RESOLUCIÓN DE GERENCIA GENERAL

Lima, 13 de julio de 2021 **N° 074-2021-GG-OSITRAN**

VISTOS:

El Informe N° 147-2021-JTI-GA-OSITRAN y el Memorando N° 180-2021-JTI-GA-OSITRAN elaborados por la Jefatura de Tecnologías de la Información de la Gerencia de Administración; el Informe N° 0054-2021-GPP-OSITRAN de la Gerencia de Planeamiento y Presupuesto; el Memorando Nº 304-2021-GAJ-OSITRAN de la Gerencia de Asesoría Jurídica; y

CONSIDERANDO:

Que, el artículo 1 de la Ley N° 27658, Ley Marco de Modernización de la Gestión del Estado, declara al Estado en proceso de modernización en sus diferentes instancias, dependencias, entidades, organizaciones y procedimientos, con la finalidad de mejorar la gestión pública y construir un Estado democrático, descentralizado y al servicio del ciudadano;

Que, mediante Decreto Supremo N° 004-2013-PCM se aprueba la Política Nacional de Modernización de la Gestión Pública que tiene como uno de sus ejes transversales, al Gobierno Electrónico, cuyo objetivo es orientar, articular e impulsar en todas las entidades públicas el proceso de modernización hacia una gestión pública para resultados que impacte positivamente en el bienestar del ciudadano y el desarrollo del país;

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

Que, mediante Resolución Ministerial N° 166-2017-PCM se modifica el artículo 5 de la Resolución Ministerial N° 004-2016-PCM relativo a la conformación del Comité de Seguridad de la Información, y se incorpora el artículo 5-A, en el cual se establecen las funciones del mencionado Comité;

Que, mediante Resolución Ministerial N° 087-2019-PCM se modifica la Resolución Ministerial N° 119-2018-PCM, aprobando disposiciones sobre la conformación y funciones del Comité de Gobierno Digital, así como dejando sin efecto los artículos 2, 5 y 5-A de la Resolución Ministerial N°004-2016-PCM, modificada mediante Resolución Ministerial N° 166-2017-PCM;

Que, mediante Resolución de Presidencia N° 0029-2019-PD-OSITRAN se actualizó la conformación y funciones del Comité de Gobierno Digital conformado mediante Resolución de Presidencia N° 037-2018-PD-OSITRAN, incorporando dentro del alcance de sus competencias funciones relativas a la gestión del Modelo de Gestión Documental, Modelo de Datos Abiertos Gubernamentales y Sistema de Gestión de Seguridad e la Información de la entidad;

Que, mediante la Resolución de Gerencia General 175-2019-GG-OSITRAN se aprobó la Directiva para la Formulación y aprobación de instrumentos de gestión interna del Ositrán, que

Calle Los Negocios 182, piso 2
Surquillo - Lima
Central Telefónica: (01) 500-9330
www.ositran.gob.pe

guía a las unidades de organización del Ositrán en el proceso de formulación, revisión, aprobación, difusión, implementación y actualización de directivas, e instructivos, que rigen la gestión administrativa interna del Ositrán.

Que, en el marco de lo dispuesto mediante la cláusula 5.2 de la Norma Técnica Peruana NTP ISO/IEC 27001:2014, mediante Resolución de Presidencia N° 042-2019-PD-OSITRAN, la presidente del Consejo Directivo aprueba la Política y Objetivos de Seguridad de la Información del OSITRAN;

Que, a través del Informe N° 147-2021-JTI-GA-OSITRAN de 27 de mayo de 2021, la Jefatura de Tecnologías de la Información elaboró la propuesta de Directiva de Seguridad de la Información del Ositrán, así como sustentó la necesidad técnica de su aprobación, toda vez que permitirá establecer mecanismos que contribuyen al despliegue exitoso de la fase de operación y mantenimiento del Sistema de Gestión de Seguridad de la Información de la entidad, a fin de dar cumplimiento a los controles técnicos establecidos por la Norma Técnica Peruana ISO/IEC 27001:2014. Esto, permitirá dar cumplimiento a las disposiciones de la Resolución Ministerial N°004-2016-PCM, así como contribuir al logro de los compromisos establecidos en la Política de Seguridad de la Información vigente;

Que, con Informe N° 0054-2021-GPP-OSITRAN, la Gerencia de Planeamiento y Presupuesto, emitió opinión técnica respecto del referido proyecto en el marco de sus competencias en materia de presupuesto, desarrollo organizacional, racionalización, mejora continua y calidad, indicando que cumple con lo dispuesto en la Directiva para la Formulación, Revisión y Aprobación de instrumentos de Gestión Interna del Ositrán;

Que, mediante Memorando N° 180-2021-JTI-GA-OSITRAN de 12 de julio de 2021, la Jefatura de Tecnologías de la Información remitió una nueva versión de la propuesta de Directiva de Seguridad de la Información del Ositrán, recogiendo las modificaciones solicitadas por la Gerencia General mediante Memorando N° 257-2021-GG-OSITRAN;

Que, la Gerencia de Asesoría Jurídica, a través del Memorando N° 304-2021-GAJ-OSITRAN, luego de la revisión de los aspectos legales del procedimiento seguido en la formulación de la propuesta de Directiva de Seguridad de la Información del Ositrán, elaborada por la Jefatura de Tecnologías de la Información; considera la propuesta jurídicamente viable;

Que, en mérito a lo establecido en los artículos 10° y 11° del Reglamento de Organización y Funciones del OSITRAN, aprobado por Decreto Supremo N° 012-2015-PCM y modificatorias, la Gerencia General es la máxima autoridad administrativa del Ositrán y es responsable de aprobar normas y otros documentos e instrumentos de gestión interna, relativos a la marcha administrativa de la institución para el cumplimiento de las unidades de organización del Ositrán, y;

De conformidad con lo dispuesto en la Resolución Ministerial N°004-2016-PCM; el Reglamento de Organización y Funciones del Ositrán, aprobado por Decreto Supremo N° 012-2015-PCM; y la Directiva para la Formulación y Aprobación de Instrumentos de Gestión Interna del OSITRAN, aprobada por Resolución de Gerencia General Nº 175-2019-GG-OSITRAN.

Calle Los Negocios 182, piso 2
Surquillo - Lima
Central Telefónica: (01) 500-9330
www.ositran.gob.pe

SE RESUELVE:

Artículo 1.- Aprobar la Directiva de Seguridad de la Información del Ositrán, que como anexo forma parte de la presente resolución.

Artículo 2.- Dejar sin efecto todos aquellos lineamientos de la DIR-GG-ODIS-001-14 "Directiva para la gestión de recursos informáticos del Ositran", aprobada mediante Resolución de Gerencia General Nº 01-2014-GG-OSITRAN, que se opongan a la directiva que se aprueba mediante la presente resolución.

Artículo 3.- Encargar a la Gerencia de Administración, a través de la Jefatura de Tecnologías de la Información, el seguimiento del cumplimiento de la directiva que se aprueba mediante la presente resolución.

Artículo 4.- Poner en conocimiento de la presente directiva a la Oficina de Comunicación Corporativa para la difusión en la intranet y en el portal institucional de la entidad (www.ositran.gob.pe).

Regístrese y comuníquese,

JUAN CARLOS MEJÍA CORNEJO
Gerente General

NT: 2021061966

Calle Los Negocios 182, piso 2
Surquillo - Lima
Central Telefónica: (01) 500-9330
www.ositran.gob.pe

	Denominación	Código:
OSITRAN EL REGULADOR DE LA INFRAESTRUCTURA DE TRANSPORTE DE USO PÚBLICO	**DIRECTIVA DE SEGURIDAD DE LA INFORMACIÓN DEL OSITRAN**	DIR-GA-JTI-01
		Versión 01
	Aprobado por Resolución N°	074-2021-GG-OSITRAN

I. Objeto

Establecer lineamientos para la gestión y operación de la seguridad de la información en el Organismo Supervisor de la Inversión en Infraestructura de Transporte de Uso Público (en adelante Ositrán).

