**RESOLUCIÓN DE JEFATURA N.° 036 -2018-OSINFOR**

Lima, 14 NOV. 2018

**VISTOS:**

El Informe N.° 041-2018-OSINFOR/05.1, de fecha 01 de octubre de 2018, de la Oficina de Tecnología de la Información, el Informe N.° 096-2018-OSINFOR/04.1, de fecha 11 de octubre de 2018, de la Oficina de Planificación y Presupuesto y el Memorándum N.° 347-2018-OSINFOR/04.2, de fecha 15 de octubre de 2018, de la Oficina de Asesoría Jurídica, y;

**CONSIDERANDO:**

Que, el Decreto Legislativo N.° 1085, crea el Organismo de Supervisión de los Recursos Forestales y de Fauna Silvestre - OSINFOR, encargado a nivel nacional de la supervisión y fiscalización del aprovechamiento sostenible y la conservación de los recursos forestales y de fauna silvestre, así como de los servicios ambientales provenientes del bosque, otorgados por el Estado;

Que, en el marco de la Política Nacional de Modernización de la Gestión Pública, aprobada por Decreto Supremo N.° 004-2013-PCM, la entidad viene implementando la norma ISO/IEC 27001:2013 orientada a establecer un sistema gerencial que permita minimizar el riesgo y proteger la información institucional, de amenazas externas o internas;

Que, mediante Resolución Ministerial N.° 004-2016-PCM, se aprobó el uso obligatorio de la Norma Técnica Peruana "NTP ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 2ª Edición", en todas las entidades integrantes del Sistema Nacional de Informática; siendo pertinente señalar, que la NTP ISO/IEC 27001:2014 corresponde a la traducción de la Norma Internacional ISO/IEC 27001:2013;

Que, el artículo 3° de la Resolución Ministerial N.° 166-2017-PCM, estipula que las entidades comprendidas en el artículo 1° de la Resolución Ministerial N.° 004-2016-PCM, deben asegurar la implementación del Sistema de Gestión de Seguridad de la Información en su institución, priorizando en el alcance los procesos misionales y aquellos que sean relevantes para su operatividad;

Que, la Cláusula 6.1.3 de la NTP ISO/IEC 27001:2014, establece que la organización debe definir y aplicar un proceso de tratamiento de riesgos de seguridad de la información para determinar todos los controles que sean necesarios para implementar las opciones elegidas de tratamiento de riesgos de seguridad de la información;

Que, como parte de la implementación de las normas ISO 9001:2015 Sistema de Gestión de Calidad (SGC) y 27001:2013 Sistema de Gestión de Seguridad de la Información (SGSI), se aprobó la Política SIG-E1-POL-001-V.01, "Política del Sistema Integrado de Gestión del OSINFOR" a través de la Resolución Presidencial N.° 121-2018-OSINFOR, de fecha 26 de julio de 2018, la cual establece como compromisos de la Alta Dirección; entre otros, el cumplimiento de los requisitos aplicables a los servicios de la Entidad, el cumplimiento de los requisitos legales vigentes, la búsqueda de la mejora de los procesos y la eficacia del Sistema Integrado de Gestión - SIG;

Que, en la línea de lo expuesto, la Oficina de Tecnología de la Información mediante informe de vistos, da cuenta del Acta N.° 002, de fecha 29 de agosto de 2018, de los miembros del Comité de Gestión de Seguridad de la Información, liderado por el Oficial de Seguridad de la Información, en la cual validaron y propusieron las dieciséis (16) Políticas para la Seguridad de

la Información que se detallan en el Cuadro N.° 01 de la presente resolución, con la finalidad de dar cumplimiento a la NTP ISO/IEC 27001:2014 Sistemas de Gestión de Seguridad de la Información; recomendando que la aprobación de las políticas en mención sea con eficacia anticipada al 29 de agosto de 2018;

Que, por su parte, la Oficina de Planificación y Presupuesto, mediante informe de vistos, concluye que el acotado documento de gestión ha sido verificado sin objeción alguna para su aprobación; indicando además que el documento se encuentra acorde a lo establecido en la Directiva SIG-E2-DIR-001-V.01 "Directiva de control de documentos del OSINFOR", aprobada por Resolución Presidencial N.° 110-2018-OSINFOR;

Que, mediante documento de vistos la Oficina de Asesoría Jurídica otorga conformidad a las Dieciséis (16) Políticas para la Seguridad de la Información del OSINFOR, propuestas por el Comité de Gestión de Seguridad de la Información, recomendando su aprobación con eficacia anticipada al 29 de agosto de 2018, de conformidad al artículo 17° del Texto Único Ordenado de la Ley N.° 27444, Ley del Procedimiento Administrativo General, aprobado por Decreto Supremo N.° 006-2017-JUS;

Que, conforme al artículo 51° del Decreto Legislativo N.° 1451 concordante con el literal a) del artículo 7° del Reglamento de Organización y Funciones del OSINFOR, aprobado por Decreto Supremo N.° 029-2017-PCM, es función de la Jefatura del OSINFOR, aprobar la política institucional, instrumentos normativos y documentos de gestión en el ámbito de competencia de la Entidad;

Con las visaciones de la Gerencia General y de las Oficinas de Tecnología de la Información, de Planificación y Presupuesto y de Asesoría Jurídica, y;

De conformidad con lo dispuesto en el Decreto Legislativo N.° 1085, Ley que crea el Organismo de Supervisión de los Recursos Forestales y de Fauna Silvestre - OSINFOR y su Reglamento de Organización y Funciones, aprobado por Decreto Supremo N.° 029-2017-PCM y la Resolución de Jefatura N.° 010-2018-OSINFOR;

**SE RESUELVE:**

**ARTÍCULO 1.- APROBAR**, con eficacia anticipada al 29 de agosto de 2018, Dieciséis (16) Políticas para la Seguridad de la Información del Organismo de Supervisión de los Recursos Forestales y de Fauna Silvestre - OSINFOR, detalladas en el Cuadro N.° 01, que en anexo forman parte integrante de la presente resolución.

**ARTÍCULO 2.- NOTIFICAR** la presente resolución a todos los órganos y unidades orgánicas del OSINFOR, para su conocimiento y cumplimiento según corresponda.

**ARTÍCULO 3.- DISPONER** que la Oficina de Tecnología de la Información publique la presente resolución en el Portal Institucional www.osinfor.gob.pe

Regístrese y comuníquese,

**MÁXIMO SALAZAR ROJAS**
Jefe (e)
Organismo de Supervisión de los Recursos Forestales y de Fauna Silvestre - OSINFOR

CUADRO N.° 01
Políticas para la Seguridad de la Información del OSINFOR

| N° | Código | Documento |
|---|---|---|
| 1 | SGSI-A5-POL-001-V.01 | Política de Organización de la Seguridad de la Información |
| 2 | SGSI-A5-POL-002-V.01 | Política de Seguridad en Dispositivos Móviles |
| 3 | SGSI-A5-POL-003-V.01 | Política de Seguridad Ligada a los Recursos Humanos |
| 4 | SGSI-A5-POL-004-V.01 | Política de Gestión de Activos |
| 5 | SGSI-A5-POL-005-V.01 | Política de Control de Accesos |
| 6 | SGSI-A5-POL-006-V.01 | Política de Criptografía |
| 7 | SGSI-A5-POL-007-V.01 | Política de Seguridad Física y del Ambiente |
| 8 | SGSI-A5-POL-008-V.01 | Política de Pantallas y Escritorios Limpios |
| 9 | SGSI-A5-POL-009-V.01 | Política de Seguridad de las Operaciones |
| 10 | SGSI-A5-POL-010-V.01 | Política de Seguridad de las Comunicaciones |
| 11 | SGSI-A5-POL-011-V.01 | Política de Adquisición, Desarrollo y Mantenimiento de Sistemas de Información |
| 12 | SGSI-A5-POL-012-V.01 | Política de Ingeniería de Software |
| 13 | SGSI-A5-POL-013-V.01 | Política de Relación con Proveedores |
| 14 | SGSI-A5-POL-014-V.01 | Política de Gestión de Incidentes de Seguridad de la Información. |
| 15 | SGSI-A5-POL-015-V.01 | Política de Aspectos de Seguridad de la Información en la Continuidad del Negocio |
| 16 | SGSI-A5-POL-016-V.01 | Política de Cumplimiento |

# POLÍTICA DE ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

**DOCUMENTO CONTROLADO**

| | | | |
|---|---|---|---|
| Propuesto por: | Gestión de Tecnologías de la Información | Fecha de propuesta: | 29 AGO. 2018 |
| Aprobado por: | Jefatura del OSINFOR (antes Presidencia Ejecutiva)[1] | Fecha de aprobación: | |

[1] Decreto Legislativo N° 1085 Artículo 51.- "Modificación de los artículos 6 y 7 del OSINFOR"

## Índice

## POLÍTICA DE ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

I. **Objetivos** ..... 3

II. **Alcance** ..... 3

III. **Política** ..... 3

**3.1 Organización Interna** ..... 3

**Control de cambios** ..... 4

# POLÍTICA DE ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

## I. Objetivos

Establecer un marco de gestión para iniciar y controlar la implementación y operación de seguridad de la información dentro del OSINFOR.

## II. Alcance

El alcance de la presente política de seguridad de la información abarca todos los aspectos administrativos y de control que debe ser conocida y cumplida por los directivos, personal que labora designado o contratado, así como por terceros que presten algún servicio al OSINFOR.

## III. Política

El OSINFOR debe mantener una organización interna que le permita prevenir, detectar y responder apropiadamente a eventos de seguridad de la información. Para ello, es necesario que se definan las responsabilidades del personal en el contexto de la seguridad de la información.

### 3.1 Organización Interna

#### 3.1.1 Funciones y responsabilidades de la seguridad de la información

Se han establecido los roles y funciones en el OSINFOR para el cumplimiento de la normatividad vigente, las que se detallan en el Manual de Funciones y Responsabilidades del Sistema de Gestión de la Seguridad de la Información (SGSI-A5-MAN-001).

#### 3.1.2 Separación de funciones

Se cuentan con responsabilidades definidas para segregar funciones y así reducir los riesgos por mal uso de los activos de Seguridad de la información del OSINFOR.

#### 3.1.3 Contacto con autoridades

a) A efectos de intercambiar experiencias y obtener asesoramiento para el mejoramiento de las prácticas y controles de seguridad de la información, se mantendrán contactos con los Organismos relacionados en temas relativos a la seguridad de la información, los cuales se encuentran detallados en el Formato Contactos de Autoridades y Grupos de Interés del SGSI (SGSI-A5-FOR-001).
b) En los intercambios de información relacionada a seguridad de la información, no se divulgará información confidencial perteneciente al OSINFOR a personas no autorizadas.
c) Para el intercambio de información confidencial para fines de asesoramiento o de intercambio de experiencias, sólo se permitirá cuando se haya firmado previamente un Acuerdo de Confidencialidad con aquellas Organizaciones relacionadas en temas relativos a la seguridad de la información para cuyo

efecto, el personal también está obligado a mantener la confidencialidad de los temas que se tratan.

### 3.1.4 Contacto con grupos de interés especial

Para intercambiar experiencias y obtener asesoramiento para el mejoramiento de las prácticas y controles de seguridad de la información, se mantendrán contactos apropiados con grupos de interés especial y otros foros especializados en seguridad de la información que se encuentran detallados en el Formato Contactos de Autoridades y Grupos de Interés del SGSI (SGSI-A5-FOR-001).

### 3.1.5 Seguridad de la información en gestión de proyectos

El OSINFOR integra la seguridad de la información en la gestión de proyectos para garantizar que los riesgos de seguridad de la información, los cuales deberán ser identificados en una fase temprana y ser tratados oportunamente. Los tipos de proyectos a los que se va a realizar inicialmente la apreciación de riesgos son de los procesos misionales, de Tecnología de la Información y de gestión de instalaciones físicas.

**Control de cambios**

| Versión | Fecha | Justificación[1] | Textos Modificados[2] | Responsable[3] |
|---|---|---|---|---|
| 01 | Elaboración inicial del documento | | | Oficina de Tecnología de la Información |
| | | | | |
| | | | | |

[1] Justificación de la nueva versión del documento, puede darse en los casos de a) Modificación, b) Actualización c) Reestructuración

[2] Señalar los párrafos, secciones literales que se han modificado e incorporado

[3] Señalar el dueño del proceso, indicar el documento o informe sustentatorio

# POLÍTICA DE ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

**DOCUMENTO CONTROLADO**

| | | | |
|---|---|---|---|
| Propuesto por: | Gestión de Tecnologías de la Información | Fecha de propuesta: | 29 AGO. 2018 |
| Aprobado por: | Jefatura del OSINFOR (antes Presidencia Ejecutiva)[1] | Fecha de aprobación: | |

[1] Decreto Legislativo N° 1085 Artículo 51.- "Modificación de los artículos 6 y 7 del OSINFOR"

## Índice

## POLÍTICA DE ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

I. **Objetivos** ..... 3

II. **Alcance** ..... 3

III. **Política** ..... 3

**3.1 Organización Interna** ..... 3

**Control de cambios** ..... 4

# POLÍTICA DE ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

## I. Objetivos

Establecer un marco de gestión para iniciar y controlar la implementación y operación de seguridad de la información dentro del OSINFOR.

## II. Alcance

El alcance de la presente política de seguridad de la información abarca todos los aspectos administrativos y de control que debe ser conocida y cumplida por los directivos, personal que labora designado o contratado, así como por terceros que presten algún servicio al OSINFOR.

## III. Política

El OSINFOR debe mantener una organización interna que le permita prevenir, detectar y responder apropiadamente a eventos de seguridad de la información. Para ello, es necesario que se definan las responsabilidades del personal en el contexto de la seguridad de la información.

### 3.1 Organización Interna

#### 3.1.1 Funciones y responsabilidades de la seguridad de la información

Se han establecido los roles y funciones en el OSINFOR para el cumplimiento de la normatividad vigente, las que se detallan en el Manual de Funciones y Responsabilidades del Sistema de Gestión de la Seguridad de la Información (SGSI-A5-MAN-001).

#### 3.1.2 Separación de funciones

Se cuentan con responsabilidades definidas para segregar funciones y así reducir los riesgos por mal uso de los activos de Seguridad de la información del OSINFOR.

#### 3.1.3 Contacto con autoridades

a) A efectos de intercambiar experiencias y obtener asesoramiento para el mejoramiento de las prácticas y controles de seguridad de la información, se mantendrán contactos con los Organismos relacionados en temas relativos a la seguridad de la información, los cuales se encuentran detallados en el Formato Contactos de Autoridades y Grupos de Interés del SGSI (SGSI-A5-FOR-001).
b) En los intercambios de información relacionada a seguridad de la información, no se divulgará información confidencial perteneciente al OSINFOR a personas no autorizadas.
c) Para el intercambio de información confidencial para fines de asesoramiento o de intercambio de experiencias, sólo se permitirá cuando se haya firmado previamente un Acuerdo de Confidencialidad con aquellas Organizaciones relacionadas en temas relativos a la seguridad de la información para cuyo

efecto, el personal también está obligado a mantener la confidencialidad de los temas que se tratan.

### 3.1.4 Contacto con grupos de interés especial

Para intercambiar experiencias y obtener asesoramiento para el mejoramiento de las prácticas y controles de seguridad de la información, se mantendrán contactos apropiados con grupos de interés especial y otros foros especializados en seguridad de la información que se encuentran detallados en el Formato Contactos de Autoridades y Grupos de Interés del SGSI (SGSI-A5-FOR-001).

### 3.1.5 Seguridad de la información en gestión de proyectos

El OSINFOR integra la seguridad de la información en la gestión de proyectos para garantizar que los riesgos de seguridad de la información, los cuales deberán ser identificados en una fase temprana y ser tratados oportunamente. Los tipos de proyectos a los que se va a realizar inicialmente la apreciación de riesgos son de los procesos misionales, de Tecnología de la Información y de gestión de instalaciones físicas.

