Firma Digital
ONPE
OFICINA NACIONAL DE PROCESOS ELECTORALES
Firmado digitalmente por CASTILLO MEZA Adolfo Carlo Magno (FAU20291973851)
Motivo: Soy el autor del documento
Fecha: 23.03.2017 10:56:06 -05:00

ONPE
OFICINA NACIONAL DE PROCESOS ELECTORALES

*"Año del Buen Servicio al Ciudadano"*

Lima, 23 de Marzo del 2017

# RESOLUCION JEFATURAL N° 000093-2017-J/ONPE

**VISTOS**: El Acta N° 000001-2017-CGSI del Comité de Gestión de Seguridad de la Información, los Informes N° 000032, N° 000036 y N° 000037-2017-GGC/ONPE de la Gerencia de Gestión de la Calidad; el Memorando N° 000119-2017-GSFP/ONPE de la Gerencia de Supervisión de Fondos Partidarios; el Memorando N° 000256-2017-GCRC/ONPE de la Gerencia de Comunicaciones y Relaciones Corporativas; el Memorando N° 000226-2017-GIEE/ONPE de la Gerencia de Información y Educación Electoral; el Memorando N° 000091-2017-OSDN/ONPE de la Oficina de Seguridad y Defensa Nacional; el Memorando N° 000384-2017-GCPH/ONPE de la Gerencia Corporativa de Potencial Humano; así como el Memorando N° 000235-2017-GAJ/ONPE e Informe N° 000139-2017-GAJ/ONPE de la Gerencia de Asesoría Jurídica; y,

**CONSIDERANDO**:

Mediante Resolución Ministerial N° 246-2007-PCM, se aprobó el uso obligatorio de la Norma Técnica Peruana "NTP-ISO/EC 17799:2007 EDI. Tecnología de la Información. Código de Buenas Prácticas para la gestión de la seguridad de la información. 2a Edición", en todas las Entidades integrantes del Sistema Nacional de Informática;

En cumplimiento a la norma técnica antes referida, a través de la Resolución Jefatural N° 065-2008-J/ONPE y sus modificatorias, se conformó el Comité de Gestión y Seguridad de la Información de la Oficina Nacional de Procesos Electorales, el cual tiene entre sus funciones la de revisar la Política de Seguridad de la información de manera periódica y proponer las modificaciones que correspondan;

De acuerdo a lo establecido en el literal a) del artículo 45° del Reglamento de Organización y Funciones de la Oficina Nacional de Procesos Electorales (ONPE), aprobado por Resolución Jefatural N° 063-2014-J/ONPE y sus modificatorias, la Gerencia de Gestión de la Calidad tiene como función proponer a la Gerencia General las políticas, planes y acciones relacionadas a los Sistemas de Gestión de la Calidad y la Gestión por Procesos, en beneficio de la mejora continua de la ONPE;

De la misma forma, el literal f) del acotado artículo, dispone que la citada Gerencia se encarga de proponer, implementar y mantener los Sistemas de Gestión de Calidad de la ONPE, así como formular los estándares y mejoras de los procesos, niveles de servicio, instrumentos y métodos de gestión en toda la Entidad;

Asimismo, a través de la Resolución Jefatural N° 000370-2015-J/ONPE, se aprobó la Directiva "Política de Seguridad de la Información" con Código DI03-GGC/GC, Versión: 00, cuyo objeto es establecer las normas relacionadas a la seguridad de la información, a fin de asegurar su confidencialidad, integridad y disponibilidad;

La Gerencia de Gestión de la Calidad mediante los documentos de vistos, como parte del mantenimiento y mejora continua, procedió con la evaluación y actualización de la documentación interna de seguridad de la información y considerando los aportes de los miembros del Comité de Gestión de Seguridad de la Información, recomienda a la Gerencia General la aprobación de la Directiva con

Firma Digital
ONPE
OFICINA NACIONAL DE PROCESOS ELECTORALES
Firmado digitalmente por JERI CABEZUDO Paola Silvia (FAU20291973851)
Motivo: Doy V° B°
Fecha: 22.03.2017 17:02:00 -05:00

Firma Digital
ONPE
OFICINA NACIONAL DE PROCESOS ELECTORALES
Firmado digitalmente por LOPEZ VILLAFUERTE Fernando (FAU20291973851)
Motivo: Doy V° B°
Fecha: 21.03.2017 14:43:46 -05:00

Firma Digital
ONPE
OFICINA NACIONAL DE PROCESOS ELECTORALES
Firmado digitalmente por LANDA CAMAYO Heidi Veronica (FAU20291973851)
Motivo: Doy V° B°
Fecha: 21.03.2017 14:31:37 -05:00

Firma Digital
ONPE
OFICINA NACIONAL DE PROCESOS ELECTORALES
Firmado digitalmente por VARGAS RODRIGUEZ Patricia Janette (FAU20291973851)
Motivo: Doy V° B°
Fecha: 21.03.2017 14:13:43 -05:00

Firma Digital
ONPE
OFICINA NACIONAL DE PROCESOS ELECTORALES
Firmado digitalmente por BARBOZA DAVILA Luis Brussy (FAU20291973851)
Motivo: Doy V° B°
Fecha: 21.03.2017 14:06:07 -05:00

Firma Digital
ONPE
OFICINA NACIONAL DE PROCESOS ELECTORALES
Firmado digitalmente por ALEJOS SEVILLANO DE ESCUDERO Sessy Betsy (FAU20291973851)
Motivo: Doy V° B°
Fecha: 21.03.2017 14:05:29 -05:00

Firma Digital
ONPE
OFICINA NACIONAL DE PROCESOS ELECTORALES
Firmado digitalmente por PORTOCARRERO PEÑAFIEL Sandra Lucy (FAU20291973851)
Motivo: Doy V° B°
Fecha: 21.03.2017 13:47:50 -05:00

Código DI04-GGC/GC "Lineamientos de la Seguridad de la Información", Versión 00; cuyo objetivo es establecer las normas relacionadas a la seguridad de la información, a fin de asegurar y mantener su confidencialidad, integridad y disponibilidad;

Conforme a lo expuesto, corresponde emitir la Resolución Jefatural que apruebe la Directiva Lineamientos de Seguridad de la Información de la ONPE;

De conformidad con lo dispuesto por el literal g) del artículo 5° y el artículo 13° de la Ley N° 26487, Ley Orgánica de la ONPE, así como del literal s) del artículo 11° de su Reglamento de Organización y Funciones, aprobado por la Resolución Jefatural N° 063-2014- J/ONPE y sus modificatorias;

Con el visado de la Secretaría General y de las Gerencias de Asesoría Jurídica, de Supervisión de Fondos Partidarios; de Comunicaciones y Relaciones Corporativas; de Información y Educación Electoral; de la Oficina de Seguridad y Defensa Nacional y Corporativa de Potencial Humano;

**SE RESUELVE**:

**Artículo Primero**.- Aprobar la Directiva "Lineamientos de Seguridad de la Información", con Código: DI04-GGC/GC, Versión: 00, que en anexo forma parte de la presente Resolución.

**Artículo Segundo.**- Dejar sin efecto la Directiva "Política de Seguridad de la Información", con Código: DI03-GGC/GC, Versión: 00, aprobada con Resolución Jefatural N° 000370-2015-J/ONPE.

**Artículo Tercero.-** Encargar a la Gerencia de Gestión de la Calidad efectuar el seguimiento y evaluación del cumplimiento del documento materia de aprobación en el artículo primero de la presente Resolución Jefatural.

**Artículo Cuarto**.- Disponer la publicación de la presente resolución en el portal institucional www.onpe.gob.pe y en el Portal de Transparencia de la ONPE, dentro de los tres (03) días de emitida la presente Resolución.