II. Finalidad

Procurar la preservación de la confidencialidad, disponibilidad e integridad de la información del Ositrán.

III. Base legal

3.1. Ley N° 27269, Ley de Firmas y Certificados Digitales y su modificatoria.
3.2. Ley N° 27815, Ley del Código de Ética de la Función Pública.
3.3. Ley N° 29733, Ley de Protección de Datos Personales y su modificatoria.
3.4. Ley N° 30096, Ley de Delitos Informáticos y sus modificatorias.
3.5. Decreto Legislativo N° 1412, que aprueba la Ley de Gobierno Digital.
3.6. Decreto de Urgencia N° 007-2020, que aprueba el marco de confianza digital y dispone medidas para su fortalecimiento.
3.7. Decreto Supremo N° 072-2003-PCM, que aprueba el Reglamento de la Ley de Transparencia y Acceso a la Información Pública; y sus modificatorias.
3.8. Decreto Supremo N° 52-2008-PCM, que aprueba el Reglamento de la Ley de Firmas y Certificados Digitales y sus modificatorias.
3.9. Decreto Supremo N° 003-2013-JUS, que aprueba el Reglamento de la Ley de Protección de Datos Personales.
3.10. Decreto Supremo N° 012-2015-PCM, que aprueba el Reglamento de Organización y Funciones del Ositrán.
3.11. Decreto Supremo N° 033-2015-PCM, que aprueba el Reglamento de la Ley del Código de Ética de la Función Pública.
3.12. Decreto Supremo N° 021-2019-JUS, que aprueba el Texto Único Ordenado de la Ley N° 27806, Ley de Transparencia y Acceso a la Información Pública.
3.13. Decreto Supremo Nº 029-2021-PCM, que aprueba el Reglamento del Decreto Legislativo N° 1412, Decreto Legislativo que aprueba la Ley de Gobierno Digital, y establece disposiciones sobre las condiciones, requisitos y uso de las tecnologías y medios electrónicos en el procedimiento administrativo.
3.14. Resolución N° 129-2014/CNB-INDECOPI, que aprueba 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".
3.15. Resolución Ministerial N° 004-2016-PCM, que aprueba el uso obligatorio de la Norma Técnica Peruana "NTP-ISO/IEC 27001:2014 Tecnología de la información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 2ª. Edición", en todas las entidades integrantes del Sistema Nacional de Informática.
3.16. Resolución Ministerial N°087-2019-PCM que aprueba disposiciones sobre la conformación y funciones del Comité de Gobierno Digital.

Visado por: FALCONE VARGAS Liccia Maria FAU 20420248645 hard
Motivo: Firma Digital
Fecha: 13/07/2021 17:13:26 -0500

Visado por: CHEN CHEN Thou Su FAU 20420248645 soft
Motivo: Firma Digital
Fecha: 13/07/2021 16:46:54 -0500

Visado por: TALLEDO LEON Cesar Enrique FAU 20420248645 hard
Motivo: Firma Digital
Fecha: 13/07/2021 16:31:42 -0500

IV. Alcance

La presente directiva es de observancia obligatoria para todos los servidores civiles que laboran en las unidades de organización señaladas en el ROF del Ositrán.

También se aplica, en cuanto corresponda, a quienes, no teniendo la condición de servidores civiles, por razón de sus funciones, convenios de prácticas o servicios, acceden a la información del Ositrán.

V. Glosario de Términos

Para efectos de la presente directiva se considerarán las siguientes definiciones, las cuales han sido tomadas de la ISO 27001 y del marco normativo vigente aplicable, o en su defecto han sido desarrolladas específicamente para el entendimiento del presente documento.

5.1. **Acceso:** Permiso otorgado a una cuenta de usuario, que faculta a dicho usuario a hacer uso de determinada información, sistemas, servicios u otros recursos informáticos que sean necesarios para el ejercicio de sus funciones.

5.2. **Acceso privilegiado:** Permiso otorgado a una cuenta de usuario, que otorga facultades superiores a las atribuidas a las cuentas estándar. Son asignados a los administradores de TI y faculta a los mismos a realizar configuraciones en un sistema o aplicación, añadir o eliminar cuentas, datos, entre otros.

5.3. **Acceso remoto:** Mecanismo que permite a los usuarios conectarse a una red de datos o una computadora de forma remota a través de una conexión a internet, a fin de poder hacer uso de los servicios tecnológicos, sistemas o información digital necesaria para el ejercicio de sus funciones.

5.4. **Activos de información:** Todo aquello que represente valor para el Ositrán y que participe en el proceso de almacenamiento o tratamiento de la información. Pueden ser de tipo proceso, información, sistema, hardware, software, medio de soporte, personal, red y comunicaciones, servicios tecnológicos, sitio, entre otros.

5.5. **Backup:** Copia de seguridad o de respaldo. Es una copia de los datos originales que se realiza con el fin de disponer de un medio para recuperarlos en caso de pérdida o alteración.

5.6. **Ciberseguridad:** Capacidad tecnológica de preservar el adecuado funcionamiento de las redes, activos y sistemas informáticos y protegerlos ante amenazas y vulnerabilidades en el entorno digital. Comprende la perspectiva técnica de la Seguridad Digital y es un ámbito del Marco de Seguridad Digital del país.

5.7. **Colaborador:** Servidor civil de la entidad. Así como también aquel que, no teniendo la condición de servidor civil, por razón de sus funciones, convenios de prácticas o servicios, acceden a la información del Ositrán.

5.8. **Comité de Gobierno Digital (en adelante CGD):** Grupo de personas responsables del gobierno y transformación digital en la entidad, conformado en cumplimiento de lo dispuesto por la PCM mediante Resolución Ministerial N° 087-2019-PCM.

5.9. **Confidencialidad:** Propiedad por la cual la información no está disponible o no puede ser divulgada a personas, entidades o procesos de negocio no autorizados.

5.10. **Cuenta de Usuario:** Credenciales que se le otorga a un colaborador para el acceso a la red de datos o computadora de la entidad.

5.11. **Custodio:** Colaborador de la entidad designado para administrar y hacer efectivos los controles de seguridad que el propietario del activo de información haya definido.

5.12. **Datos personales:** Toda información sobre una persona natural que la identifica o la hace identificable a través de medios que pueden ser razonablemente utilizados.

5.13. **Disponibilidad:** Propiedad de la información de estar accesible para el uso de las personas, entidades o procesos autorizados cuando lo requieran.

5.14. **Dispositivos móviles:** Teléfonos móviles o tablets que son asignados a los servidores civiles para el cumplimiento de sus funciones.
5.15. **Dueño del proceso:** Titular de la unidad de organización responsable del proceso.
5.16. **Integridad:** Propiedad de precisión y completitud de la información.
5.17. **Información:** Conjunto de datos que tiene valor para el Ositrán.
5.18. **Mesa de ayuda:** Servicio de atención y gestión de requerimientos e incidencias vinculadas con los equipos o recursos informáticos de la entidad.
5.19. **Oficial de Seguridad de la Información (OSI):** Servidor civil designado formalmente por la alta dirección y comunicado a la entidad para liderar las coordinaciones necesarias para la implementación y mantenimiento del Sistema de Gestión de Seguridad de la Información (en adelante SGSI) dentro de la entidad.
5.20. **Propietario del activo de información:** Responsable de controlar la producción, desarrollo, mantenimiento, uso y seguridad de los activos de información.
5.21. **Propietario del riesgo:** Responsable de aprobar el plan de tratamiento de los riesgos de seguridad de la información. Tiene la responsabilidad y autoridad para gestionar el riesgo. Generalmente este rol o función recae en los propietarios de los procesos.
5.22. **Seguridad de la Información:** Preservación de la confidencialidad, integridad y disponibilidad de la información.
5.23. **Seguridad Informática:** Protección de las infraestructuras tecnológicas y de comunicaciones.
5.24. **Seguridad Digital:** Estado de confianza en el entorno digital que resulta de la gestión y aplicación de un conjunto de medidas proactivas y reactivas frente a los riesgos que afectan la seguridad de las personas, la prosperidad económica y social, la seguridad y los objetivos nacionales en dicho entorno.
5.25. **Sesión:** Tiempo determinado de interacción del usuario con la computadora.
5.26. **Unidades de organización:** órganos, unidades orgánicas u oficinas establecidas en el ROF del Ositrán.
5.27. **Usuario:** Colaborador de la entidad que cuenta con acceso a la red de datos y que hace uso de servicios y recursos tecnológicos.