**Control de cambios**

| Versión | Fecha | Justificación[1] | Textos Modificados[2] | Responsable[3] |
|---|---|---|---|---|
| 01 | Elaboración inicial del documento | | | Oficina de Tecnología de la Información |
| | | | | |
| | | | | |

[1] Justificación de la nueva versión del documento, puede darse en los casos de a) Modificación, b) Actualización c) Reestructuración

[2] Señalar los párrafos, secciones literales que se han modificado e incorporado

[3] Señalar el dueño del proceso, indicar el documento o informe sustentatorio

# POLÍTICA DE SEGURIDAD EN DISPOSITIVOS MOVILES

**DOCUMENTO CONTROLADO**

| | | | |
|---|---|---|---|
| Propuesto por: | Gestión de Tecnologías de la Información | Fecha de propuesta: | 29 AGO. 2018 |
| Aprobado por: | Jefatura del OSINFOR (antes Presidencia Ejecutiva)[1] | Fecha de aprobación: | |

(1) Decreto Legislativo N° 1085 Artículo 51.- "Modificación de los artículos 6 y 7 del OSINFOR"

Índice

## POLÍTICA DE SEGURIDAD EN DISPOSITIVOS MOVILES

I. Objetivos ..... 3
II. Alcance ..... 3
III. Política ..... 3
3.1. Identificación de los dispositivos móviles ..... 3
3.2. Instalación y Configuración de Aplicaciones ..... 4
3.3. Autenticación y Acceso ..... 4
3.4. Actualización ..... 4
3.5. Controles Físicos ..... 4
3.6. Seguridad del Sistema Operativo ..... 4
3.7. Responsabilidad de los servidores y usuarios ..... 4
Control de cambios ..... 5

# POLÍTICA DE SEGURIDAD EN DISPOSITIVOS MOVILES

## I. Objetivos

Garantizar la seguridad de la información asegurando su integridad, disponibilidad y el buen uso de los dispositivos móviles usados en el OSINFOR.

## II. Alcance

La política de seguridad de dispositivos móviles debe ser conocida y cumplida por los directivos, personal que labora designado o contratado, así como por terceros que presten algún servicio al OSINFOR, respecto de las actividades de aseguramiento en el uso y administración de los dispositivos móviles y removibles.

Dispositivo móvil, se considera a los dispositivos que contenga un sistema operativo incluye: laptops, notebooks, tablets, Ipads, teléfonos celulares, equipos GPS portátiles, cámaras digitales, etc.

Dispositivo de almacenamiento removible, se considerará a tarjetas de memoria, dispositivo de almacenamiento masivo USB basados en memoria flash, en Discos magnéticos, discos Solidos, ópticos tales como CDs, DVDs, Cintas Tapes y cualquier dispositivo de almacenamiento de conexión, USB, dispositivos criptográficos.

Esta lista no es taxativa, ya que deben incluirse todos los dispositivos que pudieran contener información confidencial y/o interna del OSINFOR y, por lo tanto, ser pasibles de sufrir un incidente en el que se comprometa la seguridad del mismo.

## III. Política

### 3.1. Identificación de los dispositivos móviles

a) Si el dispositivo móvil o removible tiene código patrimonial del OSINFOR, el Especialista de Control Patrimonial registra el Formato N° 01 Acta de Asignación de Bienes en Uso o Formato N° 02 Autorización de Desplazamiento interno de Bienes Patrimoniales[1] los dispositivos móviles que asigna a los Servidores.
b) En el caso que un servidor tenga la necesidad de trabajar con su propio dispositivo móvil, el equipo deberá cumplir con los criterios de seguridad de la información aplicados a los equipos similares del OSINFOR, y para su uso debe de completar la información requerida en el Formato N° 05 Declaración Jurada de Bienes y Equipos de Propiedad Particular[1].
c) En el caso de los dispositivos removibles que no tengan código patrimonial del OSINFOR o sean de propiedad Particular, el servidor o contratista es responsable y está obligado sobre cumplimiento de la confidencialidad, integridad y disponibilidad de la información que contengan.

[1] Directiva de administración, control y asignación en uso de bienes muebles de propiedad del OSINFOR vigente.

### 3.2. Instalación y Configuración de Aplicaciones

a) El proceso de instalación y configuración de las aplicaciones de los dispositivos móviles será realizado por la Oficina de Tecnología de la Información.
b) Las características en las capacidades de los equipos serán definidos en función de la importancia de la información procesada o almacenada según el tipo de usuario que utiliza un dispositivo móvil de la institución.

### 3.3. Autenticación y Acceso

a) Se protege el acceso a los dispositivos móviles según los privilegios de cada perfil de usuario (passwords). Las capacidades del equipo respecto del control de acceso, son definidas en función de la importancia de la información que se accede, se almacena o se protege en cada equipo.

### 3.4. Actualización

a) Todos los usuarios de dispositivos móviles utilizarán la última o la más segura versión de las aplicaciones, así mismo, contarán con servicios de soporte del fabricante.

### 3.5. Controles Físicos

a) El personal protege sus dispositivos móviles, no debiendo entregarlos a otra persona, en particular en aquellos dispositivos inteligentes que almacenan información sensible de la Institución. En estos casos, incluso los mensajes recibidos de números o remitentes desconocidos deben ser denegados y borrados sin ser abiertos.

b) Equipos Servidores, equipos personales y laptops de la Institución, restringirán y asegurarán la autenticidad e integridad en las conexiones con equipos móviles.

### 3.6. Seguridad del Sistema Operativo

a) En el caso de dispositivos móviles que almacenan información sensible se podrá considerar:

i. Alternativas de autenticación de usuario.
ii. Bloqueo de acceso del dispositivo.
iii. Firewall.
iv. Antivirus.
v. Borrado seguro de contenido.

### 3.7. Responsabilidad de los servidores y usuarios

a) Permanecer siempre cerca del dispositivo
b) Mantener el equipo disponible y en buen estado.
c) No dejar desatendido los equipos.

d) No poner identificaciones del OSINFOR en el dispositivo, salvo los estrictamente necesarios.
e) Toda la información contenida en los aplicativos de OSINFOR y aquella que se haya generado por éstos, que sean propios del desempeño del servidor en el OSINFOR y que se encuentre contenida en los dispositivos móviles son de propiedad única y exclusiva del OSINFOR, la cual es clasificada como Confidencial.
f) Cuando el personal se retire de las instalaciones y no lleve el dispositivo móvil consigo, en caso sea una Laptop o cualquier otro dispositivo móvil se guarda en un lugar seguro con llave; y en ambos casos, la puerta de su oficina permanece cerrada con llave. Adicionalmente, cuando el dispositivo móvil sea una laptop se debe tener en cuenta que:

   i. El bloqueo de pantalla debe estar configurado y activado obligatoriamente.
   ii. Deben bloquearse luego de diez (10) minutos de inactividad.

## Control de cambios

| Versión | Fecha | Justificación[2] | Textos Modificados[3] | Responsable[4] |
|---|---|---|---|---|
| 01 | Elaboración inicial del documento | | | Oficina de Tecnología de la Información |
| | | | | |
| | | | | |

[2] Justificación de la nueva versión del documento, puede darse en los casos de a) Modificación, b) Actualización c) Reestructuración
[3] Señalar los párrafos, secciones literales que se han modificado e incorporado
[4] Señalar el dueño del proceso, indicar el documento o informe sustentatorio

# POLÍTICA DE SEGURIDAD LIGADA A LOS RECURSOS HUMANOS

**DOCUMENTO CONTROLADO**

| | | | |
|---|---|---|---|
| Propuesto por: | Gestión de Tecnologías de la Información | Fecha de propuesta: | 29 AGO. 2018 |
| Aprobado por: | Jefatura del OSINFOR (antes Presidencia Ejecutiva)[1] | Fecha de aprobación: | |

[1] Decreto Legislativo N° 1085 Artículo 51.- "Modificación de los artículos 6 y 7 del OSINFOR"

## Índice

## POLÍTICA DE SEGURIDAD LIGADA A LOS RECURSOS HUMANOS

I. Objetivos ..... 3
II. Alcance ..... 3
III. Política ..... 3
3.1 Responsabilidad ..... 3
3.2. Previo al empleo ..... 3
3.3. Durante el empleo ..... 4
3.4. Finalización o cambio de la relación laboral o empleo ..... 6
Control de cambios ..... 6

# POLÍTICA DE SEGURIDAD LIGADA A LOS RECURSOS HUMANOS

## I. Objetivos

**1.1.** Reducir los riesgos de error humano, comisión de ilícitos, uso inadecuado de instalaciones y recursos, y manejo no autorizado de la información.

**1.2.** Explicitar las responsabilidades en materia de seguridad de la información en la etapa de reclutamiento de personal, incluirlas en los contratos a firmarse y verificar su cumplimiento durante el desempeño de sus funciones como empleado.

**1.3.** Garantizar que los usuarios estén actualizados de las amenazas e incumbencias en materia de seguridad de la información, y se encuentren capacitados para respaldar la Política de Seguridad de la Información del OSINFOR en el transcurso de sus tareas normales.

**1.4.** Establecer Compromisos de Confidencialidad con todo el personal y usuarios externos de las instalaciones de procesamiento de información.

## II. Alcance

El alcance de la presente Política de Seguridad de la Información se aplica al personal que labora designado o contratado, así como a terceros que presten algún servicio al OSINFOR.

## III. Política

La seguridad ligada a los recursos humanos, involucra a toda persona que utiliza la información del OSINFOR para el desempeño de sus actividades, por lo tanto, se establece que:

### 3.1 Responsabilidad

La Oficina de Administración a través de **la Unidad de Recursos Humanos** informará a todos los servidores civiles de sus obligaciones respecto del cumplimiento de la Política de Seguridad de la Información, gestionará los Acuerdos de Confidencialidad y coordinará la capacitación de la presente Política con el Oficial de Seguridad de la Información, así también sobre los tratamientos disciplinarios, resultado de incidentes de seguridad de la información que requieran su intervención, serán tratados por la Secretaria Técnica Procesos Administrativos siguiendo su procedimiento regular.
La Oficina de administración a través de la **Unidad de Abastecimiento** comunicará a los terceros que presten servicios al OSINFOR, respecto del cumplimiento de la Política de Seguridad de la Información, gestionará los Acuerdos de Confidencialidad y coordinará la capacitación de la presente Política con el Oficial de Seguridad de la Información.

La **Oficina de Asesoría Jurídica** asesorará si es requerido sobre el cambio o actualización de las políticas de Seguridad de la Información.

El **Oficial de Seguridad de la Información** es responsable de realizar el cumplimiento de la presente política de seguridad.

### 3.2. Previo al empleo

#### 3.2.1. Selección

a) Se llevan a cabo controles de verificación a los postulantes ganadores de los procesos de selección. Estos controles incluyen todos los aspectos que indiquen las normas y directivas internas que, a tal efecto, alcanzan al OSINFOR.
b) La verificación de la información proporcionada incluye:
   i. Validación de no encontrarse impedido para prestar servicios al Estado en el Registro Nacional de Sanciones de Destitución y Despedido – RNSDD.
   ii. Chequeo del currículum vitae del postulante.
   iii. Confirmación de títulos académicos y profesionales mencionados por el postulante.
   iv. Acreditación de su identidad.
   v. No tener antecedentes policiales, penales y judiciales.
   vi. Verificación de parentesco.
   vii. Ausencia de nepotismo.
   viii. Consulta base de datos sobre los resultados de los antecedentes de supervisión y fiscalización ($SIGO_{sfc}$).

#### 3.2.2. Términos y condiciones de las labores y/o servicio

a) El servidor o contratista, cualquiera sea su vínculo contractual, firmará el Formato Acuerdo de Confidencialidad con los Colaboradores (SGSI-A5-FOR-003), el cual forma parte del contrato, en lo que respecta al tratamiento de la información del OSINFOR. La copia firmada del Acuerdo debe ser custodiada en forma segura por el órgano o unidad orgánica competente.
b) Asimismo, mediante el Acuerdo de Confidencialidad los servidores y/o contratistas declaran conocer y aceptar la existencia de determinadas actividades que pueden ser objeto de control y monitoreo. Dicho acuerdo no debe violar su derecho a la privacidad.
c) Los derechos y obligaciones del servidor o contratista relativos a la seguridad de la información se encontrarán incluidos en los términos y condiciones del contrato, por ejemplo, en relación con las leyes de Propiedad Intelectual o la legislación de protección de datos personales.

### 3.3. Durante el empleo

#### 3.3.1. Responsabilidades de las unidades orgánicas

Los responsables de los órganos o unidades orgánicas deben velar que todos los servidores, así como a terceros que presten algún servicio al OSINFOR cumplan con las políticas de seguridad de la información y los procedimientos establecidos por la organización, verificando que:

a) Estén adecuadamente informados de sus roles y responsabilidades de seguridad de la información antes de que se les otorgue el acceso a los sistemas de información y/o a la información sensible.
b) Cumplan con las Políticas de Seguridad de la Información del OSINFOR.

c) Alcancen un nivel de conciencia sobre la seguridad de la información acorde con sus roles y responsabilidades dentro del OSINFOR.
d) Cumplan con las condiciones y términos del empleo, los cuales incluyen las políticas de seguridad de la información del OSINFOR y métodos adecuados de trabajo.

### 3.3.2. Concientización, educación y formación en seguridad de la información

a) Los servidores y contratistas, de ser el caso, recibirán capacitación y actualización o inducción periódica en materia de políticas, normas y procedimientos del OSINFOR. Esto comprende los requerimientos de seguridad de la información y las responsabilidades legales, así como la capacitación referida al uso correcto de las instalaciones de procesamiento de información y el uso correcto de los recursos en general, el cual estará registrado en el Formato de Planificación de Capacitaciones del SGSI (SGSI-A5-FOR-004.)
b) La Oficina de Administración a través de la **Unidad de Recursos Humanos** coordinara con los servidores; y a través de la **Unidad de Abastecimiento** coordinará con los contratistas que presten algún servicio al OSINFOR, para realizar la inducción correspondiente al personal nuevo y a personal que asuma nuevas responsabilidades, en coordinación con el Oficial de Seguridad de la Información, el cual cuenta con el Formato de Inducción del Personal al SGSI (SGSI-A5-FOR-002.)
c) La oficina de administración a través de la **Unidad de Recursos Humanos** coordinara con los servidores; y a través de la **Unidad de Abastecimiento** coordinará con los contratistas que presten algún servicio al OSINFOR sobre las acciones de capacitación que estén programados en el Formato de Planificación de Capacitaciones del SGSI (SGSI-A5-FOR-004).
d) Cada año se revisará el material correspondiente a la capacitación que realiza el Oficial de Seguridad de la Información, a fin de evaluar su actualización.

### 3.3.3. Proceso disciplinario

En caso de incumplimiento o vulneración de las Políticas, Normas y/o Procedimientos de Seguridad de la Información del OSINFOR se comunicará a la Secretaria Técnica Procesos Administrativos Disciplinarios para su evaluación correspondiente de acuerdo a los lineamientos establecidos en el sistema administrativo de gestión de recursos humanos[1].

### 3.3.4. Sanción Administrativa

[1] Sistema Administrativo laboral para el OSINFOR:

- Ley N° 30057, Ley del Servicio Civil y su reglamento aprobado por DS Nº 040-2014-PCM.
- Decreto Legislativo N° 1057, que regula el régimen especial de contratación administrativa de servicios — CAS, modificado por Ley N° 29849 y su reglamento.
- El Texto Único Ordenado de la Ley 27444 Ley de Procedimiento Administrativo General aprobado con el DS N° 006-2017-JUS, y en las previstas en la Ley N° 27815, Ley del Código de Ética de la Función Pública.

Para el caso de los terceros que presten algún servicio al OSINFOR, serán pasibles de sanciones administrativas de acuerdo al régimen de infracciones y sanciones de la Ley de Contrataciones del Estado[2], quienes presuntamente hayan vulnerado las Políticas, Normas y Procedimientos de Seguridad de la Información del OSINFOR.

### 3.4. Finalización o cambio de la relación laboral o empleo

#### 3.4.1. Finalización o cambio de responsabilidades laborales

a) La **Unidad de Recursos Humanos** informa a los servidores sobre los cambios en su relación laboral o termino.
b) Los derechos de acceso a la información y a las instalaciones de procesamiento deben ser cancelados y/o restringidos al producirse el término del empleo o contrato.
c) La **Unidad de Recursos Humanos** debe solicitar por correo electrónico a la Oficina de Tecnología de la Información; la creación, actualización o desactivación de las cuentas de usuarios, a fin de mantener actualizado los accesos a los sistemas de información y servicios informáticos.
d) El jefe del órgano o unidad responsable del trabajador es quien solicitará el tipo de acceso y/o restricciones a los aplicativos y/o servicios del OSINFOR.
e) Las Políticas de Seguridad de la Información se mantienen vigente a pesar del término del contrato o cambio de puesto el del servidor.