**Regístrese y comuníquese.**

**ADOLFO CARLO MAGNO CASTILLO MEZA**
**Jefe**
**Oficina Nacional de Procesos Electorales**

ACM/pvr/spp/gec/pvv

ONPE
OFICINA NACIONAL DE PROCESOS ELECTORALES

# LINEAMIENTOS DE SEGURIDAD DE LA INFORMACIÓN

| Elaborado por: | Revisado por: |
| --- | --- |
| Verónica Ordóñez Dávila<br>Oficial de Seguridad de la Información<br><br>15 MAR 2017 | Patricia Janette Vargas Rodriguez<br>Secretaria General (e)<br>15 MAR 2017<br><br>Gilbert Fernando Vallejos Agreda<br>Gerente de la Gerencia General<br>15 MAR 2017<br><br>Jaime Enrique Molina Vilchez<br>Gerente de Gestión de la Calidad<br>15 MAR 2017<br><br>Erik Ulises Bazán Flores<br>Gerente de Información y Tecnología Electoral (e)<br>15 MAR 2017<br><br>Adelmo Canciao Cancino<br>Gerente de Gestión Electoral<br>15 MAR 2017<br><br>Mary del Rosario Hessen Vigil<br>Gerente de Planeamiento y Presupuesto<br>15 MAR 2017<br><br>Henry Josue Orna Robladillo<br>Gerente de Organización Electoral y Coordinación Regional (e)<br>15 MAR 2017<br><br>Fernando López Vilafuerte<br>Gerente de Supervisión de Fondos Partidarios (e)<br>15 MAR 2017<br><br>Heidi Veronica Landa Camayo<br>Gerente de Información y Educación Electoral (e)<br>15 MAR 2017<br><br>Sandra Lucy Portocarrero Peñafiel<br>Gerente de Asesoría Jurídica<br>15 MAR 2017<br><br>Fernando López Vilafuerte<br>Gerente de la Oficina de Seguridad y Defensa Nacional<br>15 MAR 2017<br><br>Sessy Betsy Alejos Semlano De Escudero<br>Gerente Corporativo de Potencial Humano<br>15 MAR 2017<br><br>Gustavo Elias Dominguez Lopez<br>Gerente de Administración<br>15 MAR 2017<br><br>Paola Silvia Jeri Cabezudo<br>Gerente de Comunicaciones y Relaciones Corporativas (e)<br>15 MAR 2017 |
| **Código: DI04-GGC/GC**<br>**Versión: 00** | |

## ÍNDICE

## 1. OBJETIVO

Establecer las normas relacionadas a la seguridad de la información a fin de asegurar y mantener su confidencialidad, integridad y disponibilidad.

## 2. ALCANCE

Es de aplicación para todo el personal de la institución contratado bajo cualquier modalidad, proveedores de servicios y terceros.

## 3. BASE NORMATIVA

**3.1.** Resolución Ministerial Nº 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.

**3.2.** Resolución Ministerial Nº 246-2007-PCM que aprueba el uso obligatorio de la Norma Técnica Peruana "NTP-ISO/IEC 17799:2007 EDI. Tecnología de la Información. Código de buenas prácticas para la gestión de la seguridad de la información. 2a. Edición" en todas entidades integrantes del Sistema nacional de Informática.

**3.3.** Resolución Directoral Nº 001-2013-JUS/DGPDP que aprueba los formularios para la inscripción de bancos de datos personales de administración privada por persona natural, de administración privada por persona jurídica y de administración pública.

**3.4.** Ley N° 27806 – Ley de Transparencia y Acceso a la Información Pública y su reglamento.

**3.5.** Ley N° 29733 – Ley de Protección de Datos Personales, su reglamento y su directiva.

**3.6.** Ley N° 27269 – Ley de Firmas y Certificados Digitales y su reglamento.

**3.7.** Ley 27815 – Ley del Código de Ética de la Función Pública.

**3.8.** Decreto Legislativo N° 681 - "Dictan normas que regulan el uso de tecnologías avanzadas en materia de archivo de documentos e información tanto respecto a la elaborada en forma convencional cuanto la producida por procedimientos informáticos en computadoras" y su reglamento.

**3.9.** Norma Técnica Peruana NTP 392.030-2:2015 Microformas. Requisitos para las organizaciones que operan sistemas de producción de microformas. Parte 2: Medios de Archivo Electrónico.

**3.10.** Directiva del Instituto Nacional de Estadística e Informática "Normas técnicas para el almacenamiento y respaldo de la información procesada las Entidades de la Administración Pública".

**3.11.** Reglamento de Organización y Funciones de la Oficina Nacional de Procesos Electorales.

**3.12.** Reglamento Interno de Trabajo de la Oficina Nacional de Procesos Electorales.

**3.13.** Manual de Organización y Funciones de la Oficina Nacional de Procesos Electorales.

Nota: Los documentos mencionados son los vigentes incluyendo sus modificatorias.

## 4. REFERENCIAS

**4.1.** Política de Protección de Datos Personales de la Oficina Nacional de Procesos Electorales.

**4.2.** Política de Seguridad de la Información de la Oficina Nacional de Procesos Electorales.
**4.3.** Objetivos de Seguridad de la Información de la Oficina Nacional de Procesos Electorales.

**Nota:** Los documentos mencionados son los vigentes incluyendo sus modificatorias.

## 5. DEFINICIONES Y ABREVIATURAS

### 5.1. Definiciones

**5.1.1. Activos de información:** Recursos humanos, tecnológicos, administrativos, etc. que participan en el tratamiento de la información.

**5.1.2. Cifrado:** Es una forma de tratamiento que permite que la información electrónica sea leíble y modificada solo por las personas autorizadas, asegurando así su confidencialidad e integridad respectivamente.

**5.1.3. Comité de Gestión de Seguridad de la Información:** Es el comité que tiene por función gestionar la seguridad de la información en la institución. Se conforma por Resolución Jefatural.

**5.1.4. Confidencialidad:** Cualidad de prevenir la divulgación de la información a personas o sistemas no autorizados.

**5.1.5. Datos personales:** Son aquellos que identifican directa o indirectamente a una persona natural (titular de los datos): nombre, fecha de nacimiento, dirección de domicilio y de correo electrónico; números del DNI, RUC, teléfono, celular, seguro social y placa de vehículo; imagen; firma manuscrita y electrónica; y otros datos no sensibles establecidos en los formularios aprobados con Resolución Directoral N° 001-2013-JUS/DGPDP (08 de mayo de 2013).

**5.1.6. Datos personales sensibles:** Son aquellos que pueden ser objeto de tratamiento con el consentimiento expreso y por escrito de la persona natural (titular de los datos) y, por lo tanto, requieren especial protección: datos biométricos (huella dactilar o digital, retina, iris); datos de origen racial y étnico; ingresos económicos; opiniones o convicciones políticas, religiosas, filosóficas o morales; afiliación sindical; datos relacionados a la salud o a la vida sexual; y hechos o circunstancias de la vida afectiva o familiar.

**5.1.7. Disponibilidad:** Característica que determina la accesibilidad de la información a personas, procesos o sistemas en el lugar y momento oportunos.

**5.1.8. Dispositivos móviles institucionales:** Aparatos electrónicos como computadoras portátiles, *tablets*, celulares o *smartphones*, acceso portable a datos (PDA), dispositivos de almacenamiento USB u otros que permitan el tratamiento de la información durante su desplazamiento y uso en ambientes no controlados por la institución.

**5.1.9. Encargado del banco de datos personales:** Personal designado, mediante resolución jefatural, por la Jefatura Nacional como responsable de la seguridad de los bancos de datos personales que administra la institución en el ámbito de la Ley de Protección de Datos Personales.

**5.1.10. Gestión de riesgos:** Consiste en la identificación, análisis y evaluación de riesgos, así como la planificación, implementación y su correspondiente seguimiento de las acciones de tratamiento del riesgo.

**5.1.11. Integridad:** Propiedad que busca garantizar una información exacta y libre de errores, la misma que puede ser modificada bajo autorización.

**5.1.12. Interesados:** Personas u organizaciones que tienen una responsabilidad, necesidad, expectativa, o cualquier otro interés que involucra a la institución. Pueden afectar o ser afectados por alguna decisión o actividad. Ejemplo: personal; proveedores; socios por convenio interinstitucional; entidades observadoras, reguladoras, supervisoras y fiscalizadoras; y clientes.