VI. Disposiciones Generales

6.1. Todos los colaboradores del Ositrán deben cumplir los lineamientos de seguridad de la información establecidos en la presente directiva.
6.2. La información y los activos de información a la que los colaboradores accedan, deben ser empleados exclusivamente para el cumplimiento de sus funciones y/o actividades.
6.3. Todos los colaboradores del Ositrán deben involucrarse en la gestión y operación de la seguridad de la información en la entidad, de acuerdo con los roles y responsabilidades definidos en la presente directiva.
6.4. La Jefatura de Tecnologías de la Información (en adelante JTI) en coordinación con la Jefatura de Gestión de Recursos Humanos (en adelante JGRH) debe planificar y ejecutar acciones de capacitación y concientización en materia de seguridad de la información.
6.5. La JTI, en coordinación con las unidades de organización, debe ejecutar acciones para velar por el cumplimiento de las políticas y controles de seguridad de la información por parte de los proveedores. Cualquier incumplimiento por parte de estos últimos se comunicará a la Jefatura de Logística y Control Patrimonial (en adelante JLCP) para la notificación formal al proveedor.
6.6. Todos los colaboradores deben participar de las acciones de capacitación y concientización que sean programadas en materia de seguridad de la información.
6.7. La JTI es responsable de implementar los controles tecnológicos que contribuyan a preservar la confidencialidad, integridad y disponibilidad de la información institucional almacenada en los sistemas de información.

6.8. Los titulares de las unidades de organización deben velar por la preservación de la confidencialidad, integridad y disponibilidad de la información de la que son propietarios, así como facilitar las revisiones periódicas para la verificación del cumplimiento de la política, procedimientos y controles de seguridad de la información bajo el ámbito de sus competencias.

6.9. Los titulares de las unidades de organización son responsables de la identificación y gestión de los riesgos de seguridad vinculados a los procesos que se encuentran bajo el ámbito de sus competencias.

6.10. Los titulares de las unidades de organización son responsables de identificar y proteger los activos de información bajo el ámbito de sus competencias, así como procurar el tratamiento de los mismos según su clasificación; lo cual no exime de responsabilidad directa al colaborador que se le asignó el activo de información para el uso de sus actividades.

6.11. La difusión de la información institucional del Ositrán tanto a nivel interno como externo, debe realizarse exclusivamente por el personal autorizado y a través de los canales y medios oficiales.

6.12. Todo colaborador que identifique algún posible evento o incidente en materia de seguridad de la información debe reportarlo a las instancias correspondientes, a través de los canales establecidos para dicho fin.

6.13. El incumplimiento de las disposiciones de la presente directiva podría ser pasible del ejercicio de la potestad sancionadora en materia disciplinaria de la entidad.

VII. Disposiciones Específicas

7.1. Organización de la Seguridad de la Información

7.1.1. Organización Interna

7.1.1.1. Roles y responsabilidades

El Ositrán ha establecido los siguientes roles y responsabilidades para la gestión de la seguridad de la información:

Alta Dirección

La Alta Dirección para el Sistema de Gestión de Seguridad de la Información está compuesta por el Comité de Gobierno Digital.

Comité de Gobierno Digital (CGD)

a) Liderar la implementación del SGSI en la entidad.
b) Gestionar la asignación de personal y recursos necesarios para la implementación del SGSI en sus Planes Operativos Institucionales, Plan Anual de Contrataciones y otros.
c) Promover y gestionar la implementación de estándares y buenas prácticas en Seguridad de la información.
d) Vigilar el cumplimiento de la normatividad relacionada con la implementación de la seguridad de la información en las entidades públicas.
e) Gestionar, mantener y documentar el SGSI de la entidad.

Las responsabilidades antes señaladas para el Comité de Gobierno Digital en el marco del SGSI de la entidad, se ejercen sin perjuicio de las demás funciones atribuidas a dicha instancia, conforme el marco normativo vigente.

Oficial de Seguridad de la Información

a) Coordinar y monitorear las actividades relacionadas con la implementación, operación y mantenimiento del SGSI en todos los dominios de la norma ISO 27001, para determinar su eficacia.
b) Gestionar la elaboración y/o actualización de los documentos para la gestión del SGSI de la entidad.
c) Proponer políticas, directivas y/o lineamientos requeridos para un adecuado gobierno de la seguridad de la información y la ciberseguridad.
d) Coordinar y garantizar la realización de las auditorías y revisiones por la dirección del SGSI.
e) Coordinar la ejecución de actividades de capacitación y concientización a los colaboradores de la entidad en temas de seguridad de la información.
f) Impulsar el cumplimiento de la normatividad emitida por la Secretaría de Gobierno y Transformación Digital en materia de seguridad de la información y temas vinculados.
g) Coordinar las acciones operativas de seguridad de la información, planteando estrategias de acuerdo con los requerimientos de seguridad de la entidad.
h) Coordinar a todo nivel el cumplimiento de los objetivos de preservación de los principios de confidencialidad, integridad y disponibilidad de la información, acorde con el Sistema de Gestión de Seguridad de la Información.
i) Representar a la entidad ante organizaciones externas, sobre temas de seguridad de la información.
j) Asesorar para resolver problemas de seguridad de la información.
k) Definir mecanismos para monitorear efectivamente el Sistema de Gestión de Seguridad de la Información y reportar periódicamente su efectividad.
l) Coordinar con los responsables de respuesta a incidentes los resultados de las investigaciones sobre seguridad de la información.
m) Informar a la alta dirección sobre el desempeño y oportunidades de mejora del SGSI.

Analista en Seguridad de la Información

a) Proponer o actualizar documentos normativos o lineamientos que contribuyan a implementar la seguridad de la información.
b) Conducir el proceso de identificación de activos de información, así como de la identificación, análisis y evaluación de riesgos u oportunidades de seguridad de la información asociados a los mismos.
c) Efectuar seguimiento a la implementación del Plan tratamiento de riesgos, así como de los controles definidos en el SGSI.
d) Monitorear la gestión de eventos e incidentes de seguridad de la información.
e) Monitorear la infraestructura de TI del Ositrán, identificar y reportar vulnerabilidades en materia de ciberseguridad y seguridad informática.
f) Evaluar y efectuar seguimiento a la gestión de los riesgos de seguridad de la información de proyectos y requerimientos.
g) Brindar capacitación requerida por los proyectos o unidades de organización que correspondan en la gestión de riesgos de seguridad de la información.
h) Supervisar y/o ejecutar las revisiones de seguridad de los dominios de seguridad en recursos humanos, seguridad en desarrollo y/o adquisición de sistemas y seguridad en las redes y comunicaciones.