## Control de cambios

| Versión | Fecha | Justificación[3] | Textos Modificados[4] | Responsable[5] |
|---|---|---|---|---|
| 01 | Elaboración inicial del documento | | | Oficina de Tecnología de la Información |
| | | | | |
| | | | | |

[2] Ley N° 30225, Ley de Contrataciones del Estado y su reglamento aprobado mediante D.S. N° 350-2015-EF.

[3] Justificación de la nueva versión del documento, puede darse en los casos de a) Modificación, b) Actualización c) Reestructuración

[4] Señalar los párrafos, secciones literales que se han modificado e incorporado

[5] Señalar el dueño del proceso, indicar el documento o informe sustentatorio

# POLÍTICA DE GESTIÓN DE ACTIVOS

**DOCUMENTO CONTROLADO**

| | | | |
|---|---|---|---|
| Propuesto por: | Gestión de Tecnologías de la Información | Fecha de propuesta: | 29 AGO. 2018 |
| Aprobado por: | Jefatura del OSINFOR (antes Presidencia Ejecutiva)[1] | Fecha de aprobación: | |

[1] Decreto Legislativo N° 1085 Artículo 51.- "Modificación de los artículos 6 y 7 del OSINFOR"

## Índice
## POLÍTICA DE GESTIÓN DE ACTIVOS

I. Objetivos ..... 3
II. Alcance ..... 3
III. Política ..... 3
3.1 Responsabilidad por Activos ..... 3
3.2 Clasificación de Activos de Información ..... 4
3.3 Gestión de Medios ..... 5
Control de cambios ..... 6

# POLÍTICA DE GESTIÓN DE ACTIVOS

## I. Objetivos

1.1. Identificar los activos de información y mantener un inventario de los mismos.
1.2. Proveer un nivel de protección adecuado a los activos de información.
1.3. Identificar y clasificar la información sensible y critica.

## II. Alcance

El alcance de la presente Política de Seguridad de la Información abarca todos los aspectos administrativos y de control que debe ser conocida y cumplida por los directivos, personal que labora designado o contratado, así como por terceros que presten algún servicio al OSINFOR.

## III. Política

### 3.1 Responsabilidad por Activos

#### 3.1.1 Inventario y Propiedad de los Activos de Información

a) Se cuenta con el Formato Matriz de Inventario de Activos (SGSI-A5-FOR-005) donde se identifican los activos importantes, asociados a cada sistema de información, sus propietarios y ubicación. El inventario es realizado por el propietario del activo y actualizado por el dueño del proceso ante cualquier modificación de la información registrada y es revisada con una periodicidad de seis meses.
b) Toda la información y los activos junto a sus medios de procesamiento de información son propiedad de un responsable designado en el OSINFOR, aun cuando por motivos ajenos delegue en otro personal la administración de sus funciones.
c) Los cambios en el inventario de los activos es responsabilidad del propietario del activo de información cuya actualización será coordinada con el **Oficial de Seguridad de la Información.**

#### 3.1.2 Uso Aceptable de los Activos

a) El uso de los activos de información debe ser utilizado para propósitos de las actividades del OSINFOR de acuerdo a las políticas, directivas y procedimientos definidos y considerando criterios de buen uso.
b) La información que haya sido clasificada como "Confidencial" o de "Uso Interno", no puede ser divulgada salvo que haya sido expresamente autorizado por el Propietario de la Información.
c) Cuando se necesite proporcionar información clasificada como "Confidencial" o de "Uso Interno" a terceros, de deberá requerir autorización por escrito al propietario de la información.
d) Para la entrega de la información señalada en el párrafo precedente, se deberá suscribir con el tercero que recibe la información los correspondientes acuerdos de confidencialidad.
e) Todo el personal que labore, designado o contratado que ponga en riesgo los activos de información del OSINFOR, se le aplicará medidas

disciplinarias de acuerdo al Reglamento Interno de Servidores Civiles[1]. Esta sanción se encuentra sujeta a la gravedad del incidente ocasionado y conforme a las normas establecidas.

f) Para el caso de los terceros o colaboradores de terceros que presten algún servicio al OSINFOR, que pongan en riesgo los activos; serán pasibles de sanciones administrativas de acuerdo al régimen de infracciones y sanciones de la Ley de Contrataciones del Estado[2].

### 3.1.3 Devolución de los Activos

a) Todo el servidor que labore en el OSINFOR, designado o contratado debe devolver todos los activos en su poder al término del vínculo laboral su empleo, contrato o en caso de licencia o vacaciones mayores a 30 días.
b) La devolución de activos de Información sigue el procedimiento de entrega de cargo proporcionado por la Unidad de Recursos Humanos al cual debe adjuntar el Formato N° 04 Acta de entrega y recepción de Bienes en uso[3], que es proporcionado por el Especialista de Control Patrimonial de la Unidad de Abastecimiento previa verificación de los activos de información.
c) Si los activos de Información son equipos informáticos deberán seguir el procediendo de borrado seguro.

## 3.2 Clasificación de Activos de Información

### 3.2.1 Clasificación de Activos de Información

a) Toda la información de la Institución debe ser clasificada de acuerdo al procedimiento de Inventario de Activos establecido. Esta clasificación se define en 03 tipos:
   i. **Confidencial:** Activos de información cuyo contenido no debe ser divulgado ni distribuido a personas que no sean autorizadas y cuya difusión genere un impacto importante en la Institución, entre ellas: pérdida económica, sanción legal, pérdida de imagen u otras que alcancen dicho fin.
   ii. **Uso Interno:** Activos de información cuyo contenido sólo debe ser de uso y divulgación para el personal interno de la Institución, las cuales solo podrán ser divulgados a terceras partes previa suscripción del acuerdo de confidencialidad y la autorización debida del propietario de la información, siempre y cuando su divulgación no impacte a la Institución.
   iii. **Público:** Información no sensible de acceso público y que su divulgación no genera impacto en la Institución.
b) El propietario de la información es el encargado de la clasificación de los activos de información que están bajo su responsabilidad.
c) El propietario de la información realiza la actualización en forma anual y/o cuando se estime que un activo de información ha aumentado su

[1] Reglamento N° 001-2016-OSINFOR/05.2 "Reglamento Interno de los Servidores Civiles del OSINFOR" y sus anexos, aprobado con Resolución Presidencial 125-2016-OSINFOR.
[2] Ley N° 30225, Ley de Contrataciones del Estado y su reglamento Aprobado mediante D.L. N° 1017.
[3] Directiva de administración, control y asignación en uso de bienes muebles de propiedad del OSINFOR vigente.

nivel de sensibilidad, en este caso se cambia su nivel de clasificación en forma inmediata, sin esperar el próximo ciclo de actualización. En caso contrario, al considerarse que la información ha disminuido su sensibilidad, podrá opcionalmente esperarse el próximo ciclo de actualización o modificar su clasificación con efecto inmediato. La responsabilidad de la decisión corresponde al propietario de la información.

d) Toda la información que no ha sido específicamente clasificada, es considerada como "Uso Interno", por lo que el propietario de la información debe autorizarla formalmente.

### 3.2.2 Etiquetado de Activos de Información

a) El etiquetado de los Activos de Información se debe realizar para los documentos en papel que considere confidencial conforme a la clasificación de activos definida en el punto 3.2.1 del presente documento, y están identificados a continuación:
   i. Ingreso de documentos confidenciales de la Contraloría General de La República, Presidencia de Consejo de Ministros y del ente rector.
b) Todas las correspondencias deben ser realizados por medios de transporte conocidos y seguros. La correspondencia no etiquetada como información Confidencial será tratada como de uso interno.
c) Los envíos de información que se realicen por correo electrónico, son etiquetados de manera confidencial.
d) La documentación impresa y clasificada confidencial se almacena en lugares que pueda evitar riesgos tales como incendios o inundaciones.
e) Se debe realizar un seguimiento de los documentos originales y copias de información sensible, indicando como mínimo, la clasificación de información, el número de copias, la ubicación de las copias y las personas responsables de las copias.

## 3.3 Gestión de Medios

### 3.3.1 Gestión de medios extraíbles

a) Todo los medios extraíbles y su contenido que no son necesarios para el OSINFOR y no tienen posibilidad de recuperación deben seguir el procedimiento según la normas vigentes[4].
b) Los medios de almacenamiento de información son resguardados en un entorno seguro según las especificaciones del fabricante.
c) Se utilizan técnicas criptográficas para proteger los datos en caso de que la confidencialidad e integridad de la información contenida en el medio sean importantes.

### 3.3.2 Disposición de medios

a) El OSINFOR cuenta con un servicio especializado de custodia para los documentos del OSINFOR.

[4] Item 6.5.9 de la Directiva Nº 001-2015/SBN, aprobada por Resolución Nº 046-2015/SBN

b) Todo medio de almacenamiento de información debe ser resguardado o eliminado según sea el caso de forma segura, respetando la normativa vigente.
c) Se identifican los activos o dispositivos que requieren su baja o eliminación.
d) Los medios eliminados son registrados de acuerdo a la normativa de eliminación de activos vigente y se mantiene el registro con una Resolución de Jefatura para fines de auditoria.

### 3.3.3 Transferencia de medios físicos

a) Los medios que contienen información son protegidos durante su transporte para evitar el acceso no autorizado, pérdida el mal uso o alteración de la información.
b) El OSINFOR cuenta con notificadores, servicios de transporte de carga y servicio de mensajería confiables.
c) Toda información confidencial contenida en un medio y que no esté cifrada cuenta con una protección física adicional.

**Control de cambios**

| Versión | Fecha | Justificación[5] | Textos Modificados[6] | Responsable[7] |
|---|---|---|---|---|
| 01 | Elaboración inicial del documento | | | Oficina de Tecnología de la Información |
| | | | | |
| | | | | |

[5] Justificación de la nueva versión del documento, puede darse en los casos de a) Modificación, b) Actualización c) Reestructuración
[6] Señalar los párrafos, secciones literales que se han modificado e incorporado
[7] Señalar el dueño del proceso, indicar el documento o informe sustentatorio

# POLÍTICA DE CONTROL DE ACCESOS

**DOCUMENTO CONTROLADO**

| | | | |
|---|---|---|---|
| Propuesto por: | Gestión de Tecnologías de la Información | Fecha de propuesta: | 29 AGO. 2018 |
| Aprobado por: | Jefatura del OSINFOR (antes Presidencia Ejecutiva)[1] | Fecha de aprobación: | |

[1] Decreto Legislativo N° 1085 Artículo 51.- "Modificación de los artículos 6 y 7 del OSINFOR"

## Índice
## POLÍTICA DE CONTROL DE ACCESOS

I. Objetivos ..... 3
II. Alcance ..... 3
III. Política ..... 3
3.1 Responsables de acceso a la información ..... 3
3.2 Requerimientos del OSINFOR para el Control de Accesos ..... 3
3.3 Gestión de Acceso del Personal ..... 4
3.4 Responsabilidades del Personal ..... 6
3.5 Control de Acceso al Sistema y a las Aplicaciones ..... 6
Control de cambios ..... 8

# POLÍTICA DE CONTROL DE ACCESOS

## I. Objetivos

**1.1.** Prevenir, evitar y restringir el acceso no autorizado a los sistemas de información, bases de datos y servicio de información.
**1.2.** Implementar la seguridad de la información en los accesos de usuarios por medio de técnicas de autenticación y autorización.
**1.3.** Controlar la seguridad de la información en la conexión entre la red del OSINFOR y otras redes públicas y privadas.
**1.4.** Registrar y monitorear eventos y actividades críticas llevadas a cabo por los usuarios en los sistemas.
**1.5.** Garantizar la seguridad de la información cuando se utiliza computación móvil e instalaciones de trabajo remoto.

## II. Alcance

La política definida en este documento se aplica a todas las formas de acceso de aquellos a quienes se les haya otorgado permisos sobre los sistemas de información, bases de datos o servicios de información del OSINFOR, cualquiera sea la función que desempeñe.

Asimismo, se aplica al personal técnico que define, instala, administra y mantiene los permisos de acceso y las conexiones de red, y a los que administran la Seguridad de la Información.

## III. Política

A continuación, se establecen los lineamientos generales para definir las políticas de acceso a los distintos activos de información del OSINFOR.

### 3.1 Responsables de acceso a la información

Los Responsables de las unidades orgánicas autorizarán el acceso de los usuarios a los servicios, recursos de red y a internet; quien junto con el Oficial de Seguridad de la Información verificarán se adopten todas las medidas que correspondan en materia de seguridad de la información, de modo de cumplir con las normas vigentes.

### 3.2 Requerimientos del OSINFOR para el Control de Accesos

a) Todos los accesos a los activos de información del OSINFOR tanto lógicos como físicos deben basarse en la necesidad y rol del usuario y para ellos toman en cuenta los siguientes aspectos:
   i. Los requerimientos de Seguridad de la Información de cada una de los sistemas de información y servicios de Tecnología de la Información.
   ii. Identificación de toda la información relacionada a las aplicaciones y los riesgos a la que está expuesta.
   iii. Coherencia entre las políticas de control de accesos y las políticas de gestión de activos de información.
   iv. Identificar la legislación aplicable y las obligaciones contractuales con respecto a la protección del acceso a datos y servicios.
   v. Uso de perfiles de usuarios estandarizados definidos según roles.

vi. Administrar los derechos de acceso en un ambiente distribuido y de red, que reconozcan todos los tipos de conexiones y dispositivos disponibles.
vii. Revisión periódica de los controles de acceso.
viii. Revocación de los derechos de acceso.

b) Todo el personal o proveedor que requiera acceder a la red y servicios de red debe contar con las autorizaciones respectivas de los propietarios de los activos.
c) El acceso a los recursos de red, tanto internos como externos, son controlados, de manera que el personal no comprometa la seguridad de los activos de información.
d) Se tienen en cuenta los siguientes aspectos:
   i. Lineamientos de uso de la red.
   ii. Segmentación de redes.
   iii. Control de conexiones a redes.
   iv. Controles de enrutamiento de redes.
   v. Seguridad de la Información en los servicios de red.

### 3.3 Gestión de Acceso del Personal

#### 3.3.1 Registro y baja de usuarios

a) Los responsables de las unidades orgánicas son los encargados de autorizar los accesos correspondientes a los usuarios para el uso de activos de información.
b) Los usuarios contarán con la autorización del propietario de la información para el uso del sistema, base de datos o servicio de información.
c) El personal del OSINFOR, que haga uso de los activos de información ya sea de forma temporal o permanente, contará con una cuenta de usuario que le permita el mínimo acceso autorizado para el normal desarrollo de sus actividades y que permita vincularlo con sus accesos y sean responsables de ellas. Esta cuenta de usuario será gestionada por la Oficina de Tecnología de la Información.
d) En los contratos del personal o de los que prestan algún servicio al OSINFOR se especificarán sanciones si intentan accesos no autorizados.

#### 3.3.2 Gestión de acceso a los usuarios

a) Cuando un usuario nuevo se incorpore al OSINFOR se cuenta con un registro de todos los derechos de acceso otorgados para un sistema o servicio, los cuales estarán registrados en el Formato Control de accesos a aplicaciones y servicios (SGSI-A5-FOR-006).
b) Los derechos de acceso de los usuarios son cancelados inmediatamente cuando cambien sus tareas, o de aquellos a los que se les revocó la autorización, se desvincularon del OSINFOR o sufrieron la pérdida / robo de sus credenciales de acceso.
c) Efectuar revisiones periódicas con el objeto de:
   i. Cancelar identificadores y cuentas de usuario redundantes.
   ii. Inhabilitar cuentas inactivas por más de 30 días.
   iii. Desactivar cuentas inactivas por más de 90 días.

iv. En el caso de existir excepciones, deben ser debidamente justificadas y aprobadas.

### 3.3.3 Gestión de derechos de acceso privilegiados

a) Restringir y controlar la asignación y uso de los derechos de acceso privilegiados.
b) Se identifican los derechos de acceso privilegiados, asociados a cada sistema o proceso, así como los usuarios a los que se les está otorgando.
c) Se asignan privilegios de acceso alineados a la política de control de acceso basados como requisito mínimo para sus roles y funciones.
d) Se cuenta con un registro de todos los privilegios asignados.
e) Se definen requisitos para la expiración de los derechos de acceso privilegiados.
f) Revisar constantemente las cuentas de los usuarios con los accesos privilegiados y si se encuentran alineados a sus funciones.
g) Se evita el uso no autorizado del ID de usuarios de administración genérico.