**5.1.13. Líder usuario:** Personal responsable de definir y aceptar el cumplimiento de los requerimientos y requisitos del producto software. Es designado por el órgano o unidad orgánica solicitante del producto software.

**5.1.14. Medios de almacenamiento removibles:** Son aquellos dispositivos que se insertan a los conectores externos de los equipos informáticos para almacenar información, tales como memoria USB, disco duro externo o tarjetas de memoria.

**5.1.15. Controles criptográficos**: Son aquellos controles que protegen la confidencialidad e integridad de la información electrónica durante su procesamiento, almacenamiento o transmisión y que comprueban la identidad de quienes acceden a esta.

**5.1.16. Oficial de Seguridad de la Información:** Personal designado mediante, resolución jefatural, por la Jefatura Nacional, que tiene la responsabilidad de supervisar la implementación de la Política y objetivos de Seguridad de la Información de la institución, alineando los controles y recursos de acuerdo a la gestión de los riesgos.

**5.1.17. Oficial de Seguridad EREP:** Personal designado, mediante resolución gerencial, por la Gerencia de Organización Electoral y Coordinación Regional para coordinar la seguridad de la información que administra la institución como Entidad de Registro para el Estado Peruano en el ámbito de la Ley de Firmas y Certificados Digitales.

**5.1.18. Oficial de Privacidad EREP:** Personal designado, mediante resolución gerencial, por la Gerencia de Organización Electoral y Coordinación Regional para coordinar la protección de los datos personales que administra la institución como Entidad de Registro para el Estado Peruano en el ámbito de la Ley de Firmas y Certificados Digitales.

**5.1.19. PeCERT:** Grupo de trabajo permanente, denominado Coordinadora de Respuestas a Emergencias en Redes Teleinformáticas de la Administración Pública del Perú, en el ámbito de la Oficina Nacional de Gobierno Electrónico e Informática (ONGEI) de la Presidencia del Consejo de Ministros. Se encarga de coordinar con las instituciones públicas para afrontar diversas amenazas de las redes teleinformáticas a los que está expuesta la información que producen o administran, con el fin de proveer a la Nación de una postura segura en el ámbito de la seguridad informática.

**5.1.20. Propietario de activo:** Órgano de la ONPE responsable, determinado en un inventario de activos de información, que tiene la responsabilidad y autoridad, dentro del alcance de sus competencias, de asegurar el buen uso, funcionamiento y protección del activo de información mientras está a su cargo a fin de que cumpla con los objetivos para los cuales se le adquirió.

**5.1.21. Propietario de riesgo:** Órgano de la ONPE que se ve afectado por el riesgo y tiene responsabilidad y autoridad para gestionarlo.

**5.1.22. Redes inalámbricas públicas:** Son aquellas redes inalámbricas ubicadas en lugares públicos tales como restaurantes, centros comerciales, buses, hoteles, etc. en donde cualquier dispositivo móvil, institucional o no, puede conectarse a ellas.

**5.1.23. Responsable de Seguridad Tecnológica:** Personal designado, mediante resolución gerencial, por la Gerencia de Informática y Tecnología Electoral, que tiene como propósito coordinar las acciones para prevenir o mitigar los riesgos de origen tecnológico.

**5.1.24. Responsable del Sistema de Gestión del órgano:** Personal designado, mediante memorando, por el Órgano que tiene como propósito liderar aspectos de gestión de la calidad, seguridad de la información y otros en el ámbito del órgano al cual pertenece.

**5.1.25. Riesgo:** Probabilidad de que un evento, suceso o acontecimiento perjudicial (no deseado) o beneficioso (deseado), degrade o aumente el grado de la confidencialidad, integridad y disponibilidad de la información que maneja un determinado proceso o proyecto.

**5.1.26. Sistema de información:** Es todo sistema soportado por una infraestructura tecnológica informática.

**5.1.27. Tratamiento de información:** Es la acción, automatizada o no, de crear, elaborar, recopilar, registrar, almacenar, cifrar, consultar, usar, organizar, modificar, copiar, extraer, transferir, transmitir, distribuir, bloquear, procesar, conservar, eliminar, suprimir o destruir la información.

**5.1.28. Usuarios:** Personal de la institución contratado bajo cualquier modalidad, proveedores de servicios y terceros que tienen acceso a la información a través de medios convencionales u automatizados.

### 5.2. Abreviaturas

| | | |
|---|---|---|
| **5.2.1.** | **APDP** | : Autoridad Nacional de Protección de Datos Personales. |
| **5.2.2.** | **AAC** | : Autoridad Administrativa Competente. |
| **5.2.3.** | **CGSI** | : Comité de Gestión de Seguridad de la Información. |
| **5.2.4.** | **EC** | : Entidad de Certificación |
| **5.2.5.** | **EREP** | : Entidad de Registro del Estado Peruano. |
| **5.2.6.** | **GCPH** | : Gerencia Corporativa de Potencial Humano. |
| **5.2.7.** | **GG** | : Gerencia General. |
| **5.2.8.** | **GGC** | : Gerencia de Gestión de la Calidad. |
| **5.2.9.** | **GIEE** | : Gerencia de Información y Educación Electoral. |
| **5.2.10.** | **GITE** | : Gerencia de Informática y Tecnología Electoral. |
| **5.2.11.** | **INDECOPI** | : Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual. |
| **5.2.12.** | **JN** | : Jefatura Nacional. |
| **5.2.13.** | **LPDP** | : Ley de Protección de Datos Personales. |
| **5.2.14.** | **ODPE** | : Oficina Descentralizada de Procesos Electorales. |
| **5.2.15.** | **ONPE** | : Oficina Nacional de Procesos Electorales. |
| **5.2.16.** | **OSDN** | : Oficina de Seguridad y Defensa Nacional. |
| **5.2.17.** | **OSI** | : Oficial de Seguridad de la Información. |
| **5.2.18.** | **SG** | : Secretaría General. |
| **5.2.19.** | **SGSI** | : Sistema de Gestión de Seguridad de la Información. |
| **5.2.20.** | **TI** | : Tecnología de la Información. |

## 6. NORMAS GENERALES

### 6.1. Organización de la seguridad de la información

#### 6.1.1. Organización interna

La ONPE ha establecido los siguientes roles y funciones para la gestión de la seguridad de la información:

**A. Comité de Gestión de Seguridad de la Información (CGSI)**

a) Revisar las políticas, objetivos, planes, normas, responsabilidades y propuestas de mejora que reciba, asociados a la seguridad de la información, y de considerarlo pertinente, elevarlas a JN para su consideración y posterior aprobación, así como evaluar su cumplimiento.
b) Definir las estrategias de la institución respecto a la implementación de normas del Estado Peruano y estándares internacionales referidos a la seguridad de la información.
c) Revisar la Política de Seguridad de la Información una vez al año o cuando se realice alguna modificación significativa que impacte en la institución; y formular, a través del OSI, las modificaciones que correspondan para su aprobación por la JN.
d) Asegurar la comunicación a los usuarios sobre la Política y Objetivos de Seguridad de la Información, así como de los Lineamientos de Seguridad de la Información, la importancia de su cumplimiento; así como, sus responsabilidades de acuerdo a la Ley.

e) Garantizar la implementación, operación, revisión, mantenimiento y mejora del SGSI; y evaluar por lo menos una vez al año sus resultados.
f) Cumplir con alguna otra función establecida en el ordenamiento jurídico del Estado Peruano en materia de seguridad de la información.

**B. Propietario de Riesgo**

a) Gestionar los riesgos de seguridad de la información dentro del alcance de sus competencias.

