad de la información, para atender temas en materia de seguridad de la información que requiera de una definición o atención, el mismo que se encuentra conformado por:

- Director Ejecutivo.
- Jefe de la Oficina de General de Administración.
- Jefe de la Oficina de Planeamiento y Presupuesto.
- Jefe de la Oficina de Tecnologías de la Información.
- Jefe de la Oficina de Asesoría Jurídica.
- Oficial de Seguridad de la Información.

6.3. Seguridad en los Recursos Humanos

Todos los trabajadores del PRONIED deben cumplir con la normativa vigente relacionada a seguridad de la información, para lo cual deberá conocer y asumir sus responsabilidades respecto a dicha normativa.

El personal del PRONIED y terceros, con acceso a información sensible de la institución, deben firmar Acuerdos de Confidencialidad de información.

Realizar programas de sensibilización y entrenamiento en seguridad de la información para asegurar que los trabajadores del PRONIED asuman sus responsabilidades. Asimismo, establecer procesos disciplinarios para los casos de incumplimiento.

Incluir en los contratos con terceros, controles de seguridad de la información, que garanticen la confidencialidad de la información de la institución.

Al término del vínculo contractual, emplear mecanismos para la devolución de activos de información asignados y el retiro inmediato de los accesos a sistemas de información y servicios tecnológicos que se hayan otorgado.

El personal del PRONIED debe cumplir con las responsabilidades y deberes de seguridad de la información que siguen siendo válidos luego del término de la relación contractual con la institución.

6.4. Gestión de los Activos de Información

Elaborar y mantener un inventario de los activos de información para el proceso de evaluación de riesgos de seguridad de la información, asignando responsables de velar por la protección de dichos activos.

Las categorías establecidas para la clasificación de la información que administra el PRONIED en función de su valor, requisitos legales, criticidad y sensibilidad son las siguientes:

- Pública: Información de acceso libre a cualquier persona que lo requiera, haciendo uso del procedimiento establecido en la Ley N° 27806 Ley de transparencia y acceso a la información pública.
- Uso interno: Información de acceso interno, cuya divulgación o uso no autorizado, podría generar algún riesgo a la entidad o terceros.
- Información Confidencial: Información del PRONIED de acceso restringido, cuyo uso o divulgación no autorizada ocasionaría un alto impacto a la entidad o terceros.

La clasificación se hará según lo definido por el propietario de la información, la misma que será aprobada por el jefe del área responsable y distribuida a las diferentes unidades orgánicas.

Establecer la normativa relacionada a la administración de medios removibles, en concordancia con el esquema de clasificación de la información adoptada por la institución.

Antes de reasignar o dar de baja algún dispositivo de almacenamiento de información, comprobar que la información contenida sea eliminada o sobrescrita de manera segura, de modo que resulte imposible recuperar dicha información.

Proteger a los medios que contienen información, contra el acceso no autorizado, el uso indebido o la corrupción durante el transporte de los mismos.

6.5. Control de Acceso

Otorgar los accesos a los activos de información del PRONIED en base a la necesidad y en relación a las funciones del usuario. Para el caso del acceso no autorizado a los sistemas de información, servicios de red y plataforma tecnológica del PRONIED, emplear mecanismos para prevenirlos.

Implementar un proceso de autorización y un registro de todos los privilegios asignados. Es responsabilidad directa de los usuarios el velar por la confiabilidad y buen uso de su contraseña.

Restringir y controlar el uso de programas utilitarios que puedan ser capaces de anular los controles del sistema operativo y de los softwares de aplicación.

Contar con autorización para uso de recursos tecnológicos, debiéndose controlar la asignación y retiro de los mismos.

6.6. Criptografía

Establecer un mecanismo respecto a la administración de claves y la recuperación de la información cifrada en caso de pérdida, compromiso, daño y reemplazo de las claves antes mencionadas.

En los casos que se requiera el cifrado de la información, el CISO en coordinación con el propietario de la información, debe evaluar los riesgos con la finalidad de identificar el nivel requerido de protección.

6.7. Seguridad Física y Ambiental

Contar con mecanismos de control de acceso, protección física y ambiental apropiada para prevenir pérdida o daño de los activos de información.

Todas las áreas que cuenten con instalaciones de procesamiento de información consideradas críticas para el correcto funcionamiento de los

sistemas de información del PRONIED, deben estar protegidas por un perímetro de seguridad física.

Dar cumplimiento a la normativa interna relacionada al mantenimiento preventivo y correctivo de los equipos de cómputo y de comunicaciones, con la finalidad de asegurar la continuidad, disponibilidad e integridad de los mismos. Asimismo, se deberá dar cumplimiento a la normativa interna relacionada al respaldo y restauración de la información.