### 3.3.4 Gestión de la información de autenticación secreta de los usuarios

a) Se verifica la identidad del usuario antes de proporcionarle la información de autenticación secreta nueva, sustitutiva o temporal.
b) La entrega de la autenticación temporal debe hacerse en forma segura y única para cada individuo así mismo debe firmar el Formato Control de accesos a aplicaciones y servicios (SGSI-A5-FOR-006) como constancia o acuse de recibido por parte del usuario.

### 3.3.5 Revisión de los derechos de acceso de usuario

A fin de mantener un control eficaz del acceso a los datos y servicios de información, el Propietario de la Información llevará a cabo un proceso formal, a intervalos regulares de 6 meses, a fin de revisar los derechos de acceso de los usuarios. Se contemplan los siguientes controles:

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

### 3.3.6 Eliminación o ajuste de los derechos de acceso

a) Los derechos de acceso de todo personal o usuarios de proveedores a información e instalaciones de procesamiento de información son eliminados como consecuencia de la desvinculación laboral, contrato o acuerdo.
b) Para el caso de cambio de funciones a los trabajadores se realiza los ajustes de los derechos de acceso, de la siguiente manera primero se retiran los derechos de acceso que se tenía y luego se dan los nuevos

derechos de acceso, previa autorización del responsable del sistema de información.

c) Solo podrá reducirse o eliminarse todos los derechos de acceso a la información y los activos asociados a las instalaciones de procesamiento de información hasta antes de la finalización del vínculo laboral o cambio por causas justificadas.

### 3.4 Responsabilidades del Personal

a) Todo el personal es responsable de la confidencialidad de la contraseña asignada, y de las consecuencias por las acciones que terceras personas puedan hacer con el uso de la misma.
b) El personal cambiará su contraseña regularmente o cada vez que el sistema se lo solicite. Está prohibido compartir las contraseñas asignadas.
c) Para realizar la restauración de contraseñas se sigue un procedimiento formal de comunicación establecido por la Oficina de Tecnología de la Información.
d) El personal bloquea su estación de trabajo si por algún motivo se retira de su puesto de trabajo.
e) Todas las estaciones de trabajo cuentan con un protector de pantalla con clave y activación automática de bloqueo de usuario cuando no se estén utilizando.
f) El personal mantiene sus escritorios libres de documentos y/o medios de almacenamiento removibles cuando no los utilice, procurando guardarlos en gabinetes con llaves.

### 3.5 Control de Acceso al Sistema y a las Aplicaciones

#### 3.5.1 Restricción de acceso a la información

a) El acceso a la información y a las funciones del sistema cuentan con controles de seguridad de la información (por ejemplo, usuario y contraseña), a fin de evitar accesos no autorizados a recursos o información, así mismo, los derechos de acceso ya sea de lectura, escritura, borrar y ejecutar son controlados, también los datos y aplicaciones que son accedidos por el usuario.
b) Dentro de los aspectos que son tomados en consideración para definir los controles, se incluyen:
    i. Identificación automática de estación de trabajo.
    ii. Procedimiento de inicio de sesión seguros.
    iii. Identificación y autenticación de usuarios.
    iv. Sistema de gestión de contraseñas.
    v. Restricción del uso de herramientas utilitarias del sistema operativo con capacidades de eludir y/o sobrescribir los controles de Seguridad de la Información.
    vi. En caso amerite o sea necesario, se deberá limitar el acceso a los recursos de red de las cuentas de usuario, por horarios de trabajo y tiempo de conexión.
    vii. Se cancelan sesiones inactivas luego de un periodo determinado en las aplicaciones críticas y sistemas operativos.

viii. En caso de alguna posible intrusión fallida o exitosa de los controles de inicio de sesión se genera un evento de seguridad de la información.

c) Usuarios del OSINFOR
   i. Se establecen los lineamientos de control de accesos a la información y a las aplicaciones, restringiendo el acceso únicamente para el personal debidamente autorizado.
   ii. Los accesos concedidos se revisan cada seis meses, revocando los derechos del personal cuya vigencia de autorización haya caducado.
   iii. Todas las cuentas de usuarios son gestionadas por la OTI, pero las autorizaciones de cada uno de los accesos de las cuentas son suministradas por el Responsable de la unidad orgánica respectiva.
   iv. Toda la información de estas cuentas de usuarios se centraliza en un repositorio, el cual podrá servir para validar.

d) Usuarios Externos
   i. Los accesos concedidos son revisados cada seis meses, revocando los derechos del personal cuya vigencia de autorización haya caducado.
   ii. Se identifican los sistemas con información sensible asignándoles un entorno de procesamiento, creado a partir de métodos físicos o lógicos (por ejemplo, el uso combinado de cuentas de usuarios, de contraseñas).
   iii. Todos los accesos son brindados mediante una cuenta de usuario y contraseña, adicionalmente se establece una comunicación segura entre el OSINFOR y el punto de acceso del usuario externo, en el caso que se requiera podrá tenerse una línea de conexión exclusiva para transmisión de información.

### 3.5.2 Procedimientos seguros de inicio de sesión.

Todos los usuarios del OSINFOR cuentan con usuario y contraseña, lo que asegura el inicio seguro a los sistemas de información y sistema operativo.

### 3.5.3 Sistema de gestión de contraseñas

a) Los sistemas de gestión de contraseñas son interactivos y garantizan contraseñas de calidad.
b) Todas las contraseñas e identificaciones (IDs) son individuales, permitiendo a los usuarios seleccionar y cambiar sus contraseñas, incluyendo confirmación.
c) Todo el personal cuenta con contraseñas de calidad, cambiar de contraseñas cada 90 días, evitar la reutilización de contraseñas.
d) Se debe almacenar y transmitir las contraseñas en forma protegida.

### 3.5.4 Uso de programas utilitarios privilegiados

a) El uso de programas utilitarios está restringido y se limita el uso solo para usuarios autorizados.
b) Todo programa utilitario pasa por un proceso de identificación, autenticación y autorización de uso, así como su registro, definición y documentación.
c) Todo programa innecesario para el usuario según perfil es desactivado, eliminado.

### 3.5.5 Control de acceso al código fuente del programa

a) El acceso al código fuente de los programas, aplicaciones o sistemas de información del OSINFOR se encuentra restringido y controlado estrictamente.
b) El código fuente de programas, bibliotecas de programas fuente son gestionados por procedimientos establecidos.
c) Las bibliotecas de programas fuente no deben mantenerse en los sistemas en producción.
d) Se cuenta con un registro de bibliotecas fuente de programas sujetos a procedimientos estrictos de control de cambios.
e) Mantener un registro de todos los accesos a bibliotecas fuentes de programas.

## Control de cambios

| Versión | Fecha | Justificación[1] | Textos Modificados[2] | Responsable[3] |
|---|---|---|---|---|
| 01 | Elaboración inicial del documento | | | Oficina de Tecnología de la Información |
| | | | | |
| | | | | |

[1] Justificación de la nueva versión del documento, puede darse en los casos de a) Modificación, b) Actualización c) Reestructuración
[2] Señalar los párrafos, secciones literales que se han modificado e incorporado
[3] Señalar el dueño del proceso, indicar el documento o informe sustentatorio

# POLÍTICA DE CRIPTOGRAFÍA

**DOCUMENTO CONTROLADO**

| | | | |
|---|---|---|---|
| Propuesto por: | Gestión de Tecnologías de la Información | Fecha de propuesta: | 29 AGO. 2018 |
| Aprobado por: | Jefatura del OSINFOR (antes Presidencia Ejecutiva)[1] | Fecha de aprobación: | |

[1] Decreto Legislativo N° 1085 Artículo 51.- "Modificación de los artículos 6 y 7 del OSINFOR"

## Índice
## POLÍTICA DE CRIPTOGRAFÍA

I. **Objetivos** ..... 3

II. **Alcance** ..... 3

III. **Política** ..... 3

**3.1 Política de uso de controles criptográficos** ..... 3

**Control de cambios** ..... 4

# POLÍTICA DE CRIPTOGRAFÍA

## I. Objetivos

Garantizar el uso adecuado y eficaz de la criptografía para proteger la confidencialidad, autenticidad y la integridad de la información.

## II. Alcance

La política de seguridad de criptografía debe ser conocida y cumplida por los directivos, personal que labora designado o contratado, así como por terceros que presten algún servicio al OSINFOR, respecto de las actividades de aseguramiento en el uso y administración de los certificados criptográficos.

## III. Política

### 3.1 Política de uso de controles criptográficos

El OSINFOR establece la presente Política de uso de controles criptográficos, a fin de determinar su correcto uso para la protección de claves de acceso a sistemas, datos y servicios.
El dominio *osinfor.gob.pe* en la actualidad trabaja con certificados digitales, los cuales son utilizados para el acceso a los diferentes sistemas de información. El certificado digital es un mecanismo que permite autenticar un sitio web en internet de manera que la información de la organización y sus administrados se conserve protegida.
Con la finalidad de establecer un control sobre los certificados digitales vigentes se detalla el procedimiento de verificación como sigue:

a) Se solicita la información sobre los certificados actuales y los que se van a implementar.

Si es un certificado nuevo:

b) Se verifica los requerimientos técnicos del certificado digital, como son el tipo de cifrados (1024, 2048 bits), vigencia, etc.
c) Se realiza el pedido y la compra del nuevo certificado a la empresa elegida según las cotizaciones.
d) El especialista en administración de redes de la Oficina de Tecnología de la Información implementa el certificado en el aplicativo y dirección URL respectiva.
e) Valida el funcionamiento del certificado, realizando las pruebas en las páginas respectivas.
f) Se elabora un informe sobre el funcionamiento de la instalación del certificado nuevo y de los que ya están instalados.

Si no es un certificado nuevo:

g) Se verifica la vigencia del certificado de acuerdo con la información solicitada.
h) Si la vigencia es menor de 3 meses se solicita la renovación del certificado.

**Control de cambios**

| Versión | Fecha | Justificación[1] | Textos Modificados[2] | Responsable[3] |
|---|---|---|---|---|
| 01 | Elaboración inicial del documento | | | Oficina de Tecnología de la Información |
| | | | | |
| | | | | |

[1] Justificación de la nueva versión del documento, puede darse en los casos de a) Modificación, b) Actualización c) Reestructuración

[2] Señalar los párrafos, secciones literales que se han modificado e incorporado

[3] Señalar el dueño del proceso, indicar el documento o informe sustentatorio

# POLÍTICA DE SEGURIDAD FÍSICA Y DEL AMBIENTE

**DOCUMENTO CONTROLADO**

| | | | |
|---|---|---|---|
| Propuesto por: | Gestión de Tecnologías de la Información | Fecha de propuesta: | 29 AGO. 2018 |
| Aprobado por: | Jefatura del OSINFOR (antes Presidencia Ejecutiva)[1] | Fecha de aprobación: | |

[1] Decreto Legislativo N° 1085 Artículo 51.- "Modificación de los artículos 6 y 7 del OSINFOR"

## Índice
## POLÍTICA DE SEGURIDAD FÍSICA Y DEL AMBIENTE

I. Objetivos ..... 3
II. Alcance ..... 3
III. Política ..... 3
3.1 Áreas de Seguridad ..... 3
3.2 Equipos ..... 5
Control de cambios ..... 7

# POLÍTICA DE SEGURIDAD FÍSICA Y DEL AMBIENTE

## I. Objetivos

**1.1.** Evitar accesos no autorizados, daños e interferencias contra las instalaciones y la información del OSINFOR

**1.2.** Proteger los equipos de procesamiento de información crítica del OSINFOR ubicándolo en áreas protegidas y resguardadas por un perímetro de seguridad definido según corresponda, con medidas de seguridad de la información y controles de acceso apropiados. Asimismo, contemplar la protección del mismo en su traslado y permanencia fuera de las áreas restringidas, por motivos de mantenimiento u otros.

**1.3.** Evitar pérdidas, daños a los activos de información, así como la interrupción de las actividades del OSINFOR.

## II. Alcance

La política de seguridad física y del ambiente debe ser conocida y cumplida por los directivos, personal que labora designado o contratado, así como por terceros que presten algún servicio al OSINFOR, y se aplica a todos los recursos físicos relativos a los sistemas de información del OSINFOR: instalaciones, equipamiento, cableado, documentos de archivo, medios de almacenamiento, etc.

## III. Política

### 3.1 Áreas de Seguridad

#### 3.1.1 Perímetro de seguridad física

a) El procedimiento de Seguridad y Correcto Uso de las Instalaciones (SGSI-A5-PRO-002) es revisado anualmente, para identificar áreas de mejora y evaluar su alineamiento a los objetivos de la institución.

b) El perímetro de seguridad física encuentra claramente definido. Las especificaciones técnicas dependerán del nivel de protección que se requiera implementar.

c) Se protegen las áreas donde funcionan las instalaciones de procesamiento de información, suministro de energía eléctrica, aire acondicionado y cualquier otra que sea clasificada como crítica y que pudiera afectar el funcionamiento de los sistemas de información.

d) Un área segura puede ser una oficina con llave, o varias oficinas rodeadas por una barrera de seguridad física interna continua. Pueden ser necesarios barreras y perímetros adicionales para controlar el acceso físico entre las áreas con diferentes requerimientos de seguridad, dentro del mismo perímetro de seguridad.

#### 3.1.2 Controles de acceso físico

a) En acceso a la institución cuenta con controles que aseguren el acceso físico sólo al personal debidamente autorizado. En caso de terceros se cuenta con autorización expresa del personal que gestionará las actividades, así como las responsabilidades de estos.

b) El acceso y la permanencia de visitas sólo serán permitidos para propósitos específicos y con autorización respectiva, quedando debidamente registrados.
c) La persona que atiende al visitante será responsable de la permanencia hasta salida del mismo de la institución.
d) De preferencia el administrado será atendido en la sala de atención al ciudadano para cualquier caso.
e) Controlar y limitar el acceso a la información clasificada y a las instalaciones de procesamiento de información, el cual deberá ser exclusivamente a las personas autorizadas. Se utilizarán los siguientes controles de autenticación para autorizar y validar todos los accesos:
   i. Sede Central, Sede Jr. Trujillo y Oficinas Desconcentradas (Pucallpa):
      - Personal de vigilancia.
      - Cámaras de seguridad con DVR
   ii. Centro de Datos (Sede Central):
      - Cámaras de seguridad internas y externas con DVR.
      - Unidad de control de acceso biométrico (huella)
   iii. Gabinete de Contingencia (Sede Jr. Trujillo):
      - Cámara de seguridad interna y externa con DVR.
      - Unidad de control de acceso (Llave).
      - Unidad de control de acceso biométrico (huella)
   iv. Para el caso de las Oficinas Desconcentradas no cuentan con centro de datos.
   v. Archivo Central (Sede Jr. Trujillo):
      - Personal de vigilancia.
      - Puerta con llave.
      - Cámara de seguridad externa.
f) Los registros se mantendrán protegidos por el periodo de 6 meses para permitir auditar todos los accesos, para el Archivo Central.

### 3.1.3 Seguridad en oficinas, despachos e instalaciones

a) Las áreas dedicadas al procesamiento de información se encuentran ubicadas en lugares que no presenten riesgos desde el punto de vista de acceso al público.
b) El personal autorizado (servidores y proveedores) no debe facilitar el acceso a las instalaciones a personas desconocidas.
c) Toda persona visitante deberá ser identificado y cumplir con el protocolo establecido.
d) Los servidores, proveedores y visitantes deben hacer uso en forma visible de la tarjeta de acceso (Fotocheck) para el ingreso y durante la permanencia en las instalaciones.
e) Se mantiene un registro de contratistas autorizados para acceder a las instalaciones.
f) Se mantiene un registro de los visitantes a las instalaciones.
g) Se controlará y se registrará en el cuaderno del personal de seguridad el ingreso de computadoras portátiles, equipos fotográficos, de vídeo, audio o cualquier otro tipo de equipamiento que registre información,

h) Se realiza un monitoreo inopinado al personal de vigilancia sobre las actividades de vigilancia en periodos de 06 meses como máximo.
i) Ubicar el equipamiento de soporte, por ejemplo: impresoras, fotocopiadoras, adecuadamente dentro del área protegida para evitar accesos no autorizados que podrían comprometer la información.
j) Las puertas y ventanas permanecerán cerradas fuera del horario laboral.

