RESOLUCIÓN DE GERENCIA GENERAL

N° 00004-2025-GG-OSITRAN

Lima, 8 de enero de 2025

VISTOS:

El Informe N° 00618-2024-JTI-GA-OSITRAN y Memorando N° 00003-2025-JTI-GA-OSITRAN elaborados por la Jefatura de Tecnologías de la Información de la Gerencia de Administración; el Informe N° 00116-2024-GPP-OSITRAN de la Gerencia de Planeamiento y Presupuesto; el Informe Nº 00004-2025-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 Legislativo N° 1412 de fecha 12 de setiembre de 2018, se aprueba la Ley de Gobierno Digital, documento que establece el marco para la gestión del gobierno y transformación digital de las entidades públicas, en cuyo literal d) del artículo 32, se señala que "Las entidades de la Administración Pública deben establecer, mantener y documentar un Sistema de Gestión de la Seguridad de la Información (SGSI)";

Que, mediante Resolución de Presidencia N° 042-2019-PD-OSITRAN de fecha 11 de setiembre de 2019, la Presidenta del Consejo Directivo aprueba la Política y Objetivos de Seguridad de la Información del Ositrán;

Que, mediante Resolución de Gerencia General N° 074-2021-GG-OSITRAN de fecha 13 de julio de 2021, se aprueba la Directiva de Seguridad de la Información del Ositrán, con el objeto de establecer lineamientos para la gestión y operación de la seguridad de la información en la entidad;

Que, mediante Resolución de Secretaría de Gobierno y Transformación Digital N° 002-2023-PCM/SGTD de fecha 08 de setiembre de 2023, se aprueba la Directiva N° 001-2023-PCM/ SGTD, Directiva que establece el perfil y responsabilidades del Oficial de Seguridad y Confianza Digital;

Que, a través de la Resolución de Secretaría de Gobierno y Transformación Digital N° 003-2023-PCM/SGTD de fecha 08 de setiembre de 2023, se establece la implementación y mantenimiento del Sistema de Gestión de Seguridad de la Información en las entidades públicas;

Que, mediante Resolución de Gerencia General N° 004-2024-GG-OSITRAN de 17 de enero de 2024, se aprueba la "Directiva de Seguridad de la Información del Ositrán" – versión 02, con el objeto de dar cumplimiento a las disposiciones establecidas en el marco normativo en materia de seguridad de la información, así como de efectuar precisiones y mejoras a los lineamientos establecidos para asegurar la vigencia de los mismos y su adecuación con los procesos institucionales vinculados;

Que, a través del Informe N° 00618-2024-JTI-GA-OSITRAN de 16 de diciembre de 2024, complementado con el Memorando N° 00003-2025-JTI-GA-OSITRAN de 2 de enero de 2025, la Jefatura de Tecnologías de la Información plantea y sustenta la necesidad de actualizar la "Directiva de Seguridad de la Información del Ositrán" a la versión 03, con el objeto de guardar alineamiento con el marco normativo vigente en materia de seguridad de la información y gobierno digital, así como facilitar el proceso de transición del SGSI implementado en la entidad

hacia la versión vigente de la norma NTP ISO/IEC 27001:2022 aprobada por el Instituto Nacional de la Calidad mediante Resolución Directoral N° 022-2022-INACAL/DN;

Que, con Informe N° 00116-2024-GPP-OSITRAN, la Gerencia de Planeamiento y Presupuesto, ha emitido 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 y aprobación de instrumentos de gestión interna del Ositrán y que la Jefatura de Tecnologías de la Información es la unidad de organización competente para formular dicha propuesta;

Que, la Gerencia de Asesoría Jurídica, a través del Informe N° 00004-2025-GAJ-OSITRAN, ha emitido opinión, indicando que encuentra jurídicamente viable la propuesta de actualización de la "Directiva de Seguridad de la Información del Ositrán" - versión 03;

Que, en mérito a lo establecido en los artículos 10° y 11° del Reglamento de Organización y Funciones del Ositrán, 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 los órganos del Ositrán;

Que, de conformidad con lo dispuesto en la Ley de Gobierno Digital aprobada mediante Decreto Legislativo N° 1412; la Resolución de Secretaría de Gobierno y Transformación Digital N° 003-2023-PCM/SGTD, el Reglamento de Organización y Funciones del Ositrán, aprobado por Decreto Supremo N° 012-2015-PCM y modificatorias; y la Directiva para la Formulación y Aprobación de Instrumentos de Gestión Interna del Ositrán, aprobada por Resolución de Gerencia General Nº 175-2019-GG-OSITRAN;

SE RESUELVE:

Artículo 1.- Aprobar la "Directiva de Seguridad de la Información del Ositrán" - versión 03, que como anexo forma parte de la presente resolución.

Artículo 2.- Dejar sin efecto la Resolución de Gerencia General N° 004-2024-GG-OSITRAN mediante la cual se aprobó la "Directiva de Seguridad de la Información del Ositrán" – versión 02.

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

Artículo 4.- Comunicar la presente resolución y la directiva señalada en el artículo 1 precedente a las gerencias y jefaturas del Ositrán, para conocimiento y fines.

Artículo 5.- Disponer que la Oficina de Comunicación Corporativa publique la presente Resolución en la intranet y su anexo en el Portal Institucional del Ositrán, ubicado en la Plataforma Digital Única del Estado Peruano para Orientación al Ciudadano (www.gob.pe/ositran).

Regístrese, comuníquese y publíquese.