**C. Oficial de Seguridad de la Información (OSI)**

a) Proponer a los demás miembros del CGSI las políticas, objetivos, lineamientos, planes, roles y funciones necesarias para la ~~administración~~ gestión técnica y efectiva de la seguridad de la información.
b) Coordinar la ejecución de la evaluación de riesgos de seguridad de la información y de sus resultados.
c) Coordinar con el Oficial de Seguridad de la EREP y los Responsables del Sistema de Gestión y de Seguridad Tecnológica, la adecuada implementación de las políticas, objetivos, planes y controles de seguridad de la información que les corresponda.
d) Verificar que las ejecuciones de las pruebas hayan cumplido con los procedimientos relacionados con la continuidad de la seguridad de la información.
e) Identificar las necesidades de capacitación, difusión y sensibilización en seguridad de la información.

**D. Oficial de Seguridad de la EREP**

a) Velar por la estricta observancia de la política, objetivos y lineamientos de Seguridad de la Información de la institución dentro del alcance de la EREP-ONPE.
b) Cuidar que los procesos y procedimientos relacionados a la firma digital, se realicen en el marco de la Infraestructura Oficial de Firma Electrónica, garantizando el no repudio de los documentos electrónicos generados por la EREP-ONPE.
c) Proponer las acciones necesarias para dar cumplimiento a la política, objetivos y lineamientos de Seguridad de la Información que se encuentren dentro del alcance de la EREP-ONPE.
d) Asegurar la implementación de controles de seguridad de la información para los procesos a cargo de la EREP-ONPE.
e) Revisar permanentemente la política, objetivos y lineamientos de Seguridad de la Información dentro del alcance de la EREP-ONPE, proponiendo de ser el caso su actualización.
f) Promover la adopción de buenas prácticas en materia de seguridad de la información.
g) Identificar las necesidades de capacitación y sensibilización para una adecuada protección de la seguridad de la información, dentro del marco de los servicios de la EREP-ONPE.
h) Adoptar las medidas correctivas en caso se identifique algún tipo de vulneración real o potencial de la seguridad de la información.

i) Gestionar los riesgos y dar respuesta ante incidentes en los procesos a cargo de la EREP-ONPE.
j) Determinar y analizar los requerimientos necesarios para la recuperación en caso de desastres.

**E. Responsable de Seguridad Tecnológica**

a) Administrar los procesos de seguridad tecnológica.
b) Proponer guías, normas o estándares de seguridad para el diseño de las soluciones tecnológicas que se implementen.
c) Elaborar los planes de seguridad tecnológica y de contingencia.
d) Ejecutar charlas de sensibilización al personal sobre aspectos de seguridad tecnológica.
e) Participar en la implantación del programa de seguridad de la información de acuerdo a los lineamientos establecidos por el CGSI.
f) Identificar y gestionar los riesgos e incidentes de seguridad tecnológica.
g) Coordinar la ejecución del análisis de vulnerabilidades para los servicios tecnológicos y asegurar su tratamiento.
h) Asumir las funciones del OSI ante su ausencia.

**F. Responsables del Sistema de Gestión del órgano**

a) Coordinar con los involucrados del órgano al cual pertenecen respecto a la implementación del cumplimiento de la Política, objetivos y lineamientos de Seguridad de la Información y de las acciones de tratamiento de riesgos; a su vez, efectuar el seguimiento respectivo.
b) Proponer controles de seguridad durante la elaboración o actualización de las directivas, procedimientos e instructivos para mejorar los niveles de seguridad de la información existentes.
c) Apoyar en la gestión de los riesgos de seguridad de la información.
d) Respaldar durante las auditorías internas de seguridad de la información al personal auditado del órgano al cual pertenecen.
e) Coordinar con los involucrados del órgano la solución de incidentes de seguridad de la información dentro del alcance de sus competencias.
f) Capacitar y sensibilizar en temas de seguridad de la información al personal involucrado del órgano al cual pertenecen.
g) Difundir la Política, objetivos y lineamientos de Seguridad de la Información.
h) Durante la creación o actualización de procedimientos e instructivos, asegurar la segregación de tareas del personal involucrado para reducir los riesgos de modificaciones no autorizadas, así como del uso indebido de los activos de información.

**G. Encargado del Banco de Datos Personales**

a) Asegurar la implementación de los controles de seguridad de los datos personales según normas emitidas por la APDP.

**H. Oficial de Privacidad de la EREP**

a) Velar por la estricta observancia de la Política de Protección de Datos Personales de la ONPE dentro del ámbito de la EREP-ONPE.

b) Proponer la adopción de buenas prácticas en materia de protección de datos personales tratados por la EREP-ONPE.
c) Identificar las necesidades de capacitación y sensibilización para una adecuada protección de los datos personales, dentro del marco de los servicios de la EREP-ONPE.
d) Implementar las medidas correctivas en caso se identifique algún tipo de vulneración real o potencial, relacionado al tratamiento de los datos personales por la EREP-ONPE.
e) Coordinar permanentemente con el Encargado del Banco de Datos Personales de la ONPE las acciones o controles a implementar relacionados al tratamiento de los datos personales.
f) Reportar, a solicitud del Encargado del Banco de Datos Personales, las incidencias relacionadas al tratamiento de datos personales, así como el progreso de las acciones y controles a implementar por la EREP ONPE.

**I. Todo el personal en general**

a) Cumplir y hacer cumplir al personal a su cargo, a los proveedores de servicios y a los terceros con quienes coordine, las políticas, objetivos y lineamientos de seguridad de la información que apliquen de la presente directiva.
b) Participar en la implementación de la política, objetivos y lineamientos de seguridad de la información, así como de las acciones de tratamiento de riesgos y acciones correctivas de acuerdo al alcance de sus competencias.
c) Reportar los eventos, incidentes y debilidades de seguridad de la información de acuerdo a los procedimientos establecidos por la institución.

### 6.1.2. Dispositivos móviles institucionales

La GITE debe:

a) Configurar en los dispositivos móviles institucionales el tiempo de inactividad para el bloqueo automático del mismo; así como, algún método de seguridad para su desbloqueo (por ejemplo, contraseñas, biométricos, patrones, reconocimiento de voz).
b) Implementar controles criptográficos en los dispositivos móviles institucionales a solicitud de los usuarios cuando estos almacenen información laboral que no sea de carácter público.
c) Con respecto a los dispositivos móviles institucionales empleados en las Soluciones Tecnológicas de Voto Electrónico, asegurar que se implementen todos los controles de seguridad necesarios y adecuados para cada modalidad de votación electrónica con la finalidad de asegurar la confidencialidad, integridad y disponibilidad de la información.

Los usuarios deben:

d) Evitar el uso de los dispositivos móviles institucionales en lugares que no les ofrezcan las garantías de seguridad física necesarias, para evitar pérdida o robo de estos.

e) Evitar la modificación de las configuraciones de seguridad de los dispositivos móviles institucionales, ni la desinstalación del software provisto en ellos. De requerirlo, deben solicitárselas a la GITE.
f) Evitar el uso de redes inalámbricas públicas para prevenir riesgos de seguridad a la información almacenada en el dispositivo móvil institucional.
g) Realizar el respaldo de su información laboral almacenada en su dispositivo móvil institucional.

#### 6.1.3. Teletrabajo

a) Solo los usuarios que administran sistemas de información están permitidos a ingresar a estos, desde fuera de las instalaciones de la institución y mediante canales de comunicación seguros (encriptados) previa autenticación, para brindar soporte ante la pérdida o degradación del servicio, contando con la autorización de su propietario.

b) Los usuarios solo deben acceder desde fuera de las instalaciones de la institución a los sistemas de información previa autorización del responsable del órgano al cual pertenece.

### 6.2. Seguridad relacionada con los Recursos Humanos

La ONPE debe promover una cultura en seguridad de la información, de tal manera que las acciones del personal no conduzcan a poner en riesgo a la confidencialidad, integridad y disponibilidad de la información.