Titulares de las unidades de organización

a) Participar de las actividades de identificación de activos de información, así como de la identificación, análisis y evaluación de riesgos de los procesos bajo el ámbito de sus competencias. Asimismo, aprobar los documentos resultantes de dichas actividades.
b) Apoyar y facilitar las revisiones periódicas para la verificación del cumplimiento de las políticas y procedimientos de seguridad de la información en los procesos bajo el ámbito de sus competencias.
c) Comunicar requerimientos de control y protección de la información al Oficial de Seguridad de la Información y asegurar que la información y activos bajo su control estén debidamente protegidos.
d) Apoyar en la difusión de la(s) política(s) y procedimiento(s) de seguridad de la información a los colaboradores bajo su cargo.
e) Determinar los niveles de acceso de los colaboradores a su cargo a la información, sistemas de información y servicios tecnológicos bajo el ámbito de sus competencias. Así como, notificar la modificación o cancelación de los accesos asignados.
f) Reportar inmediatamente el incumplimiento o infracciones a las políticas y normas de seguridad de la información a través del canal establecido para dicho fin.
g) Revisar y validar todos los procedimientos y formatos del SGSI que le correspondan.

Propietario de riesgos

a) Participar y/o designar a los miembros del equipo de trabajo para el proceso de identificación, análisis y evaluación de los riesgos y oportunidades de seguridad de la información.
b) Aprobar las acciones del plan de tratamiento de riesgos y riesgo residual correspondiente, en el ámbito de sus competencias y gestionar su implementación.
c) Informar al OSI respecto del nivel de implementación de las acciones de tratamiento de riesgos bajo su competencia.
d) Firmar las actas de aceptación de riesgos cuando corresponda.

Propietario de activos

a) Valorizar los activos de información bajo su competencia.
b) Validar la clasificación de la información con el propósito de verificar que se cumpla con los requerimientos de la entidad.
c) Apoyar activamente en las actividades de identificación, análisis, evaluación y tratamientos de riesgos de seguridad de la información.
d) Autorizar la asignación de accesos sobre la información bajo el alcance de sus competencias en coordinación con el titular de la unidad de organización.
e) Autorizar los cambios sobre los activos de información bajo el alcance de sus competencias en coordinación con el titular de la unidad de organización.
f) Contribuir a la implementación de los controles de seguridad que estén relacionados con sus funciones.
g) Revisar y dar la conformidad a los resultados de la gestión de riesgos, el plan de tratamiento de riesgos y los riesgos residuales.
h) Brindar información oportuna y pertinente para la elaboración de indicadores y métricas, auditoría, revisión y mejora continua del SGSI, respecto a los activos de información a su cargo.

Colaboradores del Ositrán

a) Conocer, comprender y dar cumplimiento a las políticas, directivas, procedimientos o lineamientos en materia de seguridad de la información de la entidad.
b) Reportar eventos, incidentes y riesgos de seguridad de la información identificados durante el desempeño de sus funciones; a las instancias pertinentes, a través de los canales correspondientes.
c) Participar en las actividades relacionadas a la gestión de riesgos de seguridad de la información.
d) Utilizar la información, activos, sistemas y servicios tecnológicos de la entidad únicamente para los propósitos autorizados e inherentes a sus funciones o actividades.
e) Proteger los recursos informáticos a fin de mantener y preservar la disponibilidad, confidencialidad e integridad de la información a la que tienen acceso, evitando, además, su divulgación fuera de los canales formales establecidos.

7.1.1.2. **Segregación de funciones**

El OSI, con el fin de reducir el riesgo de uso incorrecto de los activos de la entidad, ya sea accidental o intencionado, debe gestionar la segregación de las funciones o roles en las unidades de organización que presentan conflicto en sus actividades dentro del SGSI.

7.1.1.3. **Contacto con autoridades y grupos de interés en Seguridad de la Información**

a) El OSI debe mantener activamente comunicación con autoridades y grupos de interés relacionados con la seguridad de la información, pudiendo estas ser instancias técnicas de apoyo o asesoría en dicha materia u otras a quienes se podrá recurrir en el caso de un incidente que pusiera en riesgo la confidencialidad, integridad y disponibilidad de la información de la entidad.
b) El listado de dichas autoridades o grupos de interés debe ser registrada en una matriz, la cual debe ser actualizada por el OSI o por quien este designe, de manera periódica o cuando ocurran cambios significativos en el contexto externo y/o interno en la entidad.
c) En el caso de un incidente mayor, que requiera el pronunciamiento institucional ante la sociedad, autoridades o grupos de interesados, esta comunicación podrá ser efectuada por la Alta Dirección o por quien ésta designe.

7.1.1.4. **Seguridad de la información en la gestión de proyectos**

Las unidades de organización son responsables de considerar aspectos de seguridad de la información descritos en la presente directiva o en los procedimientos del SGSI, en cada uno de los proyectos que ejecuten en la entidad. Para ello, deben solicitar asistencia al OSI para asegurar que los riesgos de seguridad de la información se identifican y se contemplan en el marco del proyecto.

7.1.2. Dispositivos móviles y teletrabajo o trabajo remoto

7.1.2.1. **Seguridad de la información para el uso de dispositivos móviles**

a) El OSI debe proponer los lineamientos y medidas de seguridad apropiadas para la protección contra los riesgos asociados a la utilización de dispositivos móviles en la entidad.

b) El uso y asignación de dispositivos móviles debe ser autorizado y solicitado por el titular de la unidad de organización.
c) La JTI activará en los dispositivos móviles asignados las configuraciones y herramientas de seguridad para su uso.
d) Todos los dispositivos móviles asignados deben contar con la última o la más segura actualización de los sistemas operativos y aplicativos obtenidos de fuentes originales y seguras.
e) No está permitido la utilización del dispositivo móvil para divulgar información no autorizada de la entidad, o para un uso diferente para el que fue asignado.
f) En caso de pérdida o robo del dispositivo asignado por la entidad, el servidor civil debe reportarlo inmediatamente a la mesa de ayuda de la JTI.

7.1.2.2. **Seguridad de la información en el teletrabajo o trabajo remoto**

a) El OSI debe disponer de un lineamiento y medidas de seguridad que defina las condiciones y restricciones para acceder, tratar o almacenar la información en el uso del trabajo remoto o teletrabajo en la entidad.
b) Por defecto el acceso remoto a la red de datos y sistemas de la entidad se encuentra restringido y para su activación deberá ser autorizado de manera expresa por el titular de la unidad de organización y validado por el OSI. Dicho acceso es otorgado por un periodo determinado y de acuerdo con el perfil del usuario.
c) El acceso remoto a la red de datos y sistemas de la entidad es activado por la JTI, y se debe efectuar a través accesos de tipo VPN (Red Privada Virtual por sus siglas en inglés) o mecanismos equivalentes y de las correspondientes credenciales de red (usuario y contraseña) previamente asignadas al colaborador.
d) El acceso remoto a la red de datos y sistemas de la entidad se debe realizar únicamente a través de equipos informáticos asignados por la entidad, los mismos que cuentan con los mecanismos de seguridad necesarios.
e) El uso de un equipo de propiedad del colaborador está permitido únicamente para el acceso vía web a las herramientas colaborativas de la entidad (correo electrónico, teams, sharepoint, onedrive o similares) o para el uso de herramientas de escritorio remoto o virtual previamente habilitados por la JTI.
f) El colaborador es responsable de mantener el equipo de su propiedad con antivirus y las actualizaciones de seguridad vigentes para el acceso vía web a las herramientas colaborativas de la entidad, lo cual puede ser verificado por personal de la JTI. En caso de los servidores civiles que no puedan mantener el equipo de su propiedad con antivirus y las actualizaciones de seguridad correspondientes, éstos deberán necesariamente emplear un equipo de la entidad.

7.2. Seguridad de la Información relacionada con los Recursos Humanos

7.2.1. Antes del empleo

La JGRH, en el marco de sus funciones y conforme a lo definido en sus documentos internos de gestión o normativa vigente en la materia, debe:

a) Asegurar que todos los servidores civiles cumplan con los requisitos necesarios para el desempeño de las funciones que se le sean asignadas, así como entiendan sus responsabilidades.
b) Durante el proceso de selección, comprobar los antecedentes del personal que ingresa a laborar en la entidad, de acuerdo con las leyes y regulaciones vigentes, independientemente de su modalidad de contrato con la entidad.

c) Al inicio del vínculo laboral, entregar al nuevo servidor civil un ejemplar de la política y objetivos de seguridad de la información, dejando evidencia de su recepción.
d) Asimismo, gestionar la suscripción por parte del servidor civil de una declaración jurada referida al cumplimiento de la política, directiva y demás lineamientos establecidos de seguridad de la información; así como de un acuerdo de confidencialidad y no divulgación de la información a la cual tendrá acceso en el ejercicio de sus funciones.