Firmada por
JUAN CARLOS MEJÍA CORNEJO
Gerente General
Gerencia General

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

Visada por
AMÉRICO ABREU HIDALGO
Jefe de Tecnologías de la Información (e)
Jefatura de Tecnologías de la Información

Visado por:
THOU SU CHEN CHEN
Jefa de la Gerencia de Administración
Gerencia de Administración

Visada por:
RICARDO MERCADO TOLEDO
Jefe de la Gerencia de Planeamiento y Presupuesto
Gerencia de Planeamiento y Presupuesto

Visada por:
JAVIER CHOCANO PORTILLO
Jefe de la Gerencia de Asesoría Jurídica
Gerencia de Asesoría Jurídica

Visada por:
VLADIMIR FERNÁNDEZ CASTRO
Asesor en Gestión Administrativa
Gerencia General

NT 2025002692

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

	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 03
	Aprobado por Resolución N°	00004-2025-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° 033-2005-PCM, que aprueba el Reglamento de la Ley del Código de Ética de la Función Pública.
3.8. Decreto Supremo N° 052-2008-PCM, que aprueba el Reglamento de la Ley de Firmas y Certificados Digitales y sus modificatorias.
3.9. Decreto Supremo N° 012-2015-PCM, que aprueba el Reglamento de Organización y Funciones del Ositrán.
3.10. 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.
3.11. 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.
3.12. Decreto Supremo N° 075-2023-PCM, que modifica el Reglamento del Decreto Legislativo Nº 1412, Decreto Legislativo que aprueba la Ley de Gobierno Digital.
3.13. Decreto Supremo N° 007-2024-JUS, que aprueba el Reglamento de la Ley de Transparencia y Acceso a la Información Pública.
3.14. Decreto Supremo N° 016-2024-JUS, que aprueba el Reglamento de la Ley N° 29733, Ley de Protección de Datos Personales.
3.15. Resolución Ministerial N° 087-2019-PCM que aprueba disposiciones sobre la conformación y funciones del Comité de Gobierno Digital.
3.16. Resolución de Secretaría de Gobierno y Transformación Digital N° 002-2023-PCM/SGTD, que aprueba la Directiva N° 001-2023-PCM/ SGTD, Directiva que establece el perfil y responsabilidades del Oficial de Seguridad y Confianza Digital.
3.17. Resolución de Secretaría de Gobierno y Transformación Digital N° 003-2023-PCM/SGTD que establece la implementación y mantenimiento del Sistema de Gestión de Seguridad de la Información en las entidades públicas.

Las normas mencionadas en la base legal de la presente directiva incluyen sus disposiciones modificatorias, complementarias y conexas.

IV. Alcance

Las disposiciones contenidas en la presente directiva son de aplicación obligatoria para todo el personal del Ositrán, cualquiera fuere su régimen laboral o relación contractual.

V. Glosario de términos y acrónimos

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 brinda 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. **Área segura:** Espacio definido por la entidad, en el cual se procesa, almacena o transfiere información sensible y que contiene equipos informáticos críticos. Este espacio cuenta con barreras de seguridad física para proteger los activos de información de amenazas físicas.

5.6. **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.

5.7. **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.

5.8. **Colaborador:** Servidor civil perteneciente al régimen del D. Leg. 728, del D. Leg. 1057 y de la Ley N° 30057 o practicante de las unidades de organización del Ositrán.

5.9. **Comité de Gobierno y Transformación Digital:** 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. Entiéndase como equivalente la denominación de Comité de Gobierno Digital.

5.10. **Confianza digital:** Estado que emerge como resultado de cuán veraces, predecibles, éticas, proactivas, transparentes, seguras, inclusivas y confiables son las interacciones digitales que se generan entre personas, empresas, entidades públicas o cosas en el entorno digital, con el propósito de impulsar el desarrollo de la economía digital y la transformación digital. Es un componente de la transformación digital y tiene como ámbitos la protección de datos personales, la ética, la transparencia, la seguridad digital y la protección del consumidor en el entorno digital.

5.11. **Confidencialidad:** Propiedad por la cual la información no está disponible o no puede ser divulgada a personas, entidades o procesos de negocio no autorizados.
5.12. **Cuenta de Usuario:** Credenciales que se le otorga a un usuario para el acceso a la red de datos o computadora de la entidad.
5.13. **Custodio:** Colaborador de la entidad designado para administrar y hacer efectivos los controles de seguridad que el propietario del activo de información haya definido.
5.14. **Datos personales:** Toda información sobre una persona natural que la identifica o la hace identificable a través de medios que pueden ser razonablemente utilizados.
5.15. **Disponibilidad:** Propiedad de la información de estar accesible para el uso de las personas, entidades o procesos autorizados cuando lo requieran.
5.16. **Dispositivos móviles:** Teléfonos móviles o tablets que son asignados a los servidores civiles para el cumplimiento de sus funciones.
5.17. **Dispositivos de usuario:** Equipos terminales (equipos informáticos y dispositivos móviles) otorgados a los servidores civiles para el cumplimiento de sus funciones.
5.18. **Dueño del proceso:** Titular de la unidad de organización responsable del proceso.
5.19. **Evento de seguridad de la información:** Ocurrencia que podría comprometer la confidencialidad, integridad y disponibilidad de un activo de información y que aún no ha afectado la operación o procesos de la organización.
5.20. **Incidente de seguridad de la información:** Ocurrencia que ha comprometido la confidencialidad, integridad y/o disponibilidad de un activo de información, generando una afectación en las operaciones o procesos de la entidad.
5.21. **Integridad:** Propiedad de precisión y completitud de la información.
5.22. **Información:** Conjunto de datos que tiene valor para el Ositrán.
5.23. **Mesa de ayuda:** Servicio de atención y gestión de requerimientos e incidencias vinculadas con los equipos o recursos informáticos de la entidad.
5.24. **Oficial de Seguridad y Confianza Digital:** 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 dentro de la entidad. Entiéndase como equivalente la denominación de Oficial de Seguridad de la Información.
5.25. **Propietario del activo de información:** Responsable de controlar la producción, desarrollo, mantenimiento, uso y seguridad de los activos de información.
5.26. **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.
5.27. **Seguridad de la Información:** Preservación de la confidencialidad, integridad y disponibilidad de la información.
5.28. **Seguridad Informática:** Protección de las infraestructuras tecnológicas y de comunicaciones.
5.29. **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.
5.30. **Sesión:** Tiempo determinado de interacción del usuario con la computadora.
5.31. **Técnicas de seudonimización o anonimización:** Técnicas que se usan para proteger la privacidad de los datos personales de los usuarios. Su objetivo es ocultar los datos personales de los usuarios, para desconectar el vínculo entre la información y la identidad del propietario de la misma y así resguardar su identidad.
5.32. **Unidades de organización:** órganos, unidades orgánicas u oficinas establecidas en el ROF del Ositrán.
5.33. **Usuario:** Colaborador de la entidad o proveedor que por razones justificadas cuenta con acceso a la red de datos y que hace uso de servicios y recursos tecnológicos.