#### 6.2.1. Antes del empleo

a) La GCPH debe comprobar el cumplimiento de los requisitos del personal que ingresa a laborar en la institución, de acuerdo a las leyes y regulaciones vigentes, independientemente de su modalidad de contrato. Como mínimo, debe verificar, de acuerdo a los procedimientos establecidos, lo siguiente:

a.1) Validez del documento de identidad.
a.2) Que no cuenten con afiliación política y no se encuentren afectos a las incompatibilidades señaladas en el *articulo 16: Impedimentos para los funcionarios* de la Ley N° 26487, Ley de Orgánica de la Oficina Nacional de Procesos Electorales.
a.3) Otras que se determinen de acuerdo a las funciones que va a realizar.

b) La GCPH debe establecer en los acuerdos contractuales de empleo las cláusulas de confidencialidad, declaración de responsabilidades respecto a la seguridad de la información, cláusulas respecto a las leyes de derecho de autor o protección de datos, según corresponda. Dichos acuerdos contractuales deben estar vigentes por lo menos tres (3) años después de finalizado el contrato.

#### 6.2.2. Durante el empleo

La GCPH o la GIEE para el caso de personal de la ODPE, deben:

a) Incluir en su plan de inducción y capacitación aspectos de seguridad de la información según las políticas, normas y procedimientos relevantes relacionados, en coordinación con la GGC.

b) Asegurar, en coordinación con la GGC, que las inducciones y capacitaciones de seguridad de la información sean recibidas por el personal.

La GCPH debe:

c) A través de la Secretaria Técnica de Procedimientos Administrativos Disciplinarios[1] se procederá, previa presentación de una denuncia o informe ante los órganos competentes, con la aplicación del Procedimiento Administrativo Disciplinario, que establece la Ley del Servicio Civil y su reglamento, ante incumplimientos o faltas tipificadas en estos.

d) Realizar, en coordinación con la GGC, la inducción y de manera permanente la actualización de conocimientos relacionados con la seguridad de la información en el desarrollo de las funciones del personal de la ONPE.

El personal debe:

e) Cumplir con la política, objetivos y lineamientos de seguridad de la información emitidas en la presente directiva, así como con otras relacionadas. En caso de evidenciar una acción o evento que atente contra estas normas, debe comunicárselo al OSI.

### 6.2.3. Cese del empleo o cambio de puesto de trabajo

a) El personal, cuando cambie de puesto o termine su relación contractual con la institución, debe entregar o poner a disposición de su jefe inmediato (o a quien éste designe formalmente) todos los documentos físicos y electrónicos encargados y demás activos asociados a la información que se les haya entregado para el cumplimiento de sus funciones, así como su fotocheck e indumentarias que identifiquen a la institución. Corresponde al jefe inmediato verificar la información entregada por el personal.

b) La GCPH debe solicitar a la GITE, a la brevedad posible, la cancelación de las cuentas de acceso a los sistemas informáticos del personal cuya relación contractual se haya extinguido.

c) La GCPH deberá informar a la OSDN a la brevedad posible, la baja del personal que termine su relación contractual con la institución; y la actualización de la base de datos del personal para el control de acceso físico a las diferentes sedes de la institución.

d) La GITE y la OSDN deben, en lo que les corresponda, remover o bloquear todos los accesos físicos (permisos de acceso a lugares o sitios físicos, por

[1] Cargo designado por el titular de la institución. Las referencias de este cargo se encuentran en la Directiva Nº 02-2015-SERVIR/GPGSC Régimen Disciplinario y Procedimiento Sancionador de la Ley N° 30057, Ley del Servicio Civil.

ejemplo: llaves de puertas o de armarios) y lógicos (permisos de acceso a sistemas o información almacenada electrónicamente, por ejemplo: usuarios y claves de red, o de un sistema de información) cuando el personal cambie de puesto o termine su relación contractual con la institución.

### 6.3. Gestión de Activos

#### 6.3.1. Responsabilidad de los activos

Los responsables de los órganos de la institución deben asegurar que se elabore un inventario de activos de información.

Los propietarios de activos deben:

a) Mantener actualizado un inventario de sus activos de información, así como de clasificarlos (ver 6.3.2 Clasificación de la Información).

b) Informar el inventario de activos de información dentro del plazo de 48 horas, después de efectuada la actualización del mismo, al CGSI y a la SG

c) Asegurar el adecuado tratamiento y protección de los activos de información a su cargo.

Los usuarios deben:

d) Usar de forma ética y eficiente los activos de información que le sean asignados solo y exclusivamente para fines laborales, en cumplimiento con el marco normativo para evitar daños operativos, a la imagen o a otros intereses de la institución.

e) Evitar el uso de equipos informáticos de pertenencia personal para desempeñar sus actividades laborales.

f) Evitar la exposición o divulgación de la información confidencial, reservada o secreta que manejen, guardándolo bajo llave o caja fuerte, según amerite.

#### 6.3.2. Clasificación de la información

a) En concordancia con la Ley de Transparencia y Acceso a la Información Pública, es responsabilidad del titular de la ONPE o de los funcionarios designados por este, clasificar su información en: información secreta, reservada. Según Resolución Jefatural 086-2016-J/ONPE, se delegó a Secretaría General la facultad de clasificar y desclasificar como información SECRETA y RESERVADA los activos de información en posesión de la ONPE.
Los propietarios de activos son responsables de clasificar la información que manejan en cada proceso o proyecto, de acuerdo a lo establecido en la Ley de Transparencia y Acceso a la Información Pública.

Los propietarios de los activos deberán etiquetar la información según la clasificación realizada, y que sea conforme a los lineamientos que establezca la institución.

b) Los propietarios de activos deben asegurar el manejo de sus activos de acuerdo a lo siguiente:

| Para la información clasificada como secreta y reservada |
|---|
| i. Se debe ubicar en un ambiente que cuente con acceso biométrico o de acceso restringido con resguardo de un personal asignado por el órgano que custodia dicha información. |
| ii. Su almacenamiento debe ser mínimamente dentro de una caja fuerte (o algún otro mecanismo de seguridad similar) o ser cifrado (preferentemente con la última versión tecnológica existente), según corresponda. |
| iii. No se debe obtener copias físicas o electrónicas bajo ninguna circunstancia. |
| iv. Por lo tanto, tampoco se debe enviar por ningún medio electrónico. |
| **Para la información clasificada como confidencial** |
| v. Se debe ubicar en un ambiente que cuente con acceso restringido, registrándose los accesos a estos ambientes. |
| vi. Su almacenamiento debe ser mínimamente bajo llave (o algún otro mecanismo de seguridad similar) o ser cifrado (con la última versión tecnológica compatible con los sistemas institucionales), según corresponda. |
| vii. Se debe controlar las copias físicas o electrónicas registrándose, como mínimo, el número de identificación de la copia y de la persona quien la recibe. |
| viii. **Su envío solamente debe ser por correo electrónico institucional** y encriptado a direcciones de correos electrónicos institucionales autorizados por el propietario del activo. |

### 6.3.3. Gestión de medios de almacenamiento removibles

Los responsables de los órganos de la institución deben autorizar a su personal el uso de medios de almacenamiento removibles, en caso lo amerite. El cumplimiento de esta autorización está a cargo de la GITE.

## 6.4. Control de Accesos

Los propietarios de activos de información, incluyendo a la información en sí, deben asegurar que estos reciban los controles de accesos necesarios y adecuados sin degradación del flujo de las actividades de los procesos.

### 6.4.1. Gestión de acceso de usuario

Los responsables de los órganos de la institución deben:

a) Autorizar, y luego solicitar a la GITE el acceso a los sistemas de información para su personal, proveedor de servicios y terceros, indicando los niveles de acceso o privilegios.

b) Deberán solicitar a la GITE la cancelación de las cuentas de acceso a los servicios de tecnologías de la información otorgadas a proveedores y terceros una vez concluida la relación contractual o necesidad del servicio.

La GCPH debe:

a) Solicitar a la GITE la baja de las cuentas de acceso del personal cuando finalice la relación contractual.

La GITE debe:

b) Confirmar con la GCPH la relación contractual antes de otorgar el acceso a los sistemas de información solicitados.

c) Cancelar las cuentas de acceso una vez finalizada las labores del personal cesado, teniendo dos días hábiles de plazo a partir de la comunicación de la GCPH. Asimismo, cancelar las cuentas de acceso de proveedores y terceros previa solicitud del órgano que solicitó el servicio.

d) Coordinar la baja de las cuentas de acceso de los administradores de sistemas de información antes de su cese.

e) Llevar un registro del personal que cumple el rol de administrador de sistema de información.