7.2.2. Durante el empleo

La JGRH, conforme con lo definido en sus documentos internos de gestión o normativa vigente en la materia, debe garantizar que todos los servidores civiles conozcan y entiendan sus responsabilidades en seguridad de la información. Para ello, debe:

a) Planificar y asegurar la ejecución de actividades de inducción y capacitación en materia de seguridad de la información en coordinación con JTI, así como la participación de los servidores civiles en las mismas; a fin de lograr un nivel de concientización y conocimiento de las funciones y responsabilidades que desempeñe el servidor acorde con los objetivos de seguridad de la información.
b) Ante algún incumplimiento de la directiva, procedimiento o lineamiento relacionado a la seguridad de la información en concordancia con el Reglamento Interno de Servidores Civiles del Ositrán, poner en conocimiento del órgano competente para que se evalúe el inicio de un procedimiento administrativo disciplinario.

7.2.3. Término del empleo o cambio de puesto de trabajo

a) La JGRH debe proteger los intereses de la entidad como parte del proceso de cambio o finalización del vínculo laboral.
b) Cuando el servidor civil cambie de puesto de trabajo o se dé el término del vínculo laboral con la entidad, debe poner a disposición del titular de la unidad de organización o a quien este designe, todos los activos de información que correspondan y/o documentos (físicos y digitales) que representen valor para los procesos y funciones de la entidad, que fueron generados durante su vínculo laboral en el marco del desempeño de sus funciones.
c) La JTI procederá a actualizar, deshabilitar o remover todas las credenciales y los accesos del servidor civil a los recursos de información, la red de datos, servicios tecnológicos y los sistemas de la entidad, una vez que haya tomado conocimiento formal del cambio o desvinculación correspondiente.
d) La JTI procederá con el backup y resguardo de la información contenida en el equipo de cómputo asignado al servidor civil, una vez que haya tomado conocimiento del cambio o desvinculación correspondiente. Dicha información podrá ser entregada al titular de la unidad de organización, de solicitarlo.
e) En caso de producirse un cambio de puesto de trabajo, el titular del órgano correspondiente debe solicitar a la JTI mediante el formulario respectivo, la actualización de los accesos a los servicios tecnológicos del servidor civil según el perfil del nuevo puesto de trabajo.

7.3. Seguridad de la Información en la Gestión de Activos

7.3.1 Responsabilidad por los activos

a) El OSI debe gestionar la identificación de los activos de información de la entidad y de su correspondiente propietario, de acuerdo con lo establecido en los roles y responsabilidades de la presente directiva.
b) El OSI es responsable de mantener actualizado el inventario de activos de información bajo al alcance del SGSI.
c) El propietario del activo, en coordinación con el OSI, debe revisar periódicamente las restricciones de acceso y las clasificaciones de activos importantes, teniendo en cuenta las políticas aplicables.
d) De la misma manera, el propietario de los activos de información debe velar por el tratamiento adecuado de los mismos, garantizando la protección de la información cuando el activo es eliminado o destruido.

7.3.2 Clasificación de la información

a) El OSI debe garantizar que la información reciba un nivel adecuado de protección de acuerdo con su naturaleza.
b) El propietario de los activos de información debe clasificar los mismos según su naturaleza durante el proceso de identificación de activos.
c) Toda información debe ser clasificada según las siguientes categorías:
    - **Confidencial:** Información que no debe estar disponible o no debe ser divulgada a personas, entidades o procesos de negocio no autorizados. Esta definición se sujeta a los supuestos establecidos en el artículo 17 del Texto Único Ordenado de la Ley N° 27806, Ley de Transparencia y Acceso a la Información Pública, aprobado por Decreto Supremo N° 021-2019-JUS, o norma que los modifique, complemente o sustituya.
    - **Uso interno:** la revelación de esta información no causaría daños serios a la entidad, y su acceso es libre para los colaboradores de la entidad a través de los sistemas, aplicativos, portales o cualquier medio de almacenamiento o publicación, y cuyo acceso excepcional por parte de personal externo (auditores, entidades reguladoras, consultores externos) puede darse, pero se encuentra regulado y sujeto a condiciones específicas de acceso.
    - **Pública:** Esta información ha sido definida por la entidad para conocimiento público como son los boletines de noticias, comunicados, informes de prensa, memoria institucional, pronunciamientos, entre otros.
d) Cuando se estime que la naturaleza de una información ha cambiado, el propietario del activo de información debe revisar su clasificación, modificar de corresponder e informar al OSI.
e) En el caso de documentos físicos y digitales que hayan sido clasificados como “confidenciales”, el etiquetado y su tratamiento debe realizarse según lo dispuesto en la Directiva de Gestión Documental o documentos relacionados.
f) Los activos de información de carácter formal relacionados con los documentos internos y externos deben ser tratados de acuerdo a la Directiva de Gestión Documental o documentos relacionados.

7.3.3 Manejo de los medios

a) El OSI debe procurar la implementación de mecanismos que eviten la revelación, modificación, eliminación o destrucción no autorizada de la información almacenada en medios de soportes removibles.

b) Solo estará permitido el uso de medios removibles de tipo memoria USB o discos duros externos que sean de propiedad de la entidad.
c) La JTI asignará los medios removibles a aquellos servidores civiles que hayan sido autorizados por el titular de la unidad de organización correspondiente.
d) El resguardo del medio removible, su traslado seguro, así como la información almacenada en el mismo, es responsabilidad exclusiva del servidor civil asignado.
e) Una vez culminada la temporalidad y necesidad de uso del medio removible, este deberá ser devuelto a la JTI, quien procederá a la eliminación definitiva de su contenido.

7.4. Seguridad de la Información para el Control de Accesos

La JTI debe establecer lineamientos y medidas de seguridad apropiadas para el control de acceso en la entidad.

7.4.1 Requisitos para el control de acceso

a) La JTI debe limitar el acceso a los recursos y servicios de consulta, manejo y procesamiento de información y activos de información.
b) La JTI debe establecer, documentar y revisar lineamientos de control de accesos basada en los requisitos de negocio y de seguridad de la información.
c) El control de acceso a los activos de información, sistemas, red de datos y servicios tecnológicos debe realizarse por medio de cuentas de usuario y contraseñas únicas para cada colaborador.
d) La JTI debe establecer parámetros para el uso de contraseñas robustas para el acceso a los activos de información y servicios tecnológicos. Asimismo, establecerá parámetros para el vencimiento periódico de las contraseñas.
e) La JTI debe mantener un registro actualizado de los niveles de accesos a la red de datos, sistemas y servicios tecnológicos, considerando los perfiles establecidos para los colaboradores.
f) Los accesos deben ser solicitados por el titular de la unidad de organización y aprobados por los propietarios de los activos de información. Los usuarios solo podrán acceder a los recursos de información que han sido autorizados.