Asimismo, se precisan los siguientes acrónimos a ser mencionados en el presente documento:

5.34. **OSCD:** Oficial de Seguridad y Confianza Digital
5.35. **SGTD:** Secretaría de Gobierno y Transformación Digital
5.36. **SGSI**: Sistema de Gestión de Seguridad de la Información
5.37. **CNSD:** Centro Nacional de Seguridad Digital
5.38. **CSCD**: Coordinador de Seguridad y Confianza Digital

VI. Disposiciones Generales

6.1. Todos los usuarios del Ositrán deben cumplir las disposiciones, directrices y lineamientos de seguridad de la información establecidos en la presente directiva.
6.2. La información y los activos de información a la que los usuarios accedan, deben ser empleados exclusivamente para el cumplimiento de sus funciones y/o actividades.
6.3. Todos los usuarios 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 de la información 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. Ningún usuario de la entidad debe divulgar información declarada como confidencial y/o restringida de la Ositrán, a la cual haya accedido en el ejercicio de sus funciones.
6.13. Todo usuario 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.

6.14. El incumplimiento de las disposiciones de la presente directiva, de corresponder, podría ser pasible del ejercicio de la potestad sancionadora en materia disciplinaria de la entidad, conforme lo establecido en los artículos 44 [Sanciones] y 45 [Faltas] del Reglamento Interno de Servidores Civiles del Ositrán.

VII. Disposiciones Específicas

7.1. CONTROLES ORGANIZACIONALES

7.1.1. Roles y responsabilidades para la seguridad de la información

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 SGSI está compuesta por el Comité de Gobierno y Transformación Digital.

Comité de Gobierno y Transformación Digital (CGTD)

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 CGTD 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 y Confianza Digital (OSCD)
Conforme a lo dispuesto en la Directiva N° 001-2023-PCM/SGTD, Directiva que establece el perfil y responsabilidades del OSCD, el OSCD del Ositrán tiene las siguientes responsabilidades:

a) Coordinar la implementación, operación, mantenimiento y mejora continua del SGSI de la entidad, atendiendo las normas en materia de seguridad de la información, gestión de riesgos de seguridad de la información, gestión de incidentes de seguridad de la información, seguridad digital y confianza digital.
b) Coordinar con las unidades de organización de la entidad las acciones orientadas a implementar y/o mantener el SGSI, de acuerdo con lo establecido por la alta dirección y las normas en materia de seguridad de la información, gestión de riesgos de seguridad de la información, gestión de incidentes de seguridad de la información, seguridad digital y confianza digital.
c) Formular y proponer políticas, procedimientos y planes en materia de seguridad de la información, gestión de riesgos de seguridad de la información, gestión de incidentes de seguridad de la información, seguridad y confianza digital.
d) Promover la conformación y adecuada operación del equipo de respuestas ante incidentes de seguridad de la información.

e) Proponer medidas para la gestión de riesgos e incidentes de seguridad de la información, seguridad digital y ciberseguridad.
f) Crear y mantener un registro de los eventos e incidentes de seguridad de la información identificados.
g) Comunicar al CNSD los incidentes de seguridad digital críticos que afecten a los procesos misionales o servicios que brinda la entidad, y de ser el caso, coordinar y/o participar en su atención con el CNSD.
h) Planificar y coordinar la ejecución de pruebas de evaluación de vulnerabilidades de los aplicativos informáticos, sistemas, infraestructura, datos y redes que soportan los servicios digitales, procesos misionales o relevantes de la entidad.
i) Elaborar informes de los riesgos e incidentes de seguridad de la información críticos para la entidad pública e informarlos a la máxima autoridad administrativa.
j) Informar a la máxima autoridad administrativa acerca de los riesgos de seguridad de la información, incidentes de seguridad de la información críticos, avances y dificultades en la implementación u operación del SGSI, resultados de las auditorías de seguridad de la información internas y/o externas realizadas anualmente a la entidad, y sobre la aplicación efectiva de las normas en materia de seguridad de la información, gestión de riesgos de seguridad de la información, gestión de incidentes de seguridad de la información, seguridad digital y confianza digital.
k) Coordinar con el CNSD acciones de sensibilización y capacitación para los funcionarios y servidores civiles de la entidad sobre seguridad de la información, gestión de riesgos de seguridad de la información, gestión de incidentes de seguridad de la información, seguridad digital y confianza digital.
l) Coordinar con el Oficial de Gobierno de Datos y el Oficial de Datos Personales en todas las cuestiones relativas a la implementación de controles de seguridad de la información relacionados con las materias de gestión de datos y protección de datos personales en la entidad, respectivamente.
m) Coordinar con el Líder de Gobierno y Transformación Digital, lo concerniente a iniciativas y proyectos en materia de seguridad y confianza digital.
n) Coordinar con los dueños de procesos, propietarios de riesgos y responsables de las unidades de organización de la entidad su apoyo en la gestión de riesgos e implementación de los controles de seguridad de la información identificados en sus ámbitos de competencia, así como en la gestión de incidentes de seguridad de la información.
o) Liderar a los CSCD designados en la entidad pública para la adecuada implementación del SGSI.
p) Asegurar y supervisar la adopción y uso de estándares, normas técnicas y mejores prácticas de seguridad de la información ampliamente reconocidos por parte de la unidad de organización de tecnologías de la información cuando ésta adquiera, tercerice o desarrolle *software* o implemente otro tipo de soluciones tecnológicas.
q) Coordinar con la unidad de organización responsable de las tecnologías de la información o la que haga sus veces en la entidad, cuando corresponda, en los temas relativos a sus responsabilidades.
r) Otras responsabilidades afines que le sean asignadas por el titular de la entidad o la máxima autoridad administrativa.