Los administradores de sistemas de información deben:

f) Guardar el registro de la solicitud de autorización de acceso.

g) Revisar y mantener actualizado permanentemente los registros de cuentas de acceso a los sistemas de información que administran en coordinación con los Responsables del Sistema de Gestión de cada órgano.

El OSI debe:

h) Revisar semestralmente, en coordinación con el Responsable de la Seguridad Tecnológica, las cuentas de acceso de los administradores de los sistemas de información.

i) Revisar semestralmente, en coordinación con los Responsables del Sistema de Gestión de cada órgano, las cuentas de acceso de los usuarios de los sistemas de información.

### 6.4.2. Responsabilidades del usuario

Los usuarios de los sistemas de información[2] son responsables del uso correcto de las cuentas asignadas para el acceso a los sistemas o servicios informáticos de la institución, por lo tanto deben:

a) Cambiar las contraseñas proporcionadas por los administradores de los sistemas de información antes de su primer inicio de sesión.

b) Mantener la confidencialidad de su contraseña (no compartirlas) y cambiar la misma si tiene algún indicio de su vulnerabilidad.

c) Seleccionar una contraseña que cuente con un nivel adecuado de complejidad, siguiendo las siguientes consideraciones:

c.1) Debe tener una longitud mínima de ocho caracteres.
c.2) Debe ser una combinación de letras mayúsculas, minúsculas y números. De preferencia, incluir también caracteres especiales, evitando así el uso de palabras comunes o datos personales.

d) Evitar anotar sus contraseñas en medios físicos o electrónicos, a menos que éste cuente con algún control criptográfico.

e) Acceder a los sistemas de información de la ONPE solo desde equipos asignados por la institución.

### 6.4.3. Control de acceso a los sistemas de información

a) Los administradores de sistemas de información deben configurar tales sistemas considerando lo siguiente:

a.1) Que obliguen a los usuarios a cambiar su contraseña cuando ingrese por primera vez.
a.2) Que bloqueen el acceso por 15 minutos luego de 5 intentos fallidos.
a.3) Que permitan a los usuarios cambiar su contraseña cuando lo requiera.
a.4) Que obliguen a los usuarios cambiar su contraseña como máximo cada 60 días. En el caso de cuentas con privilegios de administrador, estas deben cambiarse cada 6 meses.
a.5) Que guarden un registro de los intentos fallidos y exitosos de acceso.
a.6) Para los sistemas de información de acceso desde fuera de las instalaciones, adicionalmente que bloqueen las cuentas que superen los 5 intentos fallidos de acceso.

b) Los administradores de sistemas de información deben solamente asignar a cada usuario una cuenta de acceso por sistema de información, salvo por razones de operación estrictamente justificados.

[2] Para las Soluciones Tecnológicas de Voto Electrónico corresponde a la GITE implementar los controles de seguridad necesarios y adecuados con la finalidad de asegurar la confidencialidad, integridad y disponibilidad de la información.

c) La GITE debe asegurar que sus desarrolladores solo tengan acceso a aquellas partes del código fuente del software que sea necesario para su trabajo.

### 6.5. Criptografía

El personal debe:

a) Enviar de manera encriptada la información electrónica que no sea de carácter público almacenada en medios tecnológicos, previa autorización de su propietario. Solicitar el apoyo de la GITE de ser necesario.

La GITE debe:

b) Implementar en los sistemas de información de acceso desde fuera de las instalaciones de la institución controles criptográficos que permitan:

b.1) Validar la integridad o identidad de los sistemas de información.
b.2) Una conexión segura para el caso que los sistemas de información requieran autenticación de los usuarios.
b.3) Proteger la integridad y confidencialidad de la información (este último de ser el caso) desde su transmisión hasta su recepción.

c) Encriptar la información que no sea de carácter público almacenada en las bases de datos.

d) Asegurar que los controles criptográficos de los sistemas de información adquiridos o desarrollados cumplan con los estándares nacionales o internacionales.

e) Asegurar que el medio de almacenamiento de los certificados digitales emitidos por una EC cumple con los estándares establecidos por la AAC.

### 6.6. Seguridad física y ambiental de las instalaciones

La ONPE tomará las medidas físicas y ambientales que sean necesarias y adecuadas dentro y fuera de sus instalaciones para proteger su información, junto con sus activos de tratamiento asociados más relevantes, contra riesgos que atenten contra su confidencialidad, integridad y disponibilidad.

#### 6.6.1. Seguridad asociada a las instalaciones

La OSDN debe a nivel nacional:

a) Realizar la evaluación correspondiente a fin de mantener asegurado el perímetro de las instalaciones, sobre todo, de las de tratamiento de información que no sea de carácter público. Asimismo, previa información de los órganos, debe evaluar y determinar los controles de seguridad a implementar por los órganos para la custodia de los activos de tratamiento de información.

b) A través de los Agentes de Vigilancia Privada – AVP, se verificará que el personal, proveedores y terceros, tanto en el ingreso como en su permanencia, porten visiblemente su fotocheck (laboral o visitante). Asimismo, debe coordinar con los demás órganos al respecto para que sea apoyada en los lugares en donde no se cuente con personal de seguridad y vigilancia.

c) A través de los Agente de Vigilancia Privada – AVP, se examinará el material que ingresa a la zona de despacho y recepción de materiales para detectar posible material explosivo, químico o algún otro peligroso antes que sea trasladado al ambiente de destino. Asimismo, coordinar con los demás órganos al respecto para que sea apoyada en los lugares en donde no se cuente con personal de seguridad y vigilancia.

Los responsables de los órganos de la institución deben:

d) Asegurar que sean registrados todos los accesos a las instalaciones no ocupadas permanentemente en donde se trate información que no sea de carácter público.

e) Asegurar que solamente exista una llave de contingencia de la puerta de acceso a las instalaciones de tratamiento de información que estén bajo su responsabilidad, y que sea custodiada por la OSDN.

f) Asegurar que los equipos de registro fotográfico, video, audio u otros, tales como cámaras en dispositivos móviles, no sean usados en los ambientes que determine, a menos que otorgue su autorización.

g) Asegurar que los proveedores y terceros que accedan a las instalaciones de tratamiento de información sensible solo usen el material estrictamente necesario para llevar a cabo las actividades acordadas.

h) Asegurar que los proveedores o los terceros no ingresen a las instalaciones de tratamiento de información sensibles sin la presencia del personal a cargo o de su representante.

i) Asegurar que los materiales peligrosos y combustibles sean almacenados en un área diferente a las instalaciones de tratamiento de información.

j) Asegurar que las puertas y ventanas exteriores e interiores estén protegidas contra accesos no autorizados, sobre todo en horas no laborales.

### 6.6.2. Seguridad asociada a los equipos institucionales

La OSDN debe:

a) Inspeccionar que los centros de datos cuenten con señaléticas de seguridad.

La GITE debe:

b) Monitorizar la temperatura y humedad de los centros de datos.

c) Asegurar el funcionamiento de los equipos de respaldo de energía eléctrica cuando falle o se corte el suministro de energía eléctrica principal.

d) Asegurar que durante el mantenimiento que realicen a los equipos servidores, no haya posibilidad de fuga de información.

e) Asegurar que se efectúe el mantenimiento a los equipos servidores, equipos de respaldo de energía eléctrica, de control de temperatura, entre otros, ubicados en los centros de datos.

f) Asegurar el mantenimiento de los equipos informáticos del personal.

g) Asegurar que los equipos informáticos institucionales involucrados en la prestación y realización de transacciones de gobierno electrónico, de acuerdo a la Ley de Certificados y Firmas Digitales, cuenten con algún tipo de certificado de dispositivo seguro emitidos por una EC debidamente acreditada ante el INDECOPI.

h) Asegurar que los medios de almacenamiento institucionales que custodian y que van a ser reutilizados, reemplazados o desechados —y, a su vez, que contengan información que no sea de carácter público o que contengan software con copia registrada (copyright)— sean destruidos físicamente o que su contenido sea borrado de manera irreversible.