Establecer controles para proteger los equipos informáticos, respecto a posibles fallas en el suministro de energía u otras anomalías eléctricas.

En todas las instalaciones del PRONIED, el cableado de energía eléctrica y de comunicaciones que transporta datos o brinda apoyo a los servicios informáticos, debe contar con mecanismos que lo protejan contra intercepción o daño. Asimismo, el cableado eléctrico debe estar separado del cableado de datos, es decir, no deben estar en el mismo ducto o canaleta con el fin de evitar interferencias.

El cableado de red de comunicaciones del PRONIED debe cumplir con los estándares nacionales e internacionales de cableado estructurado, solo el personal técnico autorizado por la OTI podrá realizar trabajos de instalación o mantenimiento del cableado eléctrico o de comunicaciones

El usuario es responsable de bloquear el acceso a su equipo cuando deje temporalmente su zona de trabajo. Como medida de apoyo, todas las estaciones de trabajo del PRONIED deben tener un mecanismo automático de bloqueo de pantalla con clave cuando no lo estén utilizando.

El usuario debe mantener en orden su área de trabajo y asegurarse que la información confidencial se encuentre en un lugar seguro cuando se ausente del lugar asignado para el desarrollo de sus funciones.

6.8. Seguridad en las Operaciones

Mantener documentado el procesamiento de la información y los recursos de comunicación del PRONIED, el mismo que deberá encontrarse disponible y accesible para todos los usuarios interesados que lo requieran.

Definir un mecanismo para el control de los cambios en los sistemas de información y recursos de tratamiento de información en el ambiente de producción.

Monitorear continuamente la plataforma tecnológica del PRONIED, con el fin de establecer niveles de capacidad y desempeño, así como también realizar proyecciones para determinar requisitos futuros de capacidad.

Mantener identificados, controlados y separados los ambientes de desarrollo, pruebas y producción, aplicando procedimientos específicos para tales fines.

No está permitido el uso de compiladores, editores, y otros utilitarios del sistema de información en el ambiente de producción, sin autorización de la Oficina de Tecnologías de la Información.

La Oficina de Tecnologías de la Información debe monitorear de forma constante la red interna, implementando las herramientas que le permitan detectar, prevenir y recuperarse de ataques de códigos maliciosos en la plataforma tecnología; lo cual debe estar acompañado de una concientización adecuada al usuario.

La Oficina de Tecnologías de la Información debe implementar mecanismos para el registro y revisión de los registros de auditoría, orientados a producir informes de las amenazas detectadas contra los sistemas de información y métodos utilizados. Además debe planificar y establecer los requisitos de auditorías y las actividades que involucran la verificación de los sistemas de información, con el propósito de minimizar la interrupción a los procesos de negocio del PRONIED.

Realizar el monitoreo de la red interna, así como detectar actividades no autorizadas y generar evidencia de los registros (Logs). Además los registros (Logs) y la información de los mismos, deberán ser protegidos contra la adulteración y el acceso no autorizado.

Obtener de manera oportuna, información sobre las vulnerabilidades técnicas de los sistemas de información a ser utilizados, y evaluar la exposición del PRONIED a dichas vulnerabilidades así como tomar las medidas adecuadas para manejar los riesgos asociados.

6.9. Seguridad de las Comunicaciones

Controlar los accesos a los recursos de la red, tanto internos como externos, de manera que los usuarios no comprometan la seguridad de los activos de información.

Establecer controles y mecanismos de autorización para otorgar acceso a los usuarios, a las redes y servicios informáticos autorizados.

El acceso externo a la red del PRONIED, se debe realizar solamente a través de una VPN (Red Privada Virtual) configurada para tal fin.

La Oficina de Tecnologías de la Información debe dar cumplimiento a la Normativa sobre la Gestión del Correo Institucional en el PRONIED.

6.10. Adquisición, Desarrollo y Mantenimiento de Sistemas

Establecer requisitos de seguridad para los sistemas de información desarrollados interna o externamente, controles de cambios, protección de código fuente y datos en producción.

Aplicar una capa de seguridad en los aplicativos dentro del ciclo de vida de desarrollo del software.

El desarrollo o mantenimiento de los sistemas de información en el PRONIED debe considerar estándares internaciones del ciclo de vida del software.

Controlar los cambios en los sistemas de información, así como autorizar y documentar los cambios realizados.

La Oficina de Tecnologías de la Información debe garantizar que los datos de prueba pueden ser seleccionados, protegidos y controlados de manera adecuada.