Especialista de Seguridad de la Información y Ciberseguridad

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 equipos de trabajo a cargo de los proyectos o el personal de las 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) Brindar facilidades para las actividades periódicas de verificación del cumplimiento de las políticas y procedimientos de seguridad de la información en los procesos bajo el ámbito de sus competencias, a ser ejecutadas por el OSCD.
c) Comunicar requerimientos de control y protección de la información al OSCD 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 de seguridad de la información

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 oportuna.
c) Informar al OSCD respecto del nivel de implementación de las acciones de tratamiento de riesgos bajo su competencia.

Propietario de activos de información

a) Valorizar los activos de información bajo su competencia.
b) Definir la clasificación de la información bajo su competencia, con el propósito de garantizar su adecuado tratamiento conforme a su naturaleza.

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 debilidades, 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.

7.1.2. Segregación de funciones

El OSCD, 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.

7.1.3. Contacto con autoridades y grupos especiales de interés

a) El OSCD 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 OSCD 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.

7.1.4. Inteligencia de amenazas

a) La JTI debe establecer objetivos para la producción de inteligencia sobre amenazas a la seguridad de la información con la finalidad de generar la conciencia del entorno de amenazas y facilitar acciones de mitigación adecuadas.
b) La JTI debe establecer y ejecutar actividades para identificar y seleccionar fuentes de información internas y externas necesarias para la producción de inteligencia de amenazas, recopilar datos, procesarlos, analizar la información para comprender su significado y relevancia, y comunicar los resultados a las partes relevantes de manera comprensible.

7.1.5. 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 otros documentos normativos del SGSI, en cada uno de los proyectos que ejecuten en la entidad. Para ello, deben solicitar asistencia al OSCD para asegurar que los riesgos de seguridad de la información se identifican y se contemplan en el marco del proyecto.

7.1.6. Seguridad de la Información en la Gestión de Activos

7.1.6.1. **Inventario y uso aceptable de la información y activos asociados**

a) El OSCD debe gestionar la identificación de los activos de información de los procesos del alcance del SGSI y de su correspondiente propietario, de acuerdo con lo establecido en los roles y responsabilidades de la presente directiva.
b) El OSCD es responsable de mantener actualizado el inventario de activos de información de los procesos bajo al alcance del SGSI.
c) El OSCD es responsable de establecer las reglas para el uso aceptable de la información y otros activos asociados.
d) El propietario del activo, en coordinación con el OSCD, debe revisar periódicamente las restricciones de acceso y las clasificaciones de activos importantes, teniendo en cuenta las políticas aplicables.
e) 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 devuelto, eliminado o destruido.

7.1.6.2. **Clasificación y etiquetado de la información**

a) El propietario de los activos de información debe clasificar los mismos según su naturaleza durante el proceso de identificación de activos, con la asistencia del OSCD.
b) El propietario de cada activo debe asegurar que la información reciba un nivel adecuado de protección de acuerdo con su naturaleza y clasificación.
c) Todo activo de tipo información debe ser clasificado 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 y que se encuentre dentro de 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:** información que puede ser accesible únicamente 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.

- **Público:** Información que puede ser accesible o ser divulgada a todo el personal y público en general, sin reservas o consideraciones. Ej: boletines de noticias, comunicados, informes de prensa, memoria institucional, entre otros.

d) Cuando se estime que la naturaleza de un activo de tipo información ha cambiado, el propietario del activo de información debe revisar su clasificación, modificar de corresponder e informar al OSCD.
e) Todo documento generado en el marco de los actuaciones y procesos de la entidad, así como todo documento externo recibido mediante los canales establecidos, se constituye en un activo de tipo información y, por ende, debe ser clasificado para recibir el tratamiento adecuado conforme a su naturaleza.
f) Es responsabilidad de cada unidad de organización como propietaria del activo, la adecuada clasificación de los documentos emitidos o gestionados por la misma en el marco de sus competencias, a fin de garantizar su tratamiento adecuado y la preservación de su contenido.
g) La clasificación de los documentos deberá efectuarse tomando en cuenta lo dispuesto en el numeral c) del presente acápite, así como las disposiciones establecidas en la Directiva de Gestión Documental sobre seguridad y acceso de documentos.
h) El Comité de Gobierno Digital, en su calidad de responsable directivo del Modelo de Gestión Documental, debe aprobar los criterios para el control del acceso y seguridad de los documentos institucionales, teniendo como marco las definiciones de la presente directiva.
i) En el caso de documentos físicos y digitales el etiquetado y su tratamiento debe realizarse según lo dispuesto en la Directiva de Gestión Documental o documentos relacionados.

7.1.6.3. **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.

7.1.7. Seguridad de la Información para el Acceso, Identidades y Autenticación

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

7.1.7.1. **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 basados 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 usuarios solo podrán acceder a los recursos de información que han sido autorizados.

7.1.7.2. **Gestión de identidades**

La JTI debe garantizar la identificación única de los colaboradores y sistemas que accedan a la información de la entidad y otros activos asociados y permitir la asignación adecuada de los accesos. 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 autorizados 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.

7.1.7.3. **Responsabilidades del usuario respecto a la gestión de accesos y autenticación**

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.

7.1.7.4. **Derechos 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 y autorizados por el titular de la unidad de organización
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.

7.1.8. Seguridad de la Información para Proveedores

7.1.8.1. **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 documentados por el OSCD, 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 coordinar con las unidades de organización competentes los niveles y el periodo 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 de los servicios bajo el ámbito de sus competencias.
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 y durante el plazo establecido del servicio.

7.1.8.2. **Seguridad de la Información en la ejecución de los servicios del proveedor**

a) El OSCD debe definir acciones para gestionar riesgos de seguridad de la información en la cadena de suministros en tecnología de la información y comunicaciones.
b) La unidad de organización responsable del servicio realizará la supervisión y la revisión del servicio, con el fin de asegurar que los términos y las condiciones de seguridad de la información de las cláusulas contractuales se están cumpliendo.
c) 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.