7.4.2 Gestión de accesos de usuarios

La JTI debe garantizar el acceso de usuarios autorizados y evitar el acceso no autorizado a la red de datos, los sistemas y servicios tecnológicos. Para ello, debe:

a) Establecer procedimientos para el control de accesos:
   - De alta y baja de usuarios basado en las autorizaciones correspondientes y generando los registros necesarios.
   - De asignación o revocación de accesos a la red de datos, sistemas y servicios tecnológicos, basado en las autorizaciones correspondientes y generando los registros necesarios.
   - De asignación o revocación de accesos privilegiados a la red de datos, sistemas y servicios tecnológicos, basado en las autorizaciones correspondientes y generando los registros necesarios.
b) Mantener un registro del colaborador que cumple el rol de administrador con accesos privilegiados a los sistemas y/o aplicativos, así como de los servicios tecnológicos.
c) Revisar periódicamente que los accesos de las cuentas de usuario de los colaboradores desvinculados hayan sido deshabilitados.

d) Revisar periódicamente que los accesos concedidos a los usuarios sean los que le corresponden a lo autorizado y según los lineamientos de control de accesos establecidos.
e) Actualizar, deshabilitar o remover todas las credenciales y los accesos del colaborador a los recursos de información, la red de datos, servicios tecnológicos y los sistemas de la entidad, una vez que haya tomado conocimiento del cambio o desvinculación correspondiente.
f) Asimismo, puede reiniciar las contraseñas en los sistemas de información y/o servicios tecnológicos únicamente a solicitud del usuario.

Los usuarios deben considerar que los accesos que superen tres (3) intentos fallidos generan automáticamente el bloqueo de la cuenta de usuario.

7.4.3 Responsabilidades del usuario respecto a la gestión de accesos

a) Los usuarios son responsables de proteger su información de autenticación.
b) Las cuentas de usuario y contraseñas son de uso exclusivo del colaborador y no deben ser compartidas. Está prohibido el acceso a la red de datos, sistemas y servicios tecnológicos con la cuenta de usuario de otro colaborador.
c) El usuario debe establecer contraseñas robustas que brinden un adecuado nivel de seguridad, cumpliendo con los parámetros establecidos en los lineamientos de control de acceso.
d) Es responsabilidad del usuario mantener la confidencialidad de su credencial de acceso (usuario y contraseña), debiendo hacer uso adecuado de la misma y asumir la responsabilidad por las actividades realizadas desde dicha cuenta.
e) Es responsabilidad del usuario mantener actualizadas sus contraseñas conforme a la periodicidad establecida en los lineamientos de control de acceso.
f) Es responsabilidad del usuario cerrar la sesión activa en la computadora o emplear el mecanismo de bloqueo de pantalla, cuando finalice sus actividades o cuando ya no esté en uso del equipo.
g) Todo usuario que identifique cualquier indicio de que su contraseña de autenticación se encuentre vulnerada, deberá proceder al cambio inmediato de contraseña e informar a la mesa de ayuda de la JTI.

7.4.4 Control de acceso a sistemas y aplicaciones

a) La JTI debe prevenir el acceso no autorizado a los sistemas y aplicaciones.
b) Los accesos deben ser solicitados por el titular de la unidad de organización y aprobados por los propietarios de los activos de información.
c) Los usuarios solo podrán acceder a las aplicaciones y sistemas que han sido autorizados según los lineamientos de control de acceso.
d) La JTI debe establecer mecanismos y procedimientos seguros de inicio de sesión a los sistemas y aplicaciones de acuerdo con los lineamientos de control de acceso.
e) La JTI debe restringir y controlar rigurosamente el uso de programas utilitarios privilegiados que puedan ser capaces de invalidar los controles del sistema y de la aplicación.
f) El acceso a los repositorios que contengan código fuente de las aplicaciones y software de la entidad debe ser controlado únicamente por personal de la JTI autorizado.

7.5. Seguridad de la Información para la Criptografía

La JTI debe garantizar un uso adecuado y eficaz de la criptografía para proteger la confidencialidad, autenticidad y/o integridad de la información de la entidad. Para ello, debe:

a) Implementar controles criptográficos en función al análisis y evaluación de los riesgos de seguridad de la información.
b) Definir métodos criptográficos que permitan una conexión segura, en el caso que los sistemas de información requieran autenticación de los usuarios.
c) Gestionar las acciones pertinentes ante los entes correspondientes para la revocación y/o cancelación de las claves criptográficas y/o certificados, en el caso que estos hayan sido comprometidos o simplemente dejaron de usarse.
d) Gestionar y/o inhabilitar la clave criptográfica en coordinación con el Oficial de Seguridad de la Información, ante el cese del personal o cambio de rol en algún sistema de información, guardando evidencia del proceso de destrucción.

7.6. Seguridad física y ambiental

7.6.1 Seguridad de la información en áreas seguras

a) El OSI debe evaluar los riesgos asociados al acceso físico no autorizado a las áreas seguras y proponer mecanismos y controles.
b) El OSI, en coordinación con la JLCP e instancias pertinentes, debe implementar los mecanismos de control para prevenir el acceso físico no autorizado a las áreas seguras y a los recursos de tratamiento de la información.
c) El OSI debe identificar cómo áreas seguras al centro de datos de la entidad y a todos aquellos espacios que contienen información sensible o crítica.
d) El OSI, en coordinación con los responsables de las áreas seguras y la JLCP, debe implementar mecanismos físicos y/o lógicos para proteger y prevenir daños por causales externas o ambientales en las áreas identificadas como seguras.
e) El acceso a las diferentes áreas seguras del Ositrán debe estar manejado a través de mecanismos de control de acceso y de la asignación de las autorizaciones de ingreso correspondientes, supervisadas por los responsables de las áreas seguras o instancias correspondientes.
f) Cualquier personal externo sólo tendrá acceso al centro de datos de la entidad para fines específicos y debe ser autorizado por el responsable del centro de datos.
g) Todo ingreso que se efectúe por parte de personal externo o visitantes a las áreas identificadas como seguras, debe ser registrada en el formato correspondiente (bitácora) por parte del responsable del área segura. Durante dicho periodo, el personal externo que no pertenece a la entidad debe portar el pase otorgado de manera visible y ser acompañado por un responsable encargado.
h) Los responsables de las áreas seguras deben evitar el trabajo no supervisado de proveedores en dichas áreas.
i) Los responsables de las áreas seguras deben controlar el ingreso de computadoras portátiles, equipos fotográficos, de video, audio o cualquier otro tipo de equipamiento que registre información, salvo previa autorización formal por correo electrónico o documento.

7.6.2 Seguridad en los equipos informáticos

El OSI debe prevenir la pérdida, daño, robo o el compromiso de los activos y la interrupción de las operaciones de la entidad.

La JTI debe:

a) Asegurar que los equipos informáticos estén ubicados en lugares con las condiciones técnicas adecuadas, con el fin de prevenir daños ante posibles riesgos del ambiente.
b) Procurar que los equipos informáticos, comunicaciones y de seguridad perimetral, sean protegidos contra daños por anomalías del servicio de fluido eléctrico.
c) Procurar que el cableado eléctrico y de red de datos se encuentren ordenados, etiquetados, separados y protegidos de acuerdo a las buenas prácticas de la industria.
d) Realizar o gestionar el mantenimiento preventivo y/o correctivo a los equipos informáticos de los usuarios y a la infraestructura tecnológica de la entidad.
e) Garantizar que los medios de almacenamiento que van a ser reutilizados, reemplazados o dados de baja, no contengan información institucional o software con copia registrada.
f) Asegurar que todo traslado de un equipo fuera de las instalaciones de la entidad sea autorizado y se realice con las debidas precauciones para su protección contra posibles daños y robos.
g) Velar que todo equipo desplazado para el trabajo remoto o teletrabajo cuente con la autorización de la Gerencia de Administración y se debe garantizar que su ubicación final cuente con las condiciones técnicas adecuadas.
h) Adoptar una política de escritorio limpio y pantalla limpia en los equipos de la red de datos de la entidad.

Los usuarios deben:

a) Asegurar que el equipo desatendido tenga la protección adecuada, evitando el acceso no autorizado en ausencia del usuario.
b) En ausencia del usuario, evitar dejar papeles de trabajo expuestos sobre el escritorio. Asimismo, guardar preferiblemente en mobiliario bajo llave los medios de almacenamiento que contengan información confidencial de la entidad.
c) Evitar dejar en fotocopiadoras o impresoras documentos con información clasificada como confidencial. Asimismo, evitar el uso de papel que contenga información confidencial como papel reciclado.
d) Eliminar de manera segura la información impresa confidencial a fin de que no sea posible su reconstrucción total o parcial.
e) Cuando el usuario se ausente de su puesto de trabajo debe quitar toda la información sensible de la pantalla del equipo de cómputo, bloqueando, cerrando sesión o apagando el equipo de cómputo.