6.11. Relaciones con los Proveedores

Los requisitos de seguridad de la información para mitigar los riesgos asociados al acceso del proveedor a los activos del PRONIED, se deben acordar con el proveedor y deben ser documentados.

Todos los requisitos relevantes de seguridad de la información, se deben establecer y acordar con cada proveedor que pueda acceder, procesar, almacenar, comunicar, o proveer componentes de Infraestructura Tecnológica para el PRONIED.

Los acuerdos con proveedores deben incluir requisitos para abordar los riesgos de seguridad de la información asociados con los servicios informáticos y la cadena de suministro de productos.

PRONIED debe implementar controles de seguridad de la información de los proveedores, como acuerdos de confidencialidad. Asimismo, debe controlar el acceso de los proveedores a las instalaciones de la entidad.

6.12. Gestión de Incidentes de Seguridad de la Información

Reportar al CISO cualquier incidente de seguridad que detecten, en el momento en que se detecte una posible amenaza que atente contra los activos de información.

Establecer procedimientos documentados para informar, evaluar, clasificar y dar respuesta a los incidentes y debilidades de seguridad de la información.

Contar con un registro organizado de los incidentes de seguridad identificados, programando la ejecución de las medidas necesarias para su tratamiento y al responsable de gestionarlas.

Promover que el conocimiento adquirido a partir de analizar y resolver los incidentes de seguridad de la información, sea utilizado para reducir la probabilidad o el impacto de incidentes futuros.

Programar revisiones semestrales, orientada a obtener información oportuna e identificar incidentes de seguridad en los sistemas de información del PRONIED.

Definir y aplicar mecanismos para la identificación, recolección, adquisición y preservación de información que pueda servir como evidencia.

6.13. Seguridad de la Información en Gestión de Continuidad del Negocio

Determinar los requisitos para la seguridad de la información y para la continuidad de la gestión de seguridad de la información en situaciones adversas.

Establecer, documentar, implementar y mantener los procesos, procedimientos y controles para garantizar el nivel requerido de continuidad de la seguridad de la información durante una situación adversa.

Verificar los controles de la continuidad de la seguridad de la información establecida e implementada, a intervalos regulares con la finalidad de asegurar la validez y efectividad durante situaciones adversas.
Implementar en las instalaciones de procesamiento de la información, la suficiente redundancia para cumplir con los requisitos de disponibilidad necesarios.

6.14. Cumplimiento

La política de seguridad de información del PRONIED ha sido diseñada para normar, sin contravenir las medidas de protección establecidas en las leyes y regulaciones vigentes.

Establecer mecanismos para el cumplimiento de requisitos legislativos, estatutarios, regulatorios y contractuales relevantes que afecten los activos de información del PRONIED.

Proteger los registros de cualquier pérdida, destrucción, falsificación, acceso no autorizado y divulgación no autorizada, de acuerdo con los requisitos legislativos, regulatorios, contractuales y del negocio.

Asegurar la privacidad y la protección de datos personales, de acuerdo a lo que se requiere en la legislación y regulación relevantes.

La gestión de la seguridad de la información del PRONIED y su implementación, deben ser revisadas de forma independiente a intervalos planeados o cuando ocurran cambios significativos en la entidad.

7. OBJETIVOS DE SEGURIDAD DE LA INFORMACIÓN

- Proteger los activos de información del PRONIED y la tecnología utilizada para su procesamiento, frente a amenazas internas y/o externas, reduciendo los riesgos para mantener la continuidad operativa de los distintos procesos que ejecuta el PRONIED.
- Determinar los requerimientos de seguridad de la información del PRONIED, a partir de los cuáles se identifiquen los controles que se deberán adoptar, para protegerse contra amenazas que podrían afectar la seguridad de la información.
- Implementar mecanismos de medición de seguridad de la información, en función al nivel de exposición a los riesgos y la eficacia de los controles implementados.
- Concientizar a los trabajadores del PRONIED y proveedores, en el proceso de preservar la seguridad de la información.

8. RESPONSABILIDADES

- **Del Director Ejecutivo**
  Es responsable de la aprobación de la presente política y propiciar su aplicación.
- **Del CISO**
  Es responsable de verificar su cumplimiento, diseñando controles, proponiendo directivas de seguridad de la información que permitan cumplir con la política declarada.
- **Del Comité de Gestión de Seguridad de la Información**
  Es responsable de coordinar, implementar, establecer las directivas, estándares lineamientos, y procedimientos requeridos para garantizar la seguridad de los activos de información.
- **Del Personal del PRONIED y Terceros**
  Es responsable del cumplimiento de la presente política, controles de seguridad, directivas, entre otros mecanismos que coadyuven en salvaguardar los activos de información de la institución.