7.1.9. Seguridad de la información para el uso de servicios en la nube

La JTI debe implementar y mantener medidas de seguridad para proteger la información almacenada, procesada o transmitida a través de servicios en la nube. Para ello debe:

a) Establecer los requisitos de seguridad de la información, los criterios de selección y el alcance del uso de servicios en la nube.
b) Determinar funciones y responsabilidades de los administradores, con relación al uso y gestión de servicios en la nube.
c) Gestionar los controles y capacidades de seguridad de los servicios en nube con el proveedor; como el monitoreo, la revisión y evaluación del uso de servicios en la nube.
d) Establecer acciones para la culminación de los servicios en la nube.

7.1.10. Gestión de incidentes de seguridad de la información

a) La JTI debe definir las responsabilidades y procedimientos para la gestión de incidentes de seguridad de la información, incluida la comunicación de eventos de seguridad y debilidades.
b) La JTI debe evaluar 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.
c) La JTI debe mantener una bitácora donde se registrarán y analizarán los eventos e incidentes de seguridad de la información, para aprender de los mismos.
d) La JTI debe responder a los incidentes de seguridad de la información de acuerdo con los métodos establecidos.
e) El OSCD, 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.
f) 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.
g) Los colaboradores deben reportar a través de los canales establecidos para este fin; todo tipo de eventos, incidentes y/o debilidades relacionadas con la seguridad de la información y seguridad digital.

7.1.11. Seguridad de la información durante una disrupción

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 OSCD, en coordinación con las unidades de organización, debe establecer los requisitos de seguridad de la información durante una disrupción.
b) La JTI, en coordinación con el OSCD, debe asegurar la implementación de los mecanismos y controles que permitan el cumplimiento de los requisitos de seguridad de la información establecidos durante una disrupción.
c) El OSCD 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 una disrupción.

7.1.12. Preparación de las TIC para la continuidad del negocio

La JTI debe establecer mecanismos para que la entidad pueda responder eficazmente ante interrupciones, mantener las actividades prioritarias y detectar anticipadamente incidentes que puedan afectar los servicios TIC. Para ello debe:

a) Planificar las acciones para la continuidad de las TIC considerando escenarios pre, durante y post interrupción.
b) Establecer una estructura adecuada para preparación, mitigación y respuesta; así como contar con personal competente, con el nivel de responsabilidad y autoridad necesaria.
c) Establecer actividades de respuesta y recuperación; así como realizar evaluaciones periódicas mediante ejercicios y pruebas.

7.1.13. Cumplimiento de requisitos legales, contractuales, de propiedad intelectual, información personal y protección de registros

El OSCD 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 OSCD 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 OSCD debe velar por 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 y suscripciones de software instaladas en los equipos informáticos de Ositrán y llevar un adecuado control de su vigencia.

f) La Gerencia de Asesoría Jurídica o la unidad de organización que corresponda, debe establecer y/o mantener vigentes los lineamientos orientados a la privacidad y protección de los datos personales que se gestionen dentro de la entidad.

7.1.14. Revisiones de seguridad de la información

El OSCD debe monitorear y controlar 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.

7.1.15. Procedimientos operativos documentados

La JTI debe elaborar y mantener actualizada la documentación de los procedimientos operativos para las instalaciones de procesamiento de información.

7.2. CONTROLES DE PERSONAL

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 buzón de correo electrónico asignado al servidor civil, una vez que haya tomado conocimiento del cambio o desvinculación, cuando corresponda. 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.

7.2.4. Seguridad de la información para el trabajo remoto

a) El OSCD debe disponer y/o gestionar el establecimiento de un lineamiento que defina las condiciones y restricciones para acceder, tratar o almacenar la información durante el teletrabajo en la entidad.
b) El acceso a la red de datos y sistemas de la entidad en el teletrabajo debe efectuarse, vía un servicio de internet, empleando obligatoriamente la VPN (Red Privada Virtual por sus siglas en inglés) o mecanismos equivalentes y las correspondientes credenciales de red (usuario y contraseña) previamente asignadas al colaborador.
c) 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.
d) El uso de un equipo de propiedad del usuario está permitido de manera excepcional, previa autorización del titular de la unidad de organización correspondiente. El acceso a los sistemas, aplicativos y páginas de internet desde equipos de propiedad de los usuarios estará sujeto a los lineamientos y restricciones que la JTI defina en los documentos pertinentes.
e) El usuario es responsable de mantener el equipo de su propiedad con un software de seguridad informática (antivirus o antimalware) y sistema operativo actualizado y vigente, así como cualquier otro requisito que sea definido por la JTI. Asimismo, deberá permitir a la JTI efectuar las verificaciones periódicas que resulten pertinentes.

f) En caso de los servidores civiles que no puedan mantener el equipo de su propiedad con los requisitos correspondientes, éstos deberán necesariamente emplear un equipo de la entidad.

7.3 CONTROLES FÍSICOS

7.3.1 Seguridad de la información en áreas seguras

a) El OSCD debe definir y revisar los controles de seguridad física en los perímetros de las áreas que contienen información.
b) El OSCD debe evaluar los riesgos asociados al acceso físico no autorizado a las áreas seguras y proponer mecanismos y controles.
c) El OSCD 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 OSCD, en coordinación con la JLCP y/o con los responsables de las áreas seguras, 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.
e) El OSCD, en coordinación con la JLCP y/o 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.
f) 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.
g) 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.
h) 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 por parte del responsable del área segura. Durante dicho periodo, el personal externo que no pertenece a la entidad debe ser acompañado por un responsable encargado.
i) Los responsables de las áreas seguras deben evitar el trabajo no supervisado de proveedores en dichas áreas.
j) 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.
k) La JLCP debe establecer actividades de monitoreo a las instalaciones para detectar y disuadir el acceso físico no autorizado.

7.3.2 Seguridad en los equipos informáticos y medios de almacenamiento

La JTI debe prevenir la pérdida, daño, robo o el compromiso de los activos y la interrupción de las operaciones de la entidad. Para tal fin 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) Realizar o gestionar el mantenimiento preventivo y/o correctivo a los equipos informáticos de los usuarios y a la infraestructura tecnológica de la entidad.

c) El OSCD debe implementar mecanismos que eviten la revelación, modificación, eliminación o destrucción no autorizada de la información almacenada en medios de soportes removibles.
d) Asegurar que todo traslado de un equipo fuera de las instalaciones de la entidad sea coordinado con la JLCP y se realice con las debidas precauciones para su protección contra posibles daños y robos.
e) Velar que todo equipo desplazado para el teletrabajo cuente con la autorización de la Gerencia de Administración.
f) Adoptar una política de escritorio limpio y pantalla limpia en los equipos de la red de datos de la entidad.
g) Verificar que la información confidencial y/o restringida; así como el software con licencia se haya eliminado o sobre escrito en los equipos antes de su eliminación o reasignación.