#### 3.1.4 Protección contra amenazas externas y del ambiente

a) Los equipos se encuentran ubicados y protegidos de tal forma que se reducen los riesgos como resultado de las amenazas y los peligros del medio ambiente, y las oportunidades de acceso no autorizado.

#### 3.1.5 Trabajo en las áreas seguras

a) Las actividades realizadas en las áreas seguras deben ser supervisadas por el Oficial de Seguridad de la Información por razones de seguridad de la información como también para evitar oportunidades de actividad maliciosa.
b) No se debe brindar información a personas no identificadas.
c) Dar a conocer al personal la existencia del área protegida, o de las actividades que allí se llevan a cabo, sólo si es necesario para el desarrollo de sus funciones.
d) Limitar el acceso al personal del servicio de soporte externo a las áreas protegidas o a las instalaciones de procesamiento de información sensible.
e) Impedir el ingreso de equipos de computación móvil, fotográfico, de video, audio o cualquier otro tipo de equipamiento de pueda registrar o almacenar información, salvo que hayan sido formalmente autorizadas por el Responsable de dicho órgano o unidad orgánica y/o el Jefe de la Oficina de Tecnología de la Información y/o el Oficial de Seguridad de la Información.

#### 3.1.6 Áreas de acceso público, de carga y descarga

a) Limitar el acceso a las áreas de depósito, desde el exterior de la sede del OSINFOR, sólo al personal previamente identificado y autorizado.
b) Inspeccionar el material entrante para descartar peligros potenciales antes de ser trasladados desde el área de depósito hasta el lugar de uso.
c) Registrar y verificar el material entrante al ingresar al área de depósito almacén tomando en consideración lo establecido en la directiva vigente para este caso.

### 3.2 Equipos

#### 3.2.1 Ubicación y protección del equipamiento

a) Los equipos se encuentran ubicados y protegidos de tal forma que se reduzcan los riesgos como resultado de las amenazas y los peligros de causas naturales del ambiente y las oportunidades de acceso no autorizado.

b) El Centro de Datos del OSINFOR, cuenta con un sistema automático/dedicado de protección contra incendios, teniendo un control de fácil acceso.
c) Se cuenta con un sistema de monitoreo automático y/o manual de las condiciones ambientales de temperatura y humedad para que no afecten el normal funcionamiento de los equipos de tratamiento de información. Este sistema debe tener un control de fácil acceso.
d) Ubicar las instalaciones de procesamiento y almacenamiento de información que manejan datos Confidenciales, en un sitio que permita su supervisión constante.

### 3.2.2 Instalaciones de suministro

a) Se cuenta con un sistema de protección eléctrica y fuente de energía tipo UPS (uninterruptible power supply) que brinda soporte al centro de datos, equipos workstations y a los equipos de telefonía fija, en caso que los equipos informáticos que no cuenten con dicha protección eléctrica se asegura el apagado y/o desconexión de los equipos de cómputo, para asegurar la continuidad de las operaciones mientras se restablecen las fallas en el suministro de energía eléctrica.
b) Los servicios de soporte son inspeccionados y probados una vez al año, para asegurar su correcto funcionamiento.

### 3.2.3 Seguridad en el cableado

a) El cableado de energía o de telecomunicaciones se encuentra protegido de cualquier intercepción o daño.
b) El cableado de suministro de energía eléctrica y telecomunicaciones en las zonas de tratamiento de información, cuenta con un sistema de puesta a tierra (pozo a tierra), el que es revisado anualmente para garantizar su adecuado funcionamiento.

### 3.2.4 Mantenimiento de equipos

a) Los mantenimientos de los equipos se realizan de acuerdo con el Procedimiento de Mantenimiento Preventivo y Correctivo de Equipos (SGSI-A5-PRO-003).

### 3.2.5 Retiro de activos de información de propiedad del OSINFOR

a) Para el retiro de materiales como equipos, información o software que son de propiedad del OSINFOR se debe contar con autorización formal, adicionalmente el Especialista en Control Patrimonial registra la salida de bienes a través del Formato N° 03 ACTA DE AUTORIZACION DE SALIDA DE BIENES PATRIMONIALES[1] .
b) El tratamiento de los expedientes en préstamo y los que se encuentran en las direcciones de línea son controlados a través del sistema del módulo de Gestión Documental SIADO.

[1] Directiva de administración, control y asignación en uso de bienes muebles de propiedad del OSINFOR vigente.

### 3.2.6 Seguridad de equipos fuera del local

a) El uso de equipos de la Institución fuera del local es autorizado, y el personal autorizado será responsable de su custodia. Para poder utilizar algún equipo de tratamiento de información fuera del OSINFOR, se deberá contar con la autorización del Jefe Inmediato Superior (quien solicita la salida del equipo) y del Jefe de la unidad de abastecimiento.

### 3.2.7 Equipo desatendido por el usuario

a) Los usuarios deben cerrar sesión de aplicaciones o servicios de red cuando finalicen o no hagan uso de ella, caso contrario luego de diez (10) minutos el equipo pasa a un estado de inactividad.

### 3.2.8 Política de escritorio y pantalla limpios

a) La política de escritorios y pantallas limpias, se encuentra en la Política de pantallas y escritorios limpios (SGSI-A5-POL-008.)

**Control de cambios**

| Versión | Fecha | Justificación[2] | Textos Modificados[3] | Responsable[4] |
|---|---|---|---|---|
| 01 | Elaboración inicial del documento | | | Oficina de Tecnología de la Información |
| | | | | |
| | | | | |

[2] Justificación de la nueva versión del documento, puede darse en los casos de a) Modificación, b) Actualización c) Reestructuración

[3] Señalar los párrafos, secciones literales que se han modificado e incorporado

[4] Señalar el dueño del proceso, indicar el documento o informe sustentatorio

# POLÍTICA DE PANTALLAS Y ESCRITORIOS LIMPIOS

**DOCUMENTO CONTROLADO**

| | | | |
|---|---|---|---|
| Propuesto por: | Gestión de Tecnologías de la Información | Fecha de propuesta: | 29 AGO. 2018 |
| Aprobado por: | Jefatura del OSINFOR (antes Presidencia Ejecutiva)[1] | Fecha de aprobación: | |

[1] Decreto Legislativo N° 1085 Artículo 51.- "Modificación de los artículos 6 y 7 del OSINFOR"

## Índice

## POLÍTICA DE ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

I. Objetivos ..... 3

II. Alcance ..... 3

III. Política ..... 3

3.1. Ubicación de escritorios y equipos ..... 3

3.2. Escritorios Limpios ..... 3

3.3. Pantallas Limpias ..... 3

Control de cambios ..... 4

# POLÍTICA DE ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

## I. Objetivos

Esta política se aplica a la protección de cualquier tipo de información, en cualquiera de sus formas y que pueden estar contenidas en escritorios, estaciones de trabajo, computadores portátiles, medios ópticos, medios magnéticos, documentos en papel y en general cualquier tipo de información que es utilizada por los directivos, todo el personal y terceros.

## II. Alcance

Esta política debe ser conocida y cumplida por los directivos, personal que labora designado o contratado, así como por terceros que presten algún servicio al OSINFOR

## III. Política

### 3.1. Ubicación de escritorios y equipos

a. Los lugares de trabajo de los usuarios se localizan en ubicaciones que no queden expuestas al acceso de personas externas. De esta forma se protege tanto el equipamiento tecnológico como los documentos que pudiera estar utilizando el usuario.
b. Los equipos que queden ubicados cerca de zonas de atención o tránsito de público se ubican de forma que las pantallas no puedan ser visualizados por personas externas.

### 3.2. Escritorios Limpios

a. Toda vez que un usuario se ausenta de su puesto de trabajo, junto con bloquear su estación de trabajo, debe guardar en lugar seguro cualquier documento, medio magnético u óptico removible que contenga información confidencial.
b. Si el usuario está ubicado cerca de zonas de atención de público, al ausentarse de su puesto de trabajo debe guardar también los documentos y medios que contengan información de uso interno.
c. Al finalizar la jornada de trabajo, el usuario debe guardar en un lugar seguro los documentos y medios que contengan información confidencial o de uso interno.
d. La información confidencial, cuando se imprima se debería retirar inmediatamente de las impresoras.

### 3.3. Pantallas Limpias

a. Las estaciones de trabajo y equipos portátiles cuentan con el protector de pantalla, de forma que se active, ante un tiempo sin uso.
b. La pantalla de autenticación a la red del OSINFOR debe requerir solamente la identificación de la cuenta y una clave y no entregar otra información.
c. Toda vez que el usuario se ausente de su lugar de trabajo debe bloquear su estación de trabajo o laptop para así proteger el acceso a las aplicaciones y servicios del OSINFOR.

**Control de cambios**

| Versión | Fecha | Justificación[1] | Textos Modificados[2] | Responsable[3] |
|---|---|---|---|---|
| 01 | Elaboración inicial del documento | | | Oficina de Tecnología de la Información |
| | | | | |
| | | | | |

[1] Justificación de la nueva versión del documento, puede darse en los casos de a) Modificación, b) Actualización c) Reestructuración

[2] Señalar los párrafos, secciones literales que se han modificado e incorporado

[3] Señalar el dueño del proceso, indicar el documento o informe sustentatorio

# POLÍTICA DE SEGURIDAD DE LAS OPERACIONES

**DOCUMENTO CONTROLADO**

| | | | |
|---|---|---|---|
| Propuesto por: | Gestión de Tecnologías de la Información | Fecha de propuesta: | 29 AGO. 2018 |
| Aprobado por: | Jefatura del OSINFOR (antes Presidencia Ejecutiva)[1] | Fecha de aprobación: | |

[1] Decreto Legislativo N° 1085 Artículo 51.- "Modificación de los artículos 6 y 7 del OSINFOR"

## Índice

## POLÍTICA DE SEGURIDAD DE LAS OPERACIONES

I. Objetivos ..... 3
II. Alcance ..... 3
III. Política ..... 3
3.1 Procedimientos y Responsabilidades Operacionales ..... 3
3.2 Protección Ante Software Malicioso ..... 4
3.3 Respaldo ..... 4
3.4 Registros y seguimiento ..... 5
3.5 Control de software en producción ..... 5
3.6 Gestión de vulnerabilidad técnicas ..... 6
3.7 Consideraciones sobre la auditoría de sistemas de información ..... 6
Control de cambios ..... 7

# POLÍTICA DE SEGURIDAD DE LAS OPERACIONES

## I. Objetivos

1.1 Asegurar la operación correcta y segura en las instalaciones de procesamiento de información del OSINFOR.
1.2 Minimizar el riesgo de fallos de los sistemas.
1.3 Proteger la integridad del software y de la información.
1.4 Monitorear las actividades de procesamiento de información para detectar acciones no autorizadas.

## II. Alcance

La política de seguridad de la información abarca todos los aspectos administrativos y de control que debe ser conocida y cumplida por los directivos, personal que labora designado o contratado, así como por terceros que presten algún servicio al OSINFOR.

## III. Política

### 3.1 Procedimientos y Responsabilidades Operacionales

#### 3.1.1 Procedimientos documentados de operación

a) La Oficina de Tecnología de la Información asegura la existencia de documentación formal de sus procedimientos operativos, los cuales se encuentran registrados en el Formato Lista de Procedimientos Operacionales (SGSI-A5-FOR-010).

b) Se prohíbe expresamente:

i. Introducir en los sistemas de información o la red de OSINFOR, contenidos obscenos, amenazadores, inmorales y ofensivos.
ii. Introducir en la red de OSINFOR cualquier tipo de malware, dispositivos lógicos, dispositivos físicos, o cualquier tipo de secuencia de órdenes que causen o sean susceptibles de causar cualquier tipo de alteración o daño en los recursos informáticos.
iii. Intentar distorsionar o falsear los registros "logs" de los Sistemas de Información de OSINFOR.
iv. Poseer, desarrollar o ejecutar programas que pudieran dañar o alterar los recursos informáticos de OSINFOR.

#### 3.1.2 Gestión de Cambios

a) Todo cambio en los procesos, sistemas o instalaciones de procesamiento de la información que afecten a la seguridad de la información son gestionados por el Procedimiento de Gestión de Cambios (SGSI-A5-PRO-004).

#### 3.1.3 Gestión de la Capacidad

La Oficina de tecnología de la Información es responsable de:

a) Identificar los requerimientos de capacidad teniendo en cuenta la criticidad del sistema para los procesos misionales del OSINFOR.
b) Realizar proyecciones de los nuevos requisitos para los procesos misionales del OSINFOR y del sistema para el aprovisionamiento de recursos.
c) Realizar depuraciones de datos obsoletos en disco.
d) Desinstalar aplicaciones, sistemas, bases de datos o entornos obsoletos.
e) Restringir el ancho de banda para servicios de alta demanda de recursos en caso de que no sean críticos para el OSINFOR.

#### 3.1.4 Separación de los ambientes para desarrollo, integración, prueba y producción

a) Los ambientes de Desarrollo, Prueba y Producción cuentan con el nivel de separación necesario para prevenir problemas operacionales, así como los controles de acceso adecuados para cada uno de ellos.

   i. El acceso a los ambientes de Desarrollo, Pruebas y Producción está restringido exclusivamente a personal de desarrollo de sistemas de la Oficina de tecnología de la Información.
   ii. El Especialista en Administración de Redes de la Oficina de Tecnología de la Información es responsable de la administración, mantenimiento, operatividad continua, seguridad y rendimiento aceptable de los ambientes de Desarrollo, Prueba y Producción.
   iii. Las pruebas de los sistemas de información son realizadas utilizando datos de prueba. En los casos en los que no se pueda recrear los datos de prueba y la organización así lo requiera, la copia de datos de producción puede ser usada para las pruebas siempre y cuando el uso de esta información sea autorizado y analizado por el propietario del activo de información relacionado y previamente tratada para el resguardo de los datos.

### 3.2 Protección Ante Software Malicioso

#### 3.2.1 Controles ante software malicioso

a) El software utilizado por el OSINFOR debe ser autorizado en forma expresa por la Oficina de Tecnología de la Información.
b) Para reducir la presencia de códigos maliciosos (virus, gusanos, troyanos, spyware, entre otros) en los sistemas de información y los medios de procesamiento, el sistema de antivirus se encuentra habilitado en los equipos del OSINFOR, así como en los equipos de personal de terceros o visitas que requieran ingresar a la red del OSINFOR.
c) El especialista en Administración de Redes es responsable de instalar, configurar, monitorear y controlar el sistema de antivirus a nivel de servidores y equipos.
d) El sistema de antivirus es actualizado periódicamente y configurado para realizar revisiones programadas para la detección de virus en los equipos del OSINFOR.

### 3.3 Respaldo

#### 3.3.1 Respaldo de la información

a) El proceso de respaldo de la información es realizado por el especialista en Administración de Redes.
b) El respaldo y recuperación de la información se realiza de acuerdo al Procedimiento de Respaldo de Información(SGSI-A5-PRO-005).

### 3.4 Registros y seguimiento

#### 3.4.1 Registro de eventos

a) Todo evento de logeo es registrado y monitoreado por el MOM (Gestión de Operativa de monitoreo).
b) Se debe registrar también el uso de privilegios, uso de utilidades y aplicaciones del sistema, archivos accedidos y tipo de acceso; direcciones y protocolos de red; alarmas configuradas por el sistema de control de acceso; activación y desactivación de los sistemas de protección, tales como sistemas de antivirus y sistemas de detección de intrusos.

#### 3.4.2 Protección de la información de registros (Logs)

La protección a los medios de registro y la información de registros contra su alteración y acceso no autorizado, así como de la edición o eliminación de archivos de registros (Log), no está permitido ingresar a los eventos de logeo. Para ello existen configuraciones especiales en los sistemas.

#### 3.4.3 Registros del administrador y operador

Todas las actividades del administrador y operador son registradas y esos registros son protegidos, así mismo se revisan regularmente para mantener la responsabilidad de los usuarios privilegiados. Esta información queda almacenada en el Log de Auditoría del sistema.

#### 3.4.4 Sincronización de relojes

Todos los equipos de la red conectados al dominio del OSINFOR se conectan al servidor NTP para su sincronización de actualización de los relojes.
Toda alteración de los relojes se registra en el servidor NTP y reportado para la identificación de causa raíz.