7.7. Seguridad de la Información en las operaciones

7.7.1 Procedimiento y responsabilidades operativas

La JTI debe garantizar el funcionamiento correcto y seguro de las instalaciones de tratamiento de la información. Para ello, debe:

a) Elaborar y mantener actualizados los documentos de los procesos relacionados con la gestión de los sistemas de información, gestión de la infraestructura tecnológica.
b) Mantener un control de los cambios que se efectúan a los sistemas de información, aplicaciones o infraestructura tecnológica de la entidad.

c) Monitorear el uso de los recursos informáticos y prever necesidades futuras de capacidad, a fin de garantizar la disponibilidad y continuidad de los servicios de la entidad.
d) Separar los recursos de desarrollo, pruebas y operación, para reducir los riesgos de acceso no autorizado o los cambios del sistema en producción.

7.7.2 Protección contra código malicioso

a) La JTI debe garantizar que los recursos y servicios de consulta, manejo y procesamiento de información y la información están protegidos contra el malware.
b) La JTI debe asegurar que todos los equipos que se asignen a los usuarios del Ositrán cuenten con software contra códigos maliciosos.

7.7.3 Respaldo de información

La JTI debe evitar la pérdida de datos. Para ello, debe:

a) Identificar los sistemas de información, servicios informáticos y la información que sean considerados críticos para la continuidad de las operaciones, con el fin de programar la ejecución, pruebas y restauración de las copias de respaldo.
b) Mantener registros exactos y completos de las copias de respaldo y de las pruebas de restauración.
c) Respaldar la información que se encuentre almacenada en los servidores del Ositrán de acuerdo con la programación de copias de respaldo establecida.
d) Realizar la ejecución de pruebas de restauración de la información relevante, con el fin de asegurar la integridad de los respaldos de información existentes.
e) Almacenar los medios que contienen las copias de respaldo en una localización remota con los niveles de protección apropiados y las condiciones físicas y ambientales de seguridad adecuadas.
f) Efectuar a solicitud del usuario, las copias de respaldo de la información almacenada en sus equipos informáticos o las restauraciones requeridas.

7.7.4 Registros y monitoreo

La JTI debe registrar eventos y generar evidencias. En ese sentido debe:

a) Monitorear los sistemas de información y/o servicios informáticos que se encuentran en producción a través del personal responsable de su administración y/o servicios especializados tercerizados.
b) Almacenar y custodiar la información del registro de eventos con las medidas de seguridad que permitan garantizar su confidencialidad, integridad, disponibilidad y trazabilidad.
c) Sincronizar los sistemas de información, los servicios informáticos y de comunicaciones con una fuente de referencia y de tiempo exactos con la hora oficial nacional.

7.7.5 Control del software de operación

La JTI debe garantizar la integridad del software operacional. Para ello, debe:

a) Implementar procedimientos para controlar la instalación del software de operación.
b) Mantener un registro de la instalación y/o desinstalación de los softwares en los sistemas operacionales.

7.7.6 Gestión de vulnerabilidades técnicas

La JTI debe mitigar los riesgos resultantes de la explotación de las vulnerabilidades técnicas. Para ello, debe:

a) Realizar el análisis de vulnerabilidades de los sistemas de información y aplicativos durante y previo a su pase a producción.
b) Evaluar periódicamente la identificación de nuevas vulnerabilidades en los sistemas de información, aplicativos o plataformas tecnológicas que se encuentren en producción.
c) Implementar las acciones correspondientes para mitigar los riesgos asociados a las vulnerabilidades identificadas.
d) Asimismo, la instalación de software en los sistemas operacionales se encuentra restringida y puede ser únicamente ejecutada por personal de la JTI, debiendo los usuarios solicitar a dicha jefatura los softwares que requieran para el cumplimiento de sus funciones.

7.7.7 Auditoría de los sistemas de información

El OSI debe planificar las actividades de auditoría en los sistemas operativos para minimizar el riesgo de las interrupciones a los procesos del negocio.

7.8. Seguridad de la Información en las Comunicaciones

7.8.1. Gestión de la seguridad de la red

La JTI debe garantizar la protección de la información en las redes, los recursos y servicios de consulta, manejo y procesamiento de información. Para ello, debe:

a) Otorgar accesos a la red de datos a los usuarios que hayan sido debidamente autorizados por el titular de la unidad de organización correspondiente.
b) Asegurar la adecuada segregación de la responsabilidad operacional de las redes y de los sistemas informáticos.
c) Asegurar que se utilicen aplicaciones con protocolos seguros para la administración de los equipos de comunicaciones de la red cambiando las configuraciones por defecto.
d) Implementar sobre la red de datos de la entidad equipos de seguridad perimetral que permitan responder ante posibles ataques internos y externos de la red.
e) Asegurar que los identificadores de las redes inalámbricas del Ositrán no divulguen información relacionada con la entidad o alguna de sus unidades de organización.
f) Mantener el registro de eventos y monitorización para lograr el registro y detección de acciones que podrían afectar la seguridad de la información.
g) Definir los mecanismos de seguridad, los niveles de servicio, y los requisitos de gestión de todos los servicios de red, los que se deben incluir en las condiciones de servicios, tanto si estos servicios se prestan dentro de la entidad como si se subcontratan.
h) Establecer segregación de redes para los segmentos de usuarios, de servidores, de acceso público (zona desmilitarizada) como mínimo.

7.8.2. Transferencia de información

La JTI debe mantener la seguridad en la información que se transfiere dentro de la entidad y con cualquier organización externa. Para ello debe:

a) Establecer lineamientos, procedimientos y/o controles formales que protejan el intercambio de información.
b) Velar por la implementación de mecanismos de seguridad de la información en los canales digitales o mensajería electrónica que se implementen para el intercambio de información entre el Ositrán y otras entidades, así como con usuarios externos.

7.9. Seguridad de la Información para la adquisición, desarrollo y mantenimiento de Sistemas de Información

7.9.1. Requisitos de seguridad de los sistemas de información

La JTI debe asegurar que la seguridad de la información sea parte integral de los sistemas de información a través de todo el ciclo de vida. Esto también incluye los requisitos para dichos sistemas que proporcionan los servicios a través de redes públicas. Para ello, debe:

a) Definir y documentar los requerimientos de seguridad previamente al desarrollo, adecuación o adquisición de los sistemas de información y/o aplicativos de la entidad.
b) Garantizar la confidencialidad, integridad y disponibilidad de la información que se procesa y/o transmite en los sistemas de información y/o aplicativos del Ositrán, mediante el cifrado de los canales de transmisión correspondientes.

7.9.2. Seguridad en el proceso de desarrollo y soporte de los sistemas de información y software

La JTI debe garantizar la seguridad de la información que se ha diseñado e implementado en el ciclo de vida de desarrollo de sistemas de información. Para ello, debe:

a) Establecer lineamientos para el desarrollo seguro de aplicaciones y sistemas, aplicables tanto al desarrollo interno y tercerizado.
b) Ejecutar pruebas de aceptación, así como de aseguramiento de calidad y seguridad informática, de manera previa al pase de producción de todo sistema de información o aplicativo de la entidad.
c) Aplicar buenas prácticas o recomendaciones internacionales en materia de desarrollo seguro durante el ciclo de vida de los sistemas de información y/o aplicativos.
d) Establecer un procedimiento para el control de los cambios en el desarrollo y/o mantenimiento de sistemas de información y/o aplicaciones, dentro del ciclo de vida del software.
e) Contar con ambientes de desarrollo seguro para las actividades de desarrollo e integración de sistemas de información y/o aplicaciones a realizarse en la entidad.
f) Supervisar y monitorear en el caso de tercerización de las actividades de desarrollo de sistemas de información y/o aplicativos, que cumplan con los lineamientos establecidos de desarrollo seguro.

7.10. Seguridad de la Información para Proveedores

7.10.1 Seguridad de la información en las relaciones con los proveedores

a) La política o lineamientos de seguridad de la información con proveedores deben ser definidos y documentado por el OSI en coordinación con la JLCP para su comunicación.
b) La unidad de organización responsable del servicio a contratar debe incluir en los documentos de la contratación cláusulas de confidencialidad respecto de la información que va a ser intercambiada con el proveedor en el marco del servicio y/o cadena de suministro.
c) La JLCP debe hacer de conocimiento del proveedor la política o lineamientos de seguridad de la información con proveedores que se encuentre vigente.
d) Los titulares de las unidades de organización responsables de la gestión de los servicios del proveedor deben de coordinar con las unidades de organización competentes los niveles de acceso físicos y lógicos que el proveedor requiere para el cumplimiento de su servicio.
e) Los titulares de las unidades de organización responsables de los servicios deben asegurar la protección de los activos de la entidad que sean accesibles a los proveedores.
f) La unidad de organización responsable del servicio debe supervisar que la información y los recursos que la entidad le proporcione al proveedor, sean utilizados únicamente para cumplir con las actividades del servicio en cuestión.

7.10.2 Gestión de entrega de servicios de proveedor

a) La unidad de organización responsable del servicio realizará la supervisión y la revisión del mismo, con el fin de asegurar que los términos y las condiciones de seguridad de la información de las cláusulas contractuales se están cumpliendo.
b) En el caso de que se realicen cambios en el equipo de trabajo del proveedor de un servicio contratado, la unidad de organización responsable del servicio deberá gestionar ante las unidades de organización correspondientes las medidas pertinentes respecto de los accesos físicos y lógicos.

7.11. Gestión de incidentes de Seguridad de la información

a) La JTI debe garantizar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación de eventos de seguridad y debilidades.
b) La JTI debe disponer las responsabilidades y método de gestión para garantizar una respuesta rápida, efectiva y adecuada a los incidentes de seguridad de la información.
c) Los colaboradores deben de reportar a través de los canales establecidos para este fin; todo tipo de eventos, incidentes, debilidades y vulnerabilidades relacionados con la seguridad de la información y seguridad digital.
d) La JTI debe evaluar periódicamente los eventos reportados mediante los canales pertinentes para determinar si corresponde su clasificación como incidentes de seguridad de la información y darle el tratamiento adecuado, según el procedimiento vigente.
e) La JTI debe mantener una bitácora donde se registrarán y analizarán los eventos e incidentes de seguridad de la información.
f) Responder a los incidentes de seguridad de la información de acuerdo con los métodos establecidos.

g) El OSI, en coordinación con los especialistas de la JTI, debe evaluar la eficacia de los controles implementados como respuesta a incidentes de seguridad de la información ocurridos, a fin de reducir la probabilidad de recurrencia y sus impactos.
h) Ante la ocurrencia de un incidente de seguridad de la información que pudiera tener un impacto legal, se debe de identificar y preservar la información que pueda servir como evidencia.

7.12. Seguridad de la información en la gestión de la continuidad del negocio

7.12.1. Continuidad de seguridad de la información

En el Ositrán la continuidad de la seguridad de la información debe formar parte de los requisitos para mantener la continuidad de negocio de la entidad. Para ello:

a) El OSI, en coordinación con las unidades de organización, debe establecer los requisitos de seguridad de la información y de continuidad de gestión de seguridad de la información en situaciones adversas.
b) La JTI, en coordinación con el OSI, debe asegurar la implementación de los mecanismos y controles que permitan garantizar los requisitos de seguridad de la información establecidos durante situaciones adversas.
c) El OSI debe de verificar los controles implementados como parte de mejora continua por lo menos una vez al año o cuando se requiera comprobando su validez y eficacia durante situaciones adversas.

7.12.2. Redundancias

La JTI debe asegurar la disponibilidad de los recursos y servicios de consulta, manejo y procesamiento de información.

Para ello, debe procurar contar con infraestructura tecnológica redundante y ambientes alternos que contribuyan a garantizar la continuidad de los sistemas y servicios de tecnologías de información críticos de la entidad.

7.13. Cumplimiento en materia de seguridad de la información

7.13.1. Cumplimiento de requisitos legales y contractuales

El OSI debe velar por el cumplimiento de las obligaciones legales, estatutarias, reglamentarias o contractuales relativas a la seguridad de la información o de los requisitos de seguridad.

a) El OSI debe identificar, implementar y mantener en el alcance del SGSI las disposiciones normativas legales, regulatorias y contractuales relevantes relacionadas con seguridad de la información.
b) El OSI debe desarrollar actividades propias para garantizar el cumplimiento de los requisitos legales, regulatorios y contractuales sobre el uso de materiales, con respecto a los cuales puedan existir derechos de propiedad intelectual y sobre el uso de productos de software patentados.
c) La JTI debe garantizar que toda adquisición de software que realice la entidad bajo licencia privativa (“copyright”) se debe realizar a través de proveedores autorizados. Asimismo, debe de mantenerse un registro y evidencias que sustenten su adquisición.

d) La JTI debe asegurar que los registros deben estar protegidos contra la pérdida, destrucción, falsificación, divulgación o acceso no autorizados de acuerdo con disposiciones legales, regulatorias, contractuales aplicables.
e) La JTI debe llevar un registro de licencias de software instaladas en sus equipos informáticos y llevar un adecuado control de su licenciamiento.
f) La JTI debe mantener vigentes los lineamientos orientados a la privacidad y protección de los datos personales que se gestionen dentro de la entidad.
g) La JTI debe mantener el control criptográfico utilizado de acuerdo con todos los contratos, leyes y regulaciones adecuadas.

7.13.2. Revisiones de seguridad de la información

El OSI debe garantizar que la seguridad de la información se implementa y opera de acuerdo con las políticas y procedimientos de la entidad. Para ello, debe:

a) Programar y realizar revisiones independientes y/o auditorías internas y/o externas, según corresponda de acuerdo con el procedimiento establecido.
b) Reportar y registrar los resultados de las revisiones y/o auditorías a los interesados para la atención de los hallazgos encontrados.
c) Comprobar periódicamente que los sistemas de información cumplan con las políticas y normas de seguridad de la información de la entidad.

VIII. Disposiciones complementarias

8.1. Los aspectos técnicos contemplados en el numeral 7. Disposiciones específicas serán implementados gradualmente en un plazo de 120 días desde la vigencia de la presente directiva. Dicho plazo aplica tanto para los lineamientos que deriven en acciones bajo el ámbito de competencias de las unidades de organización responsables, como para aquellos que demanden acciones de parte de los colaboradores para su cumplimiento.

8.2. Los aspectos no contemplados en la presente directiva serán resueltos por la Jefatura de Tecnologías de la Información.

IX. Responsabilidades

9.1. La Jefatura de Tecnologías de la Información es la responsable de verificar la implementación y/o cumplimiento de los lineamientos establecidos en el presente documento.

9.2. El Oficial de Seguridad de la Información es el responsable de realizar el seguimiento al cumplimiento y/o implementación de los lineamientos establecidos en el presente documento.

X. Cuadro de Control de Cambios

Versión	:	01
Elaborado por	:	**César Talledo León** Jefe de Tecnologías de la Información
Revisado por	:	**Víctor Hugo La Rosa Rosado** Gerente de Planeamiento y Presupuesto
		Humberto Sheput Stucchi Gerente de Asesoría Jurídica
Aprobado por	:	**Juan Carlos Mejía Cornejo** Gerente General
Control de Cambios	:	Ninguno por ser primera versión