UEB	Código	SGSI-PO-001
	Versión	01
	Clasificación	USO INTERNO

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN DE LA UNIDAD EJECUTORA 1767 "IMPLEMENTACIÓN DEL MODELO DE LA INFRAESTRUCTURA Y FUNCIONAMIENTO DE LA BICAMERALIDAD DEL PODER LEGISLATIVO"

FIRMA DIGITAL
Firmado digitalmente por: RENGIFO TAM William David FAU 20613768484 hard
Motivo: En señal de conformidad
Fecha: 16/06/2025 15:24:04-0500

FIRMA DIGITAL
Firmado digitalmente por: HUARCAYA LIMA OMAR MANUEL FIR 10720319 hard
Motivo: En señal de conformidad
Fecha: 16/06/2025 15:22:39-0500

I. PRESENTACIÓN

En el marco de la implementación del Sistema de Gestión de Seguridad de la Información, según los requerimientos de la NTP ISO/IEC 27001:2022 Seguridad de la Información, ciberseguridad y protección de la privacidad - Sistemas de gestión de seguridad de la información – Requisitos - 3ª Edición; la Unidad Ejecutora "Implementación del Modelo de la Infraestructura y Funcionamiento de la Bicameralidad del Poder Legislativo" (en adelante UEB), define las Políticas de Seguridad de la Información cuyo cumplimiento e implementación proporciona controles para el tratamiento de riesgos de seguridad de la información y el logro de los objetivos de seguridad de la información en línea con los objetivos institucionales.

Las políticas contenidas en el presente documento se encuentran organizadas en secciones de acuerdo con la clasificación establecida en la norma NTP ISO/IEC 27001:2022 Seguridad de la Información, ciberseguridad y protección de la privacidad. Sistemas de gestión de seguridad de la información. Requisitos. 3ª Edición. Las secciones del Anexo A – Tabla A.1, siendo estas las siguientes: Controles organizacionales, Controles de Personal, Controles Físicos y Controles Tecnológicos.

II. OBJETIVO

Proteger la información en concordancia con los requisitos de seguridad de la UEB y las normas relacionadas, que permitan realizar la implementación, operación, mantenimiento y mejora del Sistema de Gestión de Seguridad de la Información en la UEB, como parte de la gestión institucional.

III. BASE LEGAL

3.1. Ley N° 27269, Ley de Firmas y Certificados Digitales y su reglamento y su modificatoria.
3.2. Ley N° 27309, Ley que incorpora los delitos informáticos al Código Penal.
3.3. Ley N° 29733, Ley de Protección de Datos Personales y modificatoria.