### 3.5 Control de software en producción

#### 3.5.1 Instalación de software en los sistemas operativos

Se revisa periódicamente el software instalado y las licencias que se han adquirido para asegurar que solo el Software permitido sea utilizado en el OSINFOR.
Se mantiene un registro del software permitido en el Formato Lista de Software Permitido (SGSI-A5-FOR-012).

a) Se está familiarizado con la Ley de derechos de autor, a fin de comprender las consecuencias de su incumplimiento, incluyendo las sanciones y responsabilidades por daños y perjuicios.
b) Se mantiene actualizado el Formato Lista de Software Permitido (SGSI-A5-FOR-012), para guiar la compra de nuevo software y definir aquel que debe ser mantenido en las Computadoras y servidores.
c) El software no permitido o sin licencias serán desinstalados. Así también se desinstalarán el software que ya no se usa en las Computadoras.
d) Exigir que el software que se adquiera se realice a través de un proceso de compra formal para asegurar que se obtengan las aprobaciones adecuadas, y que los registros de compra, recepción, e inventario son creados y mantenidos.
e) Para el software desarrollado por la entidad y/o adquiridos por donación o por convenios, se solicita o genera según sea el caso la documentación necesaria para asegurar el control de los mismos.

## 3.6 Gestión de vulnerabilidad técnicas

### 3.6.1 Gestión de vulnerabilidades técnicas

a) Se realiza una vez al año con un proveedor externo un análisis de vulnerabilidades técnicas de los sistemas de información en uso y de la infraestructura tecnológica.

### 3.6.2 Restricciones en la instalación de software por los usuarios

a) Se restringe la instalación de software solo al personal autorizado de la Oficina de Tecnología de la Información. El personal encargado de instalar Software en las Computadoras es el responsable de soporte técnico.
b) Se asegura que el software que se va a instalar se encuentre registrado en el Formato Lista de Software Permitido (SGSI-A5-FOR-012).

## 3.7 Consideraciones sobre la auditoria de sistemas de información

### 3.7.1 Controles de auditoría de sistemas de información

a) Se planifica y acuerda los requisitos y las actividades de auditoria que implican la verificación de los sistemas operativos para minimizar las interrupciones en los procesos misionales del OSINFOR.
b) Se controla el alcance de las verificaciones, éstas son limitadas a accesos de sólo lectura al software y a los datos; en caso de que las verificaciones afecten la disponibilidad del sistema se realizan fuera de horario de oficina.

**Glosario de Términos**

- **Logeo:** En materia de accesos a sistemas de informáticos, "hacer login", "loguearse" o "identificarse" es la acción de introducir nuestras claves de usuario (nombre de usuario y contraseña) en una página web para acceder a una aplicación servicios o modulo informático.

- **Registros (Logs):** Un log ("registro", en español) es un archivo de texto en el que constan cronológicamente los acontecimientos que han ido afectando a un sistema informático (programa, aplicación, servidor, etc.), así como el conjunto de cambios que estos han generado.

## Control de cambios

| Versión | Fecha | Justificación[1] | Textos Modificados[2] | Responsable[3] |
|---|---|---|---|---|
| 01 | Elaboración inicial del documento | | | Oficina de Tecnología de la Información |
| | | | | |
| | | | | |

[1] Justificación de la nueva versión del documento, puede darse en los casos de a) Modificación, b) Actualización c) Reestructuración

[2] Señalar los párrafos, secciones literales que se han modificado e incorporado

[3] Señalar el dueño del proceso, indicar el documento o informe sustentatorio

# POLÍTICA DE SEGURIDAD DE LAS COMUNICACIONES

**DOCUMENTO CONTROLADO**

| | | | |
|---|---|---|---|
| Propuesto por: | Gestión de Tecnologías de la Información | Fecha de propuesta: | 29 AGO. 2018 |
| Aprobado por: | Jefatura del OSINFOR (antes Presidencia Ejecutiva)[1] | Fecha de aprobación: | |

[1] Decreto Legislativo N° 1085 Artículo 51.- "Modificación de los artículos 6 y 7 del OSINFOR"

## Índice

## POLÍTICA DE SEGURIDAD DE LAS COMUNICACIONES

I. Objetivos ..... 3
II. Alcance ..... 3
III. Política ..... 3
3.1 Gestión de la seguridad de red ..... 3
3.2 Transferencia de información ..... 4
Control de cambios ..... 6

# POLÍTICA DE SEGURIDAD DE LAS COMUNICACIONES

## I. Objetivos

**1.1.** Implementar y mantener un nivel apropiado de seguridad y de entrega de servicio en línea con los acuerdos con terceros.

**1.2.** Proteger la información de las redes y la protección de la infraestructura que la soporta.

## II. Alcance

El alcance de todas las políticas de seguridad de la información abarca todos los aspectos administrativos y de control que debe ser conocida y cumplida por los directivos, personal que labora designado o contratado, así como por terceros que presten algún servicio al OSINFOR.

## III. Política

### 3.1 Gestión de la seguridad de red

#### 3.1.1 Controles de red

a) El Procedimiento de Seguridad en las Comunicaciones (SGSI-A5-PRO-006) es evaluado por lo menos una vez por año, para identificar áreas de mejora y evaluar su alineamiento a los objetivos de los procesos misionales.

b) El Procedimiento de Seguridad en las Comunicaciones (SGSI-A5-PRO-006) permite gestionar y controlar los servicios de comunicación de los sistemas de la organización.

c) Los incidentes de seguridad detectados en los ambientes gestionados son filtrados y notificados según el Procedimiento de Gestión de Incidentes de Seguridad de la Información (SGSI-A5-PRO-008), para las acciones respectivas.

d) Controles en las redes:

   i. El Especialista en Administración de Redes es el responsable de gestionar, controlar las redes de computación, garantizar la seguridad de la información en la red del OSINFOR y proteger los servicios conectados a la red desde accesos remotos.

   ii. El Especialista en Administración de Redes administra los equipos de seguridad perimetral (Firewall, entre otros), los accesos a la red pública de los equipos, la comunicación entre equipos de diferentes redes (habilitar el acceso a nivel de Firewall) y los perfiles de internet a través de conexiones remotas vía HTTP/HTTPS, RDP o SSH hacia las consolas de administración.

   iii. El Especialista en Administración de Redes administra y monitorea los equipos de comunicaciones de la red interna y externa a través del software PRTG Network Monitor. Es responsable de la configuración de la red cableada e inalámbrica. Asimismo, garantiza la disponibilidad de la comunicación entre la

sede central y el local de contingencia a través del software RADWIN Manager.

#### 3.1.2 Seguridad de los servicios de red

a) La seguridad en los servicios de las redes es administrada y gestionada por el Especialista en Administración de Redes, a través de los requerimientos, análisis y/o monitoreo que se realiza en el Firewall.
b) Los equipos de comunicaciones deben de cumplir los requisitos mínimos de seguridad establecidos.

#### 3.1.3 Segregación en redes

a) La red del OSINFOR esta segmentada, la red interna se conforma de dos segmentos de voz y datos, las cuales a su vez están protegidas por un Firewall/UTM, un servidor antispam y un servidor de filtro web, que permite los accesos entre ellos y hacia Internet.

### 3.2 Transferencia de información

#### 3.2.1 Políticas y procedimientos de transferencia de información

a) Se mantiene la seguridad en el intercambio de información del OSINFOR con cualquier otra entidad externa, ya sean estas entidades reguladoras y otras. Los intercambios de información se realizan utilizando el protocolo SFTP. Asimismo, cualquier entidad externa que quiera conectarse al SFTP utilizando la conexión de Internet, cuenta con un acuerdo de confidencialidad firmado, y en caso de no existir, se le debe de hacer firmar uno.

#### 3.2.2 Acuerdos de transferencia de información

a) Se cuenta con acuerdos de transferencia segura de información entre el OSINFOR y las entidades externas.
b) Ambas organizaciones tienen que contar con accesos y credenciales al servidor SFTP del cual compartirán información.
c) La entidad externa que desea conectarse al servidor SFTP del OSINFOR, tiene que proveer al Especialista en Administración de Redes la dirección IP pública que utiliza, para que esta sea permitida a través del Firewall.
d) Ambas organizaciones se rigen bajo los acuerdos de confidencialidad y no divulgación de la información.

#### 3.2.3 Mensajería electrónica

a) El servicio de correo electrónico que se brinda al personal es de propiedad exclusiva del OSINFOR. El correo electrónico y su contraseña respectiva son confidenciales, personales e intransferibles.

b) OSINFOR se reserva el derecho de activar las opciones de auditoria sobre los mensajes enviados o recibidos para verificar el cumplimiento de las políticas establecidas para el uso del correo electrónico.
c) El personal del OSINFOR es el responsable de asegurar que ninguna persona ajena utilice su correo electrónico violando las políticas de seguridad, que no se realice actividades ilegales y que no utilice el acceso para fines ajenos a los de la institución. Los colaboradores se hacen responsables por todas las actividades realizadas con su cuenta.
d) El oficial de Seguridad de la Información como parte de la gestión de incidentes de seguridad es responsable de realizar las investigaciones y tomar las acciones que correspondan en coordinación con el responsable de la unidad orgánica del personal involucrado y si amerita, solicitar la revocación del privilegio si se detecta un mal uso del correo electrónico.

### 3.2.4 Acuerdos de confidencialidad o no-divulgación

a) Mantener la información confidencial.
b) No divulgar o copiar la información confidencial.
c) El valor que la información confidencial representa para el OSINFOR es un valor incuantificable, lo que debe ser considerado por los empleados a fin de determinar la cuantía de daños y perjuicios.
d) Las obligaciones de confidencialidad inician una vez firmado el acuerdo, sobreviviendo después del cese de labores y extendiéndose de manera permanente.
e) Estos acuerdos de confidencialidad deben aplicarse tanto para proveedores como para personal del OSINFOR.

**Glosario de Términos**

- **Firewall:** Programa o equipo informático que controla el acceso de una computadora a la red y de elementos de la red a la computadora, por motivos de seguridad.
- **Seguridad Perimetral:** La seguridad perimetral es un concepto emergente asume la integración de elementos y sistemas, tanto electrónicos como mecánicos, para la protección de perímetros físicos, detección de tentativas de intrusión y/o disuasión de intrusos en instalaciones especialmente sensibles.
- **Servidor Anti spam**: Permite prevenir el correo basura. Tanto los usuarios finales como los administradores de sistemas de correo electrónico.
- **Protocolo SFTP**: Es uno de los diversos protocolos de la red Internet, concretamente significa Secure File Transfer Protocol (Protocolo de Transferencia segura de Archivos) y es el ideal para transferir grandes bloques de datos por la red en modo seguro.

## Control de cambios

| Versión | Fecha | Justificación[1] | Textos Modificados[2] | Responsable[3] |
|---|---|---|---|---|
| 01 | Elaboración inicial del documento | | | Oficina de Tecnología de la Información |
| | | | | |
| | | | | |

[1] Justificación de la nueva versión del documento, puede darse en los casos de a) Modificación, b) Actualización c) Reestructuración

[2] Señalar los párrafos, secciones literales que se han modificado e incorporado

[3] Señalar el dueño del proceso, indicar el documento o informe sustentatorio

# POLÍTICA DE ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN

**DOCUMENTO CONTROLADO**

| | | | |
|---|---|---|---|
| Propuesto por: | Gestión de Tecnologías de la Información | Fecha de propuesta: | 29 AGO. 2018 |
| Aprobado por: | Jefatura del OSINFOR (antes Presidencia Ejecutiva)[1] | Fecha de aprobación: | |

(1) Decreto Legislativo N° 1085 Artículo 51.- "Modificación de los artículos 6 y 7 del OSINFOR"

## Índice

## POLÍTICA DE ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN

I. **Objetivo** ..... 3
II. **Alcance** ..... 3
III. **Política** ..... 3
3.1 **Requisitos de Seguridad de los Sistemas de Información** ..... 3
3.2 **Seguridad en los Procesos de Desarrollo y Soporte** ..... 4
3.3 **Datos de Prueba** ..... 5
**Control de cambios** ..... 6

# POLÍTICA DE ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN

## I. Objetivo

Garantizar que la seguridad de la información sea parte integral de los sistemas de información en todo el ciclo de vida. Incluyendo los requisitos para los sistemas de información que proporcionan los servicios a través de redes públicas.

## II. Alcance

Es de aplicación a todo el personal que labora directivos, personal que labora designado o contratado, así como por terceros que presten algún servicio al OSINFOR, a través de la Oficina de Tecnología de la Información que participa en la adquisición, desarrollo o mantenimiento de los Sistemas de Información.

## III. Política

### 3.1 Requisitos de Seguridad de los Sistemas de Información

#### 3.1.1 Análisis y Especificación de los Requisitos de Seguridad de la Información

a) Para todos los sistemas desarrollados por o para OSINFOR, se determinan (si aplican) los requerimientos de seguridad de información antes de comenzar la fase de desarrollo de la aplicación, con el fin de evitar o minimizar fallas de seguridad en los sistemas de información a desarrollar. El responsable de desarrollo es quien valida si se cumplen con los requerimientos de seguridad establecidos.

b) Para todos los sistemas desarrollados por o para el OSINFOR, los requerimientos mínimos de seguridad se tienen en el documento Formato Requerimiento (OTI_FREQ.). Estos requerimientos deben ser incorporados en cada fase del ciclo de desarrollo como son: Análisis de Requerimientos, Diseño, Desarrollo, Pruebas e implantación. Así mismo, en el caso que ameriten, se debe de considerar adicionar otros requerimientos sobre seguridad de la información.

#### 3.1.2 Aseguramiento de los Servicios de Aplicación en las Redes Públicas

a) Se utilizan certificados SSL para asegurar los inicios de sesión de los usuarios a los sistemas de información y a las consultas de entidades externas al OSINFOR. Así mismo, se utilizan firmas digitales de RENIEC, el cual permite firmar documentos XML con los estándares que la RENIEC exige.

#### 3.1.3 Protección de las Transacciones de los Servicios de Aplicación

a) Se utilizan certificados SSL para asegurar los inicios de sesión de los usuarios a los sistemas de información y a las consultas de entidades externas al OSINFOR. Así mismo, se utilizan firmas digitales de RENIEC el

cual permite firmar documentos XML con los estándares que la RENIEC exige.

## 3.2 Seguridad en los Procesos de Desarrollo y Soporte

### 3.2.1 Política de Desarrollo Seguro

a) Se cuenta con una política de desarrollo seguro Política de Ingeniería de Software (SGSI-A5-POL-012).

### 3.2.2 Procedimiento de Control de Cambio del Sistema

a) Se ha determinado que se realiza el versionamiento en el ambiente de integración antes de pasar los cambios al ambiente de pruebas. Esta actividad permite gestionar y controlar los cambios realizados que finalmente modifican el ambiente productivo siendo un requerimiento fundamental para realizar dichas modificaciones.
b) Se realizan las revisiones de la funcionalidad con respecto a seguridad de la información en la fase de pruebas.

### 3.2.3 Revisión Técnica de Aplicaciones después de Cambios en la Plataforma Operativa

a) Se verifica y garantiza que los cambios realizados no tengan un impacto adverso en las actividades y operaciones críticas del negocio.
b) Se realizan pruebas con la finalidad de evidenciar posibles inconvenientes, con la finalidad de evidenciar el cumplimiento de los requisitos de seguridad de la información solicitados y determinar si estos cumplen con los criterios de aceptación definidos en la etapa de análisis.

### 3.2.4 Restricciones en Cambios a Paquetes de Software

a) Las modificaciones a paquetes de software son limitados solo a cambios necesarios y todos los cambios son estrictamente controlados.
b) Se considera el impacto ocasionado, si el OSINFOR se hace responsable por el futuro mantenimiento del software como consecuencia de los cambios y la compatibilidad con otro software en uso.

### 3.2.5 Principios de la Ingeniería de Sistemas Seguros

a) Se han establecido los principios de ingeniería de sistemas seguros, los cuales se encuentran en la Política de Ingeniería de Software (SGSI-A5-POL-012).

### 3.2.6 Entorno de Desarrollo Seguro

a) Se cuenta con un ambiente seguro de Desarrollo; donde solo las personas autorizadas podrán tener acceso a dicho ambiente, de acuerdo con las funciones o actividades asignadas.