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.

7.3.3. Suministro de apoyo y seguridad en el cableado

a) La JTI debe asegurar que los equipos informáticos, comunicaciones y de seguridad perimetral, sean protegidos contra cortes de energía u otras interrupciones causadas por fallas de los servicios públicos de apoyo (fluido eléctrico, telecomunicaciones, suministro de agua, entre otros).
b) La JTI debe efectuar las gestiones pertinentes para asegurar que el cableado eléctrico y de red de datos se encuentren separados, ordenados, etiquetados, y protegidos contra intercepciones, interferencias o daños.

7.4 CONTROLES TECNOLÓGICOS

7.4.1. Seguridad de la información para uso de dispositivos de usuario.

a) El OSCD debe proponer los lineamientos y medidas de seguridad apropiadas para la protección contra los riesgos asociados al uso de dispositivos terminales de usuario en la entidad.
b) El uso y asignación de dispositivos terminales de usuario deben ser autorizados y solicitados por el titular de la unidad de organización.
c) La JTI activará en los dispositivos terminales asignados, las configuraciones y herramientas de seguridad para su uso.

d) Todos los dispositivos terminales de usuario 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 terminal de usuario 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 terminal asignado por la entidad, el servidor civil debe reportarlo inmediatamente a la mesa de ayuda de JTI.
g) Todo dispositivo terminal provisto por la entidad debe contar con controles de acceso, controles contra fuga de datos, cifrado de dispositivo de almacenamiento y protección contra *malware*.

7.4.2. Derechos de acceso privilegiados

a) La JTI debe establecer lineamientos y mecanismos para restringir y administrar la asignación y uso de derechos de acceso privilegiado.

7.4.3. Control y restricción de acceso a la información

a) La JTI debe establecer lineamientos para evitar el acceso no autorizado a la información y otros activos asociados, de acuerdo con los lineamientos de seguridad de la información para el acceso, identidades y autenticación.
b) La JTI debe implementar mecanismos para controlar el acceso a la información en sistemas, aplicaciones y servicios.

7.4.4. Control de acceso al código fuente

a) La JTI deberá controlar el acceso a los repositorios que contengan código fuente de las aplicaciones y *software* de la entidad, herramientas de desarrollo y las bibliotecas de *software*.

7.4.5. Autenticación segura

a) La JTI debe implementar mecanismos de autenticación segura, en función de las restricciones de acceso a la información y lineamientos de seguridad de la información para el acceso, identidades y autenticación.

7.4.6. Gestión de capacidad

a) La JTI debe 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.

7.4.7. Protección contra programas maliciosos

a) La JTI debe asegurar 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.

7.4.8. Gestión de vulnerabilidades técnicas

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

a) Evaluar periódicamente la identificación de nuevas vulnerabilidades en los sistemas de información, aplicativos o plataformas tecnológicas que se encuentren en producción.

b) Implementar las acciones correspondientes para mitigar los riesgos asociados a las vulnerabilidades identificadas.
c) 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.

7.4.9. Gestión de la configuración

La JTI debe monitorear y controlar que las configuraciones funcionen de acuerdo con los requisitos de seguridad y que no se vea alterada por cambios no autorizados o incorrectos. Para ello, debe:

a) Establecer, documentar e implementar configuraciones seguras para hardware, software, servicios y redes.
b) Establecer roles, responsabilidades y actividades para gestionar todos los cambios de configuración. Mantener un registro seguro de las configuraciones establecidas y sus modificaciones, siguiendo las acciones para la gestión de cambios.
c) Establecer actividades para monitorear, revisar y actualizar regularmente las plantillas de configuración para abordar nuevas amenazas o vulnerabilidades.
d) Proteger la información sensible registrada en las plantillas y objetivos de configuración contra accesos no autorizados.

7.4.10. Eliminación de la información

a) La JTI debe establecer lineamientos para la eliminación de información cuando ya no sea necesaria, considerando requisitos legales, normativos y contractuales. Estos lineamientos deben definir plazos de retención, técnicas apropiadas y métodos de eliminación seguros para diferentes tipos de información y medios de almacenamiento.

7.4.11. Enmascaramiento de datos

a) La JTI debe definir técnicas de enmascaramiento de datos a fin de limitar la exposición de datos confidenciales y/o restringidos, incluida la información de identificación personal, para cumplir con los requisitos legales, normativos y contractuales.
b) La JTI debe establecer la técnica de seudonimización o anonimización que aplicará para ocultar la data de carácter confidencial.
c) El OSCD debe verificar que los datos hayan sido adecuadamente seudonimizados o anonimizados, considerando todos los elementos de la información sensible para prevenir la identificación indirecta de los usuarios.

7.4.12. Prevención de fuga de datos

a) La JTI debe establecer medidas de prevención de fuga de datos en todos los sistemas, redes y dispositivos que procesen, almacenen o transmitan información confidencial y/o restringida, con el fin de detectar y prevenir la divulgación y extracción no autorizada de información.
b) La JTI debe monitorear los canales potenciales de fuga y actuar preventivamente mediante el uso de herramientas especializadas para controlar, detectar y bloquear posibles fugas de datos.

7.4.13. Copia de seguridad de la información

La JTI debe establecer medidas o mecanismos para 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) Ejecutar 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.

De la misma manera, todos los usuarios deben almacenar su información en los repositorios de información institucionales (Sharepoint), para asegurar su respaldo.

7.4.14. Redundancia de las instalaciones de procesamiento de información

La JTI debe asegurar el funcionamiento continuo de las instalaciones de procesamiento de información y servicios tecnológicos, para lo cual, 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.