Los responsables de los órganos de la institución a cargo del Archivo Central, del Archivo Electoral, y de otros espacios en donde se custodie información física o electrónica deben:

i) Asegurar que se efectúe el mantenimiento a los equipos e instrumentos que permiten la conservación de los medios en donde se soporta la información física y electrónica custodiada.

Los usuarios deben:

j) Efectuar, o solicitar a la GITE que puedan efectuar, una copia de respaldo de su información antes que el equipo informático institucional que le fue asignado sea reutilizado, reemplazado, desechado o pase a mantenimiento, y luego custodiarla de acuerdo a su nivel de clasificación. En caso de información que no sea de carácter público, esta debe ser eliminada de su equipo informático.

k) Evitar la apertura de los equipos informáticos; es decir, evitar acceder a los componentes internos de estos (solo el personal de soporte técnico podría hacerla en caso corresponda).

l) Evitar transportar equipos informáticos institucionales dentro o fuera de las instalaciones.

m) Asegurar que los medios de almacenamiento que custodian y que van a ser reutilizados, reemplazados o desechados —y, a su vez, que contengan

información que no sea de carácter público o que contengan softwares con copia registrada (copyright)— sean destruidos físicamente o que su contenido sea borrado de manera irreversible.

### 6.7. Seguridad de las operaciones

La ONPE tomará las medidas necesarias y adecuadas para asegurar la operación correcta y segura de sus activos de información y para prever la pérdida permanente de su información de negocio y de soporte.

La GGC debe:

a) Proponer a la GG los controles de seguridad de la información cuando se originen cambios en la organización y procesos de negocio.

La GITE debe:

b) Restringir el acceso de videos y música en línea (on-line) que no son de propósito laboral.

c) Asegurar que durante el ciclo de desarrollo de software se trabaje en ambientes de desarrollo, prueba y producción por separado y que se definan las reglas de transferencia a cada tipo de ambiente.

d) Asegurar que los equipos informáticos cuenten con un software contra códigos maliciosos y de actualización periódica.

e) Orientar a los usuarios sobre cómo afrontar un evento u ocurrencia de infección de virus informático.

f) Obtener periódicamente y etiquetar las copias de respaldo de información almacenada en los equipos servidores, así como efectuar las pruebas de restauración de la información de acuerdo a su plan respectivo (si se trata de información que no sea de carácter público, se debe contar con la presencia del Propietario o del representante que este designe).

g) Encriptar las copias de respaldo de la información que no sea de carácter público que obtenga desde los equipos servidores.

h) Ubicar las copias de respaldo de información en otro(s) local(es) distante(s) de la institución que cuenten con armarios seguros —sin perjuicio de contar también con sus duplicados en los mismos locales—, el(los) cual(es) debe(n) contar con controles de seguridad física y con adecuadas condiciones de temperatura y humedad.

i) Efectuar, a solicitud del personal, las copias de respaldo de la información almacenada en sus equipos informáticos.

j) Implementar los controles que aseguren que los eventos de sistemas de información (log) no sean manipulados por quienes los administran, tal como

la activación de registros de auditoría. Obtener las copias de seguridad de estos eventos (log) mensualmente.

k) Implementar controles de protección de privacidad de los datos personales almacenada en los eventos de sistemas de información (log).

l) Programar un análisis de vulnerabilidades técnicas de los sistemas de información más relevantes para cada proceso electoral que organice la institución; y programar las acciones necesarias para prevenir o mitigar los riesgos que se identifiquen producto de éste análisis.

m) Restringir el otorgamiento de privilegios sobre el manejo de los equipos informáticos al personal cuya función no la requiere para evitar instalaciones de software que pueden acarrear incidentes de seguridad de la información y violaciones de derechos de propiedad intelectual.

n) Restringir que las pruebas a los sistemas de información durante una revisión estén limitadas a accesos de solo lectura al software. Asimismo, asegurar, en caso se requiera acceso de escritura, se efectúe una copia de respaldo, y luego se elimine o se resguarde, según sea el caso, al culminar la revisión.

o) Asegurar que las revisiones a los sistemas de información a efectuar con datos confidenciales sean dentro de las instalaciones de la institución acompañado por el responsable del sistema de información revisado; no está permitido la entrega de este tipo de datos.

p) Asegurar que la capacidad y desempeño de la infraestructura de TI, pueden soportar eficientemente las demandas de los servicios de TI y recursos tecnológicos requeridos por la ONPE.

Los usuarios deben:

q) Realizar la copia de respaldo de su información con apoyo del personal de soporte técnico, y deben guardarlo bajo las condiciones de acuerdo a su nivel de clasificación (referencia: 6.3.2. Clasificación de la información).

r) Solicitar a la GITE el almacenamiento de su información necesaria o indispensable en el servidor de archivos.

s) Acatar las directrices de buen uso de software institucional emitidas por la GITE.

### 6.8. Seguridad relacionada a las comunicaciones

La ONPE implementará las medidas necesarias y adecuadas en los medios de transporte y de reproducción, tecnológicos o no, de la información, de tal manera que solo sea emitida y recibida íntegramente por las personas apropiadas en el momento y lugar oportunos.

La GITE debe:

a) Asegurar que los identificadores otorgados a las redes inalámbricas de la institución no contengan relación con esta. Asimismo, que el acceso a estas redes sea configurado con contraseña encriptada.

El personal debe:

b) Asegurar que la información que no sea de carácter público que vayan a adjuntar a su correo electrónico institucional solamente sea enviada con controles criptográficos según su nivel de clasificación (referencia: 6.3.2 Clasificación de la información). Bajo ningún motivo deben usar medios de mensajería que no sean institucionales.

c) Acatar las directrices de buen uso de correo electrónico institucional emitidas por la GITE.

d) Asegurar que la información que no sea de carácter público solamente sea compartida entre los usuarios autorizados por el propietario de la información.

e) Evitar que la información que no sea de carácter público sea abandonada en las instalaciones de impresión (impresoras, fotocopiadoras, faxes) o que sea grabada en máquinas contestadoras.

f) Evitar conversaciones de temas confidenciales en lugares públicos u oficinas abiertas.

g) Lacrar los sobres que envien si contienen información que no sea de carácter público.

Los responsables de los órganos de la institución deben:

h) Asegurar el uso de un acuerdo de confidencialidad y no divulgación cuando requieran transferir información que no sea de carácter público con algún otro órgano, unidad orgánica o entidad.

## 6.9. Adquisición, desarrollo y mantenimiento de sistemas de información

### 6.9.1. Requerimientos de seguridad de los sistemas de información

Los líderes usuarios de los sistemas de información deben:

a) Identificar y documentar con asesoría de la GITE, los requerimientos de seguridad en las etapas iniciales del proyecto de adquisición o desarrollo de software.

La GITE debe:

b) Asegurar que los cambios a realizar, solicitados previa y formalmente por los líderes usuarios, no causen riesgos de seguridad (de ocurrir, debe deshabilitarlos para su posterior subsanación).

c) Validar nuevamente, en caso se hayan producido cambios en el software, los datos de entrada y los datos de salida esperados.

#### 6.9.2. Seguridad en el desarrollo y en los procesos de soporte

La GITE debe:

a) Involucrar la seguridad en las metodologías de desarrollo de software que se usen, así como implementar el control de versiones.

b) Asegurar que las actualizaciones de los componentes del sistema operativo no interrumpan la funcionalidad de los sistemas de información adquiridos o desarrollados.

#### 6.9.3. Datos de prueba

La GITE debe:

a) Asegurar que los datos personales utilizados en los ambientes de desarrollo y de prueba sean sometidos a procedimientos de anonimización o disociación antes de su uso.

b) No hacer uso de datos personales sensibles para propósitos de pruebas.