### 3.2.7 Desarrollo Subcontratado

a) El OSINFOR supervisa y realiza el seguimiento de las actividades de desarrollo de sistemas subcontratados, considerando:
   i. El acuerdo de licencias, la propiedad del código y los derechos de propiedad intelectual relacionado con el contenido de terceros.
   ii. Los requisitos contractuales para el diseño, la codificación y las pruebas seguras.
   iii. Las pruebas de aceptación para la calidad y precisión de los entregables.
   iv. La presentación de pruebas de que se probaron los requisitos de seguridad para establecer los niveles mínimos aceptables de seguridad y calidad.

#### 3.2.8 Pruebas de Seguridad de Sistemas y Pruebas de Aceptación de Sistemas

a) La Oficina de Tecnología de la Información a través de los responsables de los Sistemas de Información es responsable del desarrollo de pruebas para validar el cumplimiento de los requerimientos establecidos por la necesidad del usuario. Si el resultado de estas pruebas es satisfactorio, la Oficina de Tecnología de la Información se realiza pruebas en conjunto con el usuario. Con la confirmación de dichas pruebas el usuario brinda la aprobación correspondiente a través del Formato de Acta de Pase a Producción (SGSI-A5-FOR-034) para que el cambio realizado al sistema de información pase al ambiente de Producción.
b) El analista programador revisa el cumplimiento de los requisitos mínimos de seguridad establecidos en el Formato Requerimiento (OTI_FREQ.).

### 3.3 Datos de Prueba

#### 3.3.1 Protección de los Datos de Prueba

a) Se cuenta con el Formato de Solicitud de Autorización de Datos de Prueba (SGSI-A5-FOR-035) para el caso en que se requiera migrar datos del ambiente de producción hacia el ambiente de desarrollo o pruebas, con la finalidad de utilizarlos en las diversas etapas de los proyectos de los Sistemas de Información. Esta actividad se realiza a demanda y para ello el responsable del proyecto deberá solicitar autorización al Oficial de Seguridad de la Información, registrando en un documento la solicitud que deberá contener como mínimo el nombre y cargo del solicitante, fecha, nombre del sistema, descripción de información requerida y motivo, autorizaciones correspondientes para la extracción de la información especificada.

### Glosario de Términos

- **Versionamiento:** El verbo versionar en informática indica el significado de 'hacer una versión nueva de un software informático".

**Control de cambios**

| Versión | Fecha | Justificación[1] | Textos Modificados[2] | Responsable[3] |
|---|---|---|---|---|
| 01 | Elaboración inicial del documento | | | Oficina de Tecnología de la Información |
| | | | | |
| | | | | |

[1] Justificación de la nueva versión del documento, puede darse en los casos de a) Modificación, b) Actualización c) Reestructuración

[2] Señalar los párrafos, secciones literales que se han modificado e incorporado

[3] Señalar el dueño del proceso, indicar el documento o informe sustentatorio

# POLÍTICA DE INGENIERÍA DE SOFTWARE

**DOCUMENTO CONTROLADO**

| | | | |
|---|---|---|---|
| Propuesto por: | Gestión de Tecnologías de la Información | Fecha de propuesta: | 29 AGO. 2018 |
| Aprobado por: | Jefatura del OSINFOR (antes Presidencia Ejecutiva)[1] | Fecha de aprobación: | |

[1] Decreto Legislativo N° 1085 Artículo 51.- "Modificación de los artículos 6 y 7 del OSINFOR"

## Índice

## POLÍTICA DE INGENIERÍA DE SOFTWARE

I. Objetivo ..... 3

II. Alcance ..... 3

III. Política ..... 3

Control de cambios ..... 4

# POLÍTICA DE INGENIERÍA DE SOFTWARE

## I. Objetivo

Garantizar que los desarrollos de las aplicaciones en el OSINFOR cuenten con lineamientos de ingeniería de software para el desarrollo seguro.

## II. Alcance

El alcance de esta política de seguridad de la información abarca todos los aspectos administrativos y de control que debe ser conocida y cumplida por los directivos, personal que labora designado o contratado, así como por terceros que presten algún servicio al OSINFOR.

## III. Política

Es política del OSINFOR ejecutar los proyectos de desarrollo en base a un proceso de ingeniería definido que considere los siguientes lineamientos:

3.1 Recolectar las necesidades, expectativas, restricciones de los usuarios para desarrollar sus requerimientos y priorizarlos; establecer y asignar los requerimientos del producto, identificando las interfaces tempranamente; los requerimientos se deben analizar y validar para asegurar que son necesarios y suficientes; balanceando restricciones frente a necesidades; y asegurando que el producto funcionará en el ambiente final de los usuarios.

3.2 La solución técnica elegida es el resultado de un análisis de alternativas contra criterios establecidos, que siguió un proceso formal para su selección. El diseño del producto incluye el diseño de las interfaces, así como un análisis de lo que debe desarrollarse, comprarse o re usarse. La implementación del diseño incluye la documentación de uso final que brinde soporte al mismo.

3.3 Se verifica el producto con la finalidad de asegurar que satisface los requerimientos especificados, para lo cual se seleccionan los productos a verificar, establecer el ambiente donde el producto será verificado y realizar la verificación respectiva, siguiendo los procedimientos y criterios establecidos, los resultados de la verificación deben ser analizados.

3.4 Se valida el producto con la finalidad de demostrar su correcto funcionamiento en el ambiente final, para el cual ha sido planeado. Involucra la selección de productos a validar, establecer el ambiente de validación y realizar la validación siguiendo procedimientos y criterios establecidos. Los resultados de la validación son analizados. La validación del producto se realiza por el usuario o sus representantes formalmente autorizados.

## Control de cambios

| Versión | Fecha | ustificación[1] | xtos Modificados[2] | Responsable[3] |
|---|---|---|---|---|
| 01 | Elaboración inicial del documento | | | Oficina de Tecnología de la Información |
| | | | | |
| | | | | |

[1] Justificación de la nueva versión del documento, puede darse en los casos de a) Modificación, b) Actualización c) Reestructuración

[2] Señalar los párrafos, secciones literales que se han modificado e incorporado

[3] Señalar el dueño del proceso, indicar el documento o informe sustentatorio

# POLÍTICA DE RELACIÓN CON PROVEEDORES

**DOCUMENTO CONTROLADO**

| | | | |
|---|---|---|---|
| Propuesto por: | Gestión de Tecnologías de la Información | Fecha de propuesta: | 29 AGO. 2018 |
| Aprobado por: | Jefatura del OSINFOR (antes Presidencia Ejecutiva)[1] | Fecha de aprobación: | |

[1] Decreto Legislativo N° 1085 Artículo 51.- "Modificación de los artículos 6 y 7 del OSINFOR"

## Índice
## POLÍTICA DE RELACIÓN CON PROVEEDORES

I. Objetivos ..... 3
II. Alcance ..... 3
III. Política ..... 3
3.1 Políticas Generales ..... 3
3.2 Políticas Específicas ..... 4
Control de cambios ..... 8

# POLÍTICA DE RELACIÓN CON PROVEEDORES

## I. Objetivos

**1.1** Implementar y mantener un nivel apropiado de seguridad de la información y de entrega de los servicios acordados con terceros que presten algún servicio al OSINFOR.

**1.2** Garantizar la protección de los activos de información que son accesibles por los terceros que presten algún servicio al OSINFOR.

## II. Alcance

El alcance de todas las Políticas de Seguridad de la Información de proveedores abarca todos los aspectos administrativos y de control que accedan y/o generen información y debe ser conocida y cumplida por los directivos, personal que labora designado o contratado, así como por terceros que presten algún servicio al OSINFOR.

## III. Política

### 3.1 Políticas Generales

1. Todo proveedor y/o contratista que brinde servicios al OSINFOR, deberán cumplir con la Política de Seguridad de la Información para proveedores, cuyo requisito debe formar parte de los términos de referencia a clausula será parte del contrato de prestación de servicios como anexo.
2. El proveedor y/o contratista proporcionará los datos completos de la persona de contacto, quien será el encargado de recibir todo tipo de directivas del sistema de seguridad de la información. El proveedor y/o contratista proporcionará al inicio la relación de personas, perfiles, funciones y responsabilidades asociadas al servicio provisto, e informará puntualmente de cualquier cambio (alta, baja, sustitución o cambio de funciones o responsabilidades) que se produzca en dicha relación.
3. Todo proveedor y/o contratista de servicios deberá velar que su personal, cumpla con las Políticas de Seguridad de la Información recogidas en el presente documento. En caso de incumplimiento, El OSINFOR se reserva el derecho de solicitar al proveedor y/o contratista el cambio de personal, sin perjuicio de ello, el OSINFOR podrá resolver el contrato de prestación de servicios según corresponda e iniciar las acciones legales pertinentes.
4. El proveedor y/o contratista deberá garantizar que todo su personal que brinde servicios al OSINFOR, cuente con formación y capacitación apropiada para el desarrollo del servicio contratado, y de manera transversal deberá tener conocimiento de las políticas de seguridad de la información del OSINFOR.
5. Cualquier tipo de intercambio de información que se produzca entre el OSINFOR y el Proveedor y/o contratista se entenderá que ha sido realizado dentro del marco establecido por el contrato de prestación de servicios, de modo que dicha información tendrá el carácter de confidencial y no podrá ser utilizada en ningún caso fuera de dicho marco, ni para fines diferentes a los asociados al contrato.
6. La Oficina de Tecnología de la Información centraliza los esfuerzos globales de gestión de accesos y protección de activos de Información del OSINFOR, a fin de asegurar el correcto funcionamiento de las tecnologías de la información que soportan los procesos de la organización.

7. Para el caso de los contratistas y sus colaboradores se deberá realizar una inducción sobre las políticas de seguridad de la información del OSINFOR, según corresponda.

### 3.2 Políticas Específicas

1. Todo Proveedor y/o contratista que tenga acceso a la información de OSINFOR en ejecución de la contratación, deberá considerar que dicha información, es confidencial.
2. Ningún Proveedor y/o contratista podrá utilizar la información de OSINFOR para beneficio propio o de terceros. La información a la que tenga acceso el Proveedor únicamente podrá ser utilizada para los fines específicamente indicados en la contratación. Toda información proporcionada por el OSINFOR, seguirá siendo de propiedad de esta última.
3. El Proveedor y/o contratista garantiza que al término del servicio o ante el pedido efectuado en cualquier momento por OSINFOR, cesará inmediatamente el uso de toda información proporcionada, debiendo entregar (cualquiera sea el soporte en que se encuentre) toda la información que obre en su poder y destruir toda copia que se haya realizado, entregando una confirmación por escrito de ello, en calidad de declaración jurada.
4. Todas las obligaciones de confidencialidad continuarán vigentes aun cuando la contratación haya culminado por cualquier causa.
5. El Proveedor y/o contratista solo podrá crear y/o almacenar información del OSINFOR de forma temporal, siempre que sea estrictamente necesario para el desarrollo del servicio. Esta información temporal no deberá quedar almacenada en ninguna computadora, ni unidad de memoria externa del contratista, la misma que será destruida cuando haya dejado de ser útil para la finalidad para la que se creó y/o almacenó.
6. La salida de medios informáticos que contengan información confidencial o datos de carácter personal, fuera de los locales en los que está ubicada la información, únicamente podrá ser autorizada por el responsable del equipo informático y la Oficina de Tecnología de la Información del OSINFOR.
7. Cuando el Proveedor conozca de cualquier pérdida, uso no autorizado o revelación de la Información proporcionada o de propiedad de OSINFOR, deberá comunicar inmediatamente por escrito y adoptar todos los pasos necesarios para ayudar al OSINFOR a remediarlo.
8. El proveedor debe garantizar el cumplimiento de las restricciones legales respecto del uso del material protegido por normas de propiedad intelectual.
9. El Proveedor y su personal únicamente podrá utilizar la información y activos de información autorizados por el OSINFOR para el desarrollo de los servicios contratados.
10. Queda estrictamente prohibido el uso de programas informáticos sin la correspondiente licencia en los sistemas de información del OSINFOR. No podrán ser utilizados tampoco programas de descarga gratuita que no estén autorizados por el fabricante y por la Oficina de Tecnología de la Información.
11. Asimismo, queda prohibido el uso, reproducción, cesión, transformación o comunicación pública de cualquier tipo de obra o invención protegida por derechos de propiedad intelectual sin la debida autorización de su titular.
12. La distribución de la información ya sea en formato digital o papel, se realizará mediante los recursos determinados en la contratación y para la finalidad

exclusiva de facilitar las funciones asociadas a dicho contrato. El OSINFOR, se reserva el derecho de adoptar las medidas de control, registro y auditoría sobre los recursos de difusión, en función del riesgo identificado.

13. El proveedor se compromete a informar al OSINFOR de los activos de información con los que presta el servicio.
14. Los recursos que el OSINFOR pone a disposición del Proveedor, independientemente del tipo que sean, (informáticos, datos, software, redes, sistemas de comunicación, etc.) están exclusivamente destinados para cumplir con las obligaciones y propósito para los que fueron proporcionados. El OSINFOR se reserva el derecho de implementar mecanismos de control y auditoría que verifiquen el uso apropiado de estos recursos.
15. Se deberán restituir al OSINFOR todos los activos físicos proporcionados para la ejecución de la contratación hasta su finalización. Todo activo físico del proveedor al que OSINFOR le haya instalado algún software, deberá ser entregado temporalmente al OSINFOR para que se proceda a la realización de un backup y posteriormente el "borrado seguro" de la información.
16. Se prohíbe expresamente:
    16.1. El uso de recursos proporcionados por el OSINFOR para actividades no relacionadas con el propósito de servicio.
    16.2. La conexión a la red del OSINFOR de equipos y/o aplicaciones que no estén especificados como parte del Software propio o bajo supervisión del OSINFOR.
    16.3. Introducir en los sistemas de información o la red del OSINFOR, contenidos que contravienen con la moral, ética y buenas costumbres observadas en la Ley Nº 27815 del Código de Ética de la Función Pública, para los casos que corresponda.
    16.4. Introducir, instalar y/o descargar por dolo o culpa inexcusable en la red del OSINFOR, cualquier tipo de malware, dispositivos lógicos, dispositivos físicos, o cualquier tipo de secuencia de órdenes que causen o sean susceptibles de causar cualquier tipo de alteración o daño en los recursos informáticos del OSINFOR.
    16.5. Intentar obtener sin autorización explícita otros derechos o accesos distintos a los que OSINFOR haya asignado.
    16.6. Intentar acceder, sin autorización explícita, a áreas restringidas de los Sistemas de Información del OSINFOR.
    16.7. Intentar distorsionar o falsear los registros "log" de los Sistemas de Información del OSINFOR.
    16.8. Poseer, desarrollar o ejecutar programas que pudieran dañar o alterar los recursos informáticos del OSINFOR, o intentar saltar las Políticas de Seguridad de la Información.
17. Los proveedores de servicio deberán asegurarse que todo el personal que preste servicios al OSINFOR, respete los siguientes principios básicos dentro de su actividad informática:
    17.1. Cada persona con acceso a la información del OSINFOR es responsable de la actividad desarrollada por su identificador de usuario y todo lo que derive.
    17.2. Los usuarios no deberán utilizar ningún identificador de otro usuario, aunque disponga de la autorización explícita del propietario.
18. El Proveedor deberá asegurar que los equipos que utilice su personal queden protegidos cuando no estén en uso.