7.4.15. Registro de actividades, excepciones, fallas y eventos relevantes

La JTI debe registrar eventos y generar evidencias sobre las actividades de los usuarios, excepciones, fallos y eventos de seguridad de la información. 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 asegurar su confidencialidad, integridad, disponibilidad y trazabilidad.

7.4.16. Actividades de monitoreo

a) La JTI debe monitorear las redes, sistemas y aplicaciones para detectar comportamientos anómalos y posibles incidentes de seguridad.
b) La JTI debe establecer una línea base de comportamiento normal considerando patrones de uso y acceso.
c) La JTI debe comunicar eventos anormales a las partes relevantes y establecer actividades de respuesta oportuna.

7.4.17. Sincronización de reloj

a) La JTI debe 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.

7.4.18. Uso de programas de utilidad privilegiados e instalación de software en sistemas operativos

La JTI debe garantizar la integridad del software en sistemas operativos. Para ello, debe:

a) Controlar el uso de programas utilitarios privilegiados que puedan anular los controles de seguridad de los sistemas y de las aplicaciones.
b) Implementar procedimientos para controlar la instalación del software de sistemas operativos.
c) Mantener un registro de la instalación y/o desinstalación de los softwares en los sistemas operacionales.

7.4.19. Gestión de la seguridad de redes

La JTI debe proteger 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.

7.4.20. Filtrado de la web

a) La JTI debe establecer mecanismos para bloquear el acceso a sitios web maliciosos, no autorizados o que contengan contenido ilegal.
b) La JTI debe establecer y mantener actualizados los lineamientos para el uso seguro y apropiado de recursos en línea, incluyendo restricciones específicas sobre sitios web y aplicaciones web inapropiadas.

7.4.21. Uso de Criptografía

a) La JTI debe asegurar un uso adecuado y eficaz de los controles criptográficos para proteger la confidencialidad, autenticidad y/o integridad de la información de la entidad, así como para el no repudio y la autentificación de usuarios en operaciones efectuadas por medios digitales.
b) La JTI debe implementar métodos criptográficos que permitan una conexión segura, en el caso que los sistemas de información requieran autenticación de los usuarios.
c) La JTI debe gestionar ante los entes correspondientes la revocación y/o cancelación de los certificados digitales, ante el cese del personal, o en caso de que estos hayan sido comprometidos o dejaron de usarse.
d) La JTI debe asegurar 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.

7.4.22. Seguridad en el ciclo de vida de desarrollo 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 y requisitos sobre el desarrollo seguro de aplicaciones y sistemas, para los desarrollos internos y tercerizados.
b) Establecer, mantener y aplicar a cualquier actividad de desarrollo de sistemas de información, principios para diseñar sistemas seguros.
c) Aplicar al desarrollo y/o mantenimiento de sistemas de información y/o aplicaciones, los principios de codificación segura.
d) Ejecutar las pruebas unitarias y de seguridad informática, esta última de corresponder, así como las pruebas de aceptación con el usuario final como parte del proceso del desarrollo del software.
e) 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.
f) Separar los recursos de desarrollo, pruebas y operación, para reducir los riesgos de acceso no autorizado o los cambios del sistema en producción.
g) 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.
h) Seleccionar, proteger y gestionar adecuadamente la información de prueba.

7.4.23. Protección de los Sistemas de Información durante las pruebas de Auditoría

El OSCD debe planificar las pruebas de auditoría y otras actividades de aseguramiento que involucren la evaluación de los sistemas y aplicaciones, en coordinación con el titular de la organización correspondiente.

VIII. Disposiciones complementarias

8.1. 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 las disposiciones de la presente directiva.

9.2. El Oficial de Seguridad y Confianza Digital es el responsable de realizar el seguimiento al cumplimiento y/o implementación de las disposiciones establecidas en la presente directiva.

9.3. El Oficial de Seguridad y Confianza Digital del Ositrán es responsable de revisar el presente documento, así como otras políticas y documentos normativos institucionales en materia de seguridad de la información con periodicidad anual o cuando ocurran cambios significativos, a fin de asegurar la vigencia de sus disposiciones y su efectividad continua.

Cuadro de Control de Cambios de la Directiva de Seguridad de la Información del Ositrán

Versión : 03

Elaborado por : **Américo Abreu Hidalgo**
Jefe de Tecnologías de la Información (e)

Revisado por : **Ricardo Mercado Toledo**
Jefe de la Gerencia de Planeamiento y Presupuesto

Javier Chocano Portillo
Jefe de la Gerencia de Asesoría Jurídica

Aprobado por : **Juan Carlos Mejía Cornejo**
Gerente General

Control de Cambios :

Referencia	Identificación del cambio
Versión 02	✓ Se actualizó la Directiva, de acuerdo con los requisitos y controles de la versión vigente de la norma ISO 27001:2022 ✓ Se actualizó el acápite III. Base legal. ✓ En el acápite V. Glosario de términos y acrónimos, se incorporaron los términos: Áreas seguras, confianza digital, dispositivos de usuario, técnicas de seudonimización o anonimización. Se incorporó el acrónimo CSCD. ✓ Se reorganizó el contenido de las disposiciones específicas en función de la nueva estructura de la norma vigente. ✓ Se incorporó la disposición general 6.12, relacionada a la restricción de divulgación de información. ✓ Se incorporó la sección 7.1 Controles Organizacionales ✓ Se actualizó el nombre del control 7.1.1 a Roles y responsabilidades. ✓ Se modificó en el numeral 7.1.1. el nombre de Analista en Seguridad de la Información por Especialista de Seguridad de la Información y Ciberseguridad. ✓ Se modificó el numeral 7.1.1. la función b) del rol Titulares de las unidades de organización. ✓ Se modificó el nombre del numeral 7.1.3 a Contacto con autoridades y grupos especiales de interés. ✓ Se incorporó el control 7.1.4. Inteligencia de amenazas, el cual contiene el desarrollo de los literales a) y b). ✓ Se modificó el nombre del numeral 7.1.6.1. Inventario y uso aceptable de la información y activos asociados. En esta sección se incorporó el literal c) y se modifica el literal e). ✓ Se modificó el nombre del numeral 7.1.6.2. Clasificación y etiquetado de la información. En esta sección de modifican los literales b), c), e), f), g) y h) ✓ Se modificó el nombre del numeral 7.1.7. Seguridad de la Información para el Accesos, Identidades y Autenticación. ✓ Se modificaron los literales b) y f) de la sección 7.1.7.1. Requisitos para el control de acceso. ✓ Se modificó el nombre del numeral 7.1.7.2. Gestión de identidades. Se modifica el literal d), de este numeral. ✓ Se modificó el nombre del numeral 7.1.7.3. Responsabilidades del usuario respecto a la gestión de accesos y autenticación. ✓ Se modificó el nombre del numeral 7.1.7.4. Derechos de acceso a sistemas y aplicaciones, en esta sección se modifica el literal b).