### 6.10. Relación con proveedores

#### 6.10.1. Seguridad con relación a los proveedores

Los responsables de los órganos de la institución que requieren la contratación de bienes y servicios relacionados con el acceso, procesamiento, almacenamiento, comunicación y otro tipo de tratamiento de información deben:

a) Asegurar la incorporación de requerimientos de seguridad (organizativos, jurídicos y técnicos) en los términos de referencia con asesoría de la GITE o del OSI. Tales requerimientos principalmente deben estar asociados a la transferencia de o acceso a información, la resolución de incidentes, las medidas de contingencia o a los controles de cambios, así como el derecho para efectuar auditorías al servicio brindado.

b) Asegurar que el proveedor (directo y subcontratado) que tratará información que no sea de carácter público conozca las políticas y procedimientos de seguridad que le sean aplicables, y que firme un acuerdo de confidencialidad y de no divulgación.

c) Asegurar que no manipulen cualquier tipo de documento no relacionado al motivo del servicio contratado, así como su copia (transcripción, fotocopia, fotografía, entre otros).

La SG, de acuerdo a lo establecido en los artículos 15, 16 y 17 de la Ley de Transparencia y Acceso a la Información Pública, para la información que no sea de carácter público que ingrese a la institución, debe:

d) Registrar solamente los datos que figuran en el sobre y no escanear o fotocopiar la información contenida en él.

e) Entregar la información entrante manteniendo el sobre cerrado al órgano destinatario, registrando previamente la hora de salida de la información de la mesa de partes.

### 6.10.2. Gestión de entrega de servicio del proveedor

a) Los responsables de los órganos de la institución deben asegurar el seguimiento a los niveles de desempeño del servicio, así como el cumplimiento de los requerimientos de seguridad de la información incorporados en los términos de referencia.

## 6.11. Gestión de incidentes de seguridad de la información

a) El personal, proveedores de servicios y terceros deben reportar todo tipo de eventos relacionados a la seguridad de la información, tecnológicos o no, al punto de contacto indicado en los procedimientos relacionados.

b) Los usuarios deben reportar a la OSI indicios de debilidades de seguridad de los sistemas de información. No deben intentar comprobar estos indicios para prevenir daños a la institución.

c) La OSI en coordinación con los órganos involucrados, deben evaluar mensualmente los eventos reportados para determinar si se clasifican como incidentes de seguridad de la información, analizando su causa raíz, probabilidad e impacto.

d) La GITE debe reportar los incidentes informáticos a la PeCERT según lo señalado en el procedimiento de esta autoridad, así como asegurar que se atiendan los avisos de alerta que envía esta.

## 6.12. Seguridad la información asociada a la continuidad de negocio

La ONPE asegurará que la confidencialidad, integridad y disponibilidad de su información no se degraden durante un hecho catastrófico de origen natural o humano.

### 6.12.1. Continuidad de la seguridad de la información

a) El Grupo de Trabajo de la Gestión del Riesgo de Desastres de la ONPE a través del "Plan de Continuidad Operativa", en coordinación con los demás órganos de la ONPE, deben elaborar un plan que busque proteger físicamente los activos de información, principalmente a los que acarreen catastróficos perjuicios; y deben asegurar la continuidad de los sistemas de información ante desastres naturales y ocasionados por el hombre, incluyendo aspectos relacionados a la continuidad de la confidencialidad, integridad y disponibilidad de la información, de tal forma que se mantengan sus requerimientos también en situaciones adversas.

b) El Grupo de Trabajo de la Gestión del Riesgo de Desastres de la ONPE a través del "Plan de Continuidad Operativa", en coordinación con los demás órganos, deben implementar lo contemplado en el plan relacionado a la continuidad de las operaciones de la institución, cuyo contenido debe incorporar, además de los requisitos legales aplicables, la estructura organizativa, procedimientos de respuesta y restauración, así como los controles que aseguren el nivel requerido de continuidad de la seguridad de la información durante una situación adversa.

c) La GITE, en coordinación con órganos propietarios de los sistemas de información, debe efectuar pruebas del plan de continuidad para verificar la eficacia de los controles por lo menos una vez al año o una vez en cada proceso electoral que organice la institución.

### 6.12.2. Redundancias

a) La GITE debe aplicar la redundancia a nivel de enlace de telecomunicaciones, servidores, base de datos, y otros recursos tecnológicos que asegure la continuidad de los sistemas de información que considere indispensables o necesarios. Asimismo, debe comprobar que los componentes redundantes operan ante la caída de los principales.

b) Los dueños de los procesos, en coordinación con la GGC y la GITE, deben establecer los requisitos de seguridad de la información y de continuidad para sus procesos considerando las situaciones adversas a las que pueden estar expuestas.

## 6.13. Cumplimiento

### 6.13.1. Cumplimiento de los requisitos legales y contractuales

La GITE debe:

a) Impedir que se instale software que atente contra los derechos de propiedad intelectual.

b) Llevar un registro de licencias de software y mantener las evidencias de estas.

c) Implementar controles que aseguren que el número máximo de usuarios permitidos con licencias no sea excedido.

Todos los órganos y unidades orgánicas que difundan o compartan documentos ofimáticos deben:

d) Eliminar la información de privacidad almacenada ocultamente en el software ofimático.

La SG debe:

e) Realizar los trámites de inscripción de los bancos de datos personales creados, así como para los que se generen.

Todos los órganos y unidades orgánicas que tratan datos personales de los electores o potenciales electores deben efectuar su tratamiento de acuerdo a las normas legales vigentes y lo estipulado en la Política de Protección de Datos Personales. En esta línea deben:

f) Obtener el consentimiento libre, previo, expreso, informado e inequívoco del titular para el tratamiento de sus datos con el fin de recolectar, transferir, almacenar, usar, circular, suprimir, compartir, actualizar o transmitir dichos datos personales en el marco de las actividades de la institución.

g) Gestionar la implementación de los controles de tratamiento y de protección de los datos personales que administran según las directivas emitidas por la APDP y los documentos normativos de la institución.

h) Acatar las disposiciones del Encargado de Banco de Datos Personales para el cumplimiento de la LPDP.

La GITE debe:

i) Implementar los controles de protección de los datos personales almacenada en las bases de datos o que se transmiten electrónicamente según lo establecido en la directiva emitida por la APDP.

Todos los órganos y unidades orgánicas que reciban o importen datos personales deben:

j) Implementar las medidas de seguridad definidas por el emisor o exportador de datos personales. La aceptación de la implementación de las medidas de seguridad debe establecerse por escrito mediante cláusulas contractuales u otro instrumento jurídico.

Todos los órganos y unidades orgánicas que emitan o exporten datos personales deben:

k) Disponer cláusulas contractuales u otro instrumento jurídico en los que se establezcan cuando menos las mismas obligaciones a la que se deben encontrar sujetos los receptores o importadores de los datos personales.

La GCPH debe:

l) Cumplir con las disposiciones de seguridad de los bancos de datos personales de la administración del personal emitidas por la directiva de la APDP.

### 6.13.2. Revisión independiente de la seguridad de la información

La GGC debe:

a) Planificar las auditorías internas y externas de seguridad de la información para que se lleven a cabo una vez al año mínimamente y con auditores independientes al proceso a auditar.

b) Reportar los resultados de la revisión independiente a los interesados para la atención de los hallazgos encontrados.

## 7. MECÁNICA OPERATIVA

Los procedimientos e instructivos que se elaboren deben cumplir lo dispuesto en la presente directiva.

## 8. CUADRO DE CONTROL DE CAMBIOS

| Versión Anterior | Fecha de Aprobación | Sección / Ítem | Categoría N: Nuevo M: Modificado E: Eliminado | Principales cambios realizados con respecto a la versión anterior |
|---|---|---|---|---|
| 00 | 22/12/2015 | Título | M | Se cambia la Directiva DI03-GGC/GC Política de Seguridad de la Información (versión 00) aprobada por Resolución Jefatural N° 000370-2015-J/ONPE del 22/12/2015 por la DI04-GGC/GC Lineamientos de Seguridad de la Información (versión 00) |
| 00 | 22/12/2015 | Título | E | Extrayendo del documento el numeral 6.1. Política general de seguridad de la información de la DI03-GGC/GC. |