19. Todo proveedor y/o contratista con acceso a la información del OSINFOR, deberá respetar la política de escritorio limpio, con el fin de proteger los documentos en papel y dispositivos de almacenamiento removibles y reducir los riesgos de acceso no autorizado, pérdida y daño de la información, durante el horario normal de trabajo del OSINFOR, y fuera del mismo:
    19.1. Almacenar bajo llave los documentos de papel y los medios informáticos con información del OSINFOR en mobiliario seguro cuando no están siendo utilizados.
    19.2. Bloquear el acceso de los equipos cuando no estén siendo utilizados.
    19.3. Proteger los documentos del OSINFOR que se encuentren en las impresoras.
    19.4. Los listados con datos de carácter personal o información confidencial del OSINFOR deberán almacenarse en un lugar seguro al que únicamente tengan acceso personas autorizadas.
20. Las personas con acceso a sistemas y/o información del OSINFOR nunca deberán, sin autorización explícita, realizar pruebas para detectar y/o utilizar una debilidad o incidente de seguridad de la información. En caso de identificarse algunos incidentes o debilidades relacionadas, deberán reportar lo ocurrido para su registro en el módulo de mesa de ayuda y/o informar al Oficial de Seguridad de la Información.
21. Las personas con acceso a sistemas y/o a información del OSINFOR, no deberán transgredir el sistema de seguridad de la información y las autorizaciones, ni capturar tráficos de red por parte de los usuarios, salvo que se esté llevando a cabo tareas de auditoría expresamente autorizadas.
22. Toda persona que acceda a la información y/o sistemas del OSINFOR deberá seguir las siguientes normas:
    22.1. Proteger la información confidencial de toda revelación no autorizada, modificación, destrucción o uso incorrecto, ya sea accidental o no.
    22.2. Proteger los sistemas de información y redes de telecomunicaciones contra accesos no autorizados, interrupciones de operaciones, destrucción, mal uso o robo.
    22.3. Contar con autorización necesaria para obtener acceso a los sistemas de información y/o la información accedidos.
23. El proveedor y/o contratista deberá mantener una lista actualizada de los equipos proporcionados por el OSINFOR y los usuarios de dichos activos de la información, o responsables asociados en caso que los activos no sean de uso unipersonal. Dicha relación podrá ser requerida por el OSINFOR en cualquier momento.
24. En caso de culminar el vínculo contractual del proveedor y/o contratista, este deberá devolver al OSINFOR todos los equipos recibidos.
25. Todos los servicios que impliquen accesos a la información o sistemas de información del OSINFOR, deberán cumplir con las siguientes políticas con respecto a su personal:
    25.1. El proveedor y/o contratista deberá verificar los antecedentes profesionales, penales y policiales del personal asignado al servicio.
    25.2. El proveedor y/o contratista deberá garantizar al OSINFOR la posibilidad de cambio de personal asignado al servicio, cuando se verifique algún incumplimiento de las políticas de seguridad de la información.

26. Todo proveedor deberá permitir que el OSINFOR lleve a cabo al menos una auditoría de seguridad del servicio en caso amerite, colaborando con el equipo auditor y facilitando todas las evidencias y registros que le sean requeridos.
27. El alcance y profundidad de la auditoría será establecido expresamente por el OSINFOR en cada caso.
28. El OSINFOR se reserva el derecho de realizar auditorías extraordinarias adicionales, siempre que se den las causas específicas que lo justifiquen.
29. El Proveedor y/o contratista deberá ponerse en contacto con la Oficina de Tecnología de la Información del OSINFOR en caso se detecte cualquier incidencia relacionada con la información o los recursos del OSINFOR.
30. Cualquier usuario podrá trasladar a la Oficina de Tecnología de la Información del OSINFOR, sugerencias, debilidades, vulnerabilidades y/o situaciones de riesgo que puedan tener relación con la seguridad de la información y las directrices contempladas en las presentes políticas de las que tenga conocimiento.
31. Todo personal del Proveedor y/o contratista deberá solicitar autorización expresa a la Oficina de Tecnología de la Información para ingresar a las instalaciones con un activo de información. En caso el activo sea utilizado con fines de prestación del servicio diario, se deberá completar el Formato N° 05 DECLARACIÓN JURADA DE BIENES Y EQUIPOS DE PROPIEDAD PARTICULAR1, y se deberá registrar en la lista de autorizaciones.
32. Todo personal del Proveedor y/o contratista deberá solicitar autorización expresa a la Unidad de Abastecimiento, en caso requiera ingresar y permanecer dentro de las instalaciones fuera del horario laboral.
33. El proveedor y/o contratista deberá contar con una garantía de continuidad del servicio, el cual garantizará al OSINFOR, la disponibilidad o restauración del servicio en el menor tiempo frente a cualquier evento o incidente que atente con los procesos del OSINFOR. Las características de dicha garantía se encontrarán establecidas en la contratación.
34. Todo proveedor y/o contratista será responsable de transmitir y hacer cumplir las Políticas de Seguridad de la Información del OSINFOR a terceros subcontratados, autorizados debidamente por OSINFOR.
35. Todo proveedor y/o contratista que presta servicios al OSINFOR, deberá suscribir la constancia de recepción y aceptación de esta política.
36. Todo proveedor y/o contratista en caso requiera hacer cambios en la gestión del servicio y que afecte a los activos de información, deberá solicitar autorización al OSINFOR para su evaluación.

**Glosario de Términos**

- **Proveedor:** Persona natural o jurídica que puede proveer o abastecer de bienes o servicios a cualquier cliente de lo necesario o conveniente para un fin determinado.
- **Contratista:** Contratista es un proveedor con vínculo con el OSINFOR.
- **Log:** Los Archivos de registro (o archivos de log) son archivos que contienen mensajes sobre el sistema, los servicios y las aplicaciones que se ejecutan en dicho sistema. Existen diferentes tipos de archivos de log dependiendo de la información.

[1] Directiva de administración, control y asignación en uso de bienes muebles de propiedad del OSINFOR vigente.

**Control de cambios**

| Versión | Fecha | Justificación[2] | Textos Modificados[3] | Responsable[4] |
|---|---|---|---|---|
| 01 | Elaboración inicial del documento | | | Oficina de Tecnología de la Información |
| | | | | |
| | | | | |

[2] Justificación de la nueva versión del documento, puede darse en los casos de a) Modificación, b) Actualización c) Reestructuración

[3] Señalar los párrafos, secciones literales que se han modificado e incorporado

[4] Señalar el dueño del proceso, indicar el documento o informe sustentatorio

# POLÍTICA DE GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

**DOCUMENTO CONTROLADO**

| | | | |
|---|---|---|---|
| Propuesto por: | Gestión de Tecnologías de la Información | Fecha de propuesta: | 29 AGO. 2018 |
| Aprobado por: | Jefatura del OSINFOR (antes Presidencia Ejecutiva)[1] | Fecha de aprobación: | |

(1) Decreto Legislativo N° 1085 Artículo 51.- "Modificación de los artículos 6 y 7 del OSINFOR"

## Índice

## POLÍTICA DE GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

I. Objetivo ..... 3
II. Alcance ..... 3
III. Política ..... 3
3.1 Responsabilidad ..... 3
3.2 Gestión de incidentes y mejoras de seguridad de la información ..... 3
Control de cambios ..... 5

# POLÍTICA DE GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

## I. Objetivo

Garantizar que los eventos de seguridad de la información y las debilidades asociadas a los sistemas de información sean comunicados de tal forma que se apliquen las acciones correctivas en el tiempo oportuno.

## II. Alcance

La Política definida en este documento se aplica a todo incidente que pueda afectar la seguridad de la información del OSINFOR.

## III. Política

### 3.1 Responsabilidad

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

El Oficial de Seguridad de la Información en conjunto con la **Unidad de Recursos Humanos** son responsables de comunicar los procedimientos de gestión de incidentes a los servidores al inicio y durante la relación laboral. Así mismo la el Oficial de Seguridad de la Información en conjunto con la **Unidad de Abastecimiento** son responsables de comunicar los procedimientos de gestión de incidentes a los terceros que presten algún servicio al OSINFOR.

La **Oficina de Asesoría Jurídica** participará en el tratamiento de incidentes de seguridad de la Información cuando se requiera su intervención.

Todo el personal del OSINFOR es responsable de reportar debilidades y/o incidentes de seguridad de la información que oportunamente sean detectados.

### 3.2 Gestión de incidentes y mejoras de seguridad de la información

#### 3.2.1 Responsabilidades y procedimientos

a) El Procedimiento de gestión de incidentes de seguridad de la información (SGSI-A5-PRO-008) es evaluado para identificar áreas de mejora y evaluar su alineamiento a los objetivos del proceso y de la institución.
b) Las responsabilidades de gestión de incidentes se encuentran en el Procedimiento de Gestión de Incidentes de Seguridad de la Información (SGSI-A5-PRO-008), para asegurar que se realice y comunique adecuadamente dentro del OSINFOR.
c) El Oficial de Seguridad de la Información comunica al Comité Gestión de Seguridad de la Información sobre la gestión de incidentes y a la Alta Dirección cuando corresponda.

### 3.2.2 Reporte de eventos y debilidades de seguridad de la información

a) Todo trabajador y tercero que preste algún servicio al OSINFOR tiene el deber de comunicar las debilidades, eventos o incidentes de seguridad de la información a Mesa de Ayuda mediante los canales establecidos.
b) La comunicación de los eventos, incidentes y/o debilidades es a través de teléfono 615-7373 Anexo 1234, correo electrónico (mesadeayuda@osinfor.gob.pe) o sistema web.

### 3.2.3 Evaluación, decisión y respuesta sobre los eventos de seguridad de información

a) Todo evento, debilidad y/o incidente de seguridad de la información es registrado, clasificado, evaluado y atendido de acuerdo con el Procedimiento de Gestión de Incidentes de Seguridad de la Información (SGSI-A5-PRO-008), para buscar una solución definitiva o en caso contrario brindar una solución temporal hasta establecer la solución definitiva.

### 3.2.4 Aprender de los incidentes de seguridad de la información

a) Se ha establecido el registro de lecciones aprendidas en el -Bitácora de Incidentes de Seguridad de la Información (SGSI-A5-FOR-036) con el cual buscamos generar una fuente de conocimiento en base a los incidentes reportados y así poder solucionar futuros incidentes en base a las acciones realizadas.

### 3.2.5 Recolección de evidencia

a) El OSINFOR cuenta con información para la identificación, recolección y conservación que puede servir como evidencia para propósitos de acción disciplinaria, o judicial según corresponda, conforme a lo establecido en el Procedimiento de gestión de incidentes de Seguridad de la Información (SGSI-A5-PRO-008).
b) Las evidencias de los incidentes de seguridad de la información serán conservadas en un repositorio de información.

## Glosario de Términos

- **Proveedor:** Persona natural o jurídica que puede proveer o abastecer de bienes o servicios a cualquier cliente de lo necesario o conveniente para un fin determinado.
- **Contratista:** Contratista es un proveedor con vínculo con el OSINFOR.
- **Log:** Los Archivos de registro (o archivos de log) son archivos que contienen mensajes sobre el sistema, los servicios y las aplicaciones que se ejecutan en dicho sistema. Existen diferentes tipos de archivos de log dependiendo de la información.

Falta Control de cambios

## Control de cambios

| Versión | Fecha | Justificación[1] | Textos Modificados[2] | Responsable[3] |
|---|---|---|---|---|
| 01 | Elaboración inicial del documento | | | Oficina de Tecnología de la Información |
| | | | | |
| | | | | |

[1] Justificación de la nueva versión del documento, puede darse en los casos de a) Modificación, b) Actualización c) Reestructuración

[2] Señalar los párrafos, secciones literales que se han modificado e incorporado

[3] Señalar el dueño del proceso, indicar el documento o informe sustentatorio

# POLÍTICA DE ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN EN LA CONTINUIDAD DEL NEGOCIO

**DOCUMENTO CONTROLADO**

| | | | |
|---|---|---|---|
| Propuesto por: | Gestión de Tecnologías de la Información | Fecha de propuesta: | 29 AGO. 2018 |
| Aprobado por: | Jefatura del OSINFOR (antes Presidencia Ejecutiva)[1] | Fecha de aprobación: | |

(1) Decreto Legislativo N° 1085 Artículo 51.- "Modificación de los artículos 6 y 7 del OSINFOR"

## Índice

## POLÍTICA DE ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN EN LA CONTINUIDAD DEL NEGOCIO

**I. Objetivo** ..... 3

**II. Alcance** ..... 3

**III. Política** ..... 3

**Control de cambios** ..... 3

# POLÍTICA DE ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN EN LA CONTINUIDAD DEL NEGOCIO

## I. Objetivo

Establecer los lineamientos para la Gestión de los Aspectos de Seguridad de la Información para la Continuidad del Negocio del OSINFOR.

## II. Alcance

El alcance de la Política de Aspectos de Seguridad de la Información en la Gestión de la Continuidad del Negocio debe ser conocida y cumplida por los directivos, todo el personal que laboren, designado o contratado y terceros que presten algún servicio al OSINFOR.

## III. Política

a) El Procedimiento de Gestión de la Continuidad (SGSI-A5-PRO-009), es evaluado de forma semestral, para identificar áreas de mejora y evaluar su alineamiento a los objetivos del proceso y del negocio en coordinación con el Técnico de Mantenimiento y Seguridad.
b) Se supervisa el cumplimiento del proceso de la seguridad de la información en la implementación de los controles.
c) Se cuenta con instalaciones definidas e implementadas de procesamiento de información redundante con capacidad suficiente para garantizar la disponibilidad del negocio.
d) Se cuenta con una estructura establecida y definida de personal con la responsabilidad, autoridad y competencia necesaria para la ejecución de los Planes de Contingencia.

**Control de cambios**

| Versión | Fecha | Justificación[1] | Textos Modificados[2] | Responsable[3] |
|---|---|---|---|---|
| 01 | Elaboración inicial del documento | | | Oficina de Tecnología de la Información |
| | | | | |
| | | | | |

[1] Justificación de la nueva versión del documento, puede darse en los casos de a) Modificación, b) Actualización c) Reestructuración
[2] Señalar los párrafos, secciones literales que se han modificado e incorporado
[3] Señalar el dueño del proceso, indicar el documento o informe sustentatorio

# POLÍTICA DE CUMPLIMIENTO

**DOCUMENTO CONTROLADO**

| | | | |
|---|---|---|---|
| Propuesto por: | Gestión de Tecnologías de la Información | Fecha de propuesta: | 29 AGO. 2018 |
| Aprobado por: | Jefatura del OSINFOR (antes Presidencia Ejecutiva)[1] | Fecha de aprobación: | |

(1) Decreto Legislativo N° 1085 Artículo 51.- "Modificación de los artículos 6 y 7 del OSINFOR"

## Índice
## POLÍTICA DE CUMPLIMIENTO

I. **Objetivos** ..... 3
II. **Alcance** ..... 3
III. **Política** ..... 3
**Control de cambios** ..... 4

# POLÍTICA DE CUMPLIMIENTO

## I. Objetivos

**1.1.** Garantizar el cumplimiento de cualquier requisito reglamentario, regulación u obligación contractual y de todos los requisitos de seguridad de la información implementados por el OSINFOR.
**1.2.** Verificar el cumplimiento de las políticas y normas de Seguridad de la Información en los sistemas de información del OSINFOR.
**1.3.** Mantener un efectivo proceso de auditoría a los sistemas de información.

## II. Alcance

El alcance de todas las políticas de seguridad de la información abarca todos los aspectos administrativos y de control que debe ser conocida y cumplida por los directivos, personal que labora designado o contratado, así como por terceros que presten algún servicio al OSINFOR.

## III. Política

1. Se supervisa el cumplimiento de requisitos legales y normativas vigentes según lo detallado en el Procedimiento de Gestión de Cumplimiento (SGSI-A5-PRO-010).
2. Se evalúa el impacto de todos los requisitos legales y normativas vigentes que aplican al OSINFOR, esta información la remite la Oficina de Asesoría Jurídica. Para el control interno del SGSI se debe completar el Formato Matriz de Evaluación de Requisitos Legales y Otros Requisitos (SGSI-A5-FOR-026), verificado su cumplimiento.
3. Se supervisa el cumplimiento del uso de software permitido y los respectivos acuerdos contractuales relacionados a los derechos de propiedad intelectual.
4. Se cumple con el resguardo de registros de backups según los lineamientos establecidos en la Política de Seguridad de las Comunicaciones (SGSI-A5-POL-010), con ello se debe resguardar los registros garantizando la confidencialidad y disponibilidad de dicha información.
5. Se supervisa el cumplimiento del Programa Anual de Auditorías del SGSI de manera que permita evaluar la efectividad de los controles implementados.
6. Los responsables de los diferentes procesos son los encargados de supervisar el cumplimiento de los procedimientos y del procesamiento de la información dentro de su área de responsabilidad, de acuerdo sus políticas y controles.
7. Se supervisa anualmente evaluaciones técnicas especializadas mediante un tercero para verificar el cumplimiento de los controles técnicos implementados.

## Control de cambios

| Versión | Fecha | Justificación[1] | Textos Modificados[2] | Responsable[3] |
|---|---|---|---|---|
| 01 | Elaboración inicial del documento | | | Oficina de Tecnología de la Información |
| | | | | |
| | | | | |

[1] Justificación de la nueva versión del documento, puede darse en los casos de a) Modificación, b) Actualización c) Reestructuración

[2] Señalar los párrafos, secciones literales que se han modificado e incorporado

[3] Señalar el dueño del proceso, indicar el documento o informe sustentatorio