	✓ Se modificaron los literales d), e) y f) de la sección 7.1.8.1. Seguridad de la información en las relaciones con los proveedores. ✓ Se modificaron el nombre del numeral 7.1.8.2. Seguridad de la información en la ejecución de los servicios del proveedor, en esta sección se modifican los literales a) y b). ✓ Se incorporó el numeral 7.1.9. Seguridad de la información para el uso de servicio en la nube. Esta sección contiene los literales a), b), c) y d). ✓ Se modificaron los literales a), b) y c) y se incorpora el literal g) del numeral 7.1.10. Gestión de incidentes de seguridad de la información. ✓ Se incorporaron el numeral 7.1.11. Seguridad de la información durante una disrupción. Esta sección contiene los literales a) y b) y c. ✓ Se incorporaron el numeral 7.1.12. Preparación de las TIC para la continuidad del negocio, el cual contiene el desarrollo de los literales a) y b). ✓ Se actualizó el numeral 7.1.13. Cumplimiento de requisitos legales y contractuales, de propiedad intelectual, información personal y protección de registros. En esta sección se modifica el literal e). ✓ Se modificó la parte introductoria del numeral 7.1.14. Revisiones de seguridad de la información. ✓ Se incorporó el numeral 7.1.15. Procedimientos operativos documentados. ✓ Se incorporó la sección 7.2. Controles de personal. ✓ Se modificó el literal d) del numeral 7.2.3 Termino del empleo o cambio de puesto de trabajo. ✓ Se incorporó el numeral 7.2.4. Seguridad de la información para el trabajo remoto, en el cual se modifican los literales b), d) y e). ✓ Se incorporó la sección 7.3. Controles físicos. ✓ En el numeral 7.3.1. Seguridad de la información en áreas seguras, se incorporan los literales a) y k). ✓ Se incorporó el numeral 7.3.2. Seguridad en los equipos informáticos y medios de almacenamiento, el cual contiene el desarrollo de los literales a), b), c), d), e), f) y g). ✓ Se incorporó el numeral 7.3.3. Suministro de apoyo y seguridad en el cableado, el cual contiene los literales a) y b). ✓ Se incorporó la sección 7.4. Controles tecnológicos. ✓ Se incorporó el numeral 7.4.1. Seguridad de la información para uso de dispositivos de usuario. Se modifican los literales a), b), c), d), e), f) y g). ✓ Se incorporó el numeral 7.4.2. Derecho de accesos privilegiados. El cual cuenta con el literal a). ✓ Se incorporó el numeral 7.4.3. Control y restricción de acceso a la información. El cual cuenta con los literales a) y b). ✓ Se incorporó el numeral 7.4.4. Control de acceso al código fuente. El cual cuenta con el literal a). ✓ Se incorporó el numeral 7.4.5. Autenticación segura. El cual cuenta con el literal a). ✓ Se incorporó el numeral 7.4.6. Gestión de capacidad. El cual cuenta con el literal a). ✓ Se incorporó el numeral 7.4.7. Protección contra programas maliciosos, el cual contiene el desarrollo de los literales a) y b). ✓ Se incorporó el numeral 7.4.8. Gestión de vulnerabilidades técnicas, el cual contiene los literales a), b) y c). ✓ Se incorporó el numeral 7.4.9. Gestión de la configuración, el cual contiene los literales a), b), c) y d).

	✓ Se incorporó el numeral 7.4.10. Eliminación de la información, el cual contiene el literal a). ✓ Se incorporó el numeral 7.4.11. Enmascaramiento de datos, el cual contiene los literales a), b) y c). ✓ Se incorporó el numeral 7.4.12. Prevención de fuga de datos, el cual contiene los literales a) y b). ✓ Se modificó la parte introductoria y el literal d) del numeral 7.4.13. Copia de seguridad de la información. ✓ Se incorporó el numeral 7.4.14. Redundancia de las instalaciones de procesamiento de información. ✓ Se modificó el nombre del numeral 7.4.15. Registro de actividades, excepciones fallas y eventos relevantes. Además, se modifican los literales a) y b). ✓ Se incorporó el nombre del numeral 7.4.16. Actividades de monitoreo. Además, se modifican los literales a), b) y c). ✓ Se reubica el numeral 7.4.17. Sincronización de reloj. ✓ Se modificó el nombre del numeral 7.4.18. Uso de programas de utilidad privilegiados e instalación de software en sistemas operativos. En esta sección se modificó la introducción, y los literales a) y b). ✓ Se modificó el nombre del numeral 7.4.19. Gestión de la seguridad de redes. Se adecúa la introducción de esta sección. ✓ Se incorporó el numeral 7.4.20 Filtrado de la web, el cual contiene los literales a) y b). ✓ Se modificó el nombre del numeral 7.4.21 Uso de Criptografía. Adicionalmente se modifican los literales a). b) y c) ✓ Se modificó el nombre del numeral 7.4.22. Seguridad en el ciclo de vida de desarrollo de los sistemas de información y software. Adicionalmente se modifican el literal a) y se incorporan los literales b), c), f) y h). ✓ Se modificó el numeral 7.4.23. Protección de los sistemas de información durante las pruebas de auditoría.

Visado por:
AMÉRICO ABREU HIDALGO
Jefe de Tecnologías de la Información (e)
Jefatura de Tecnologías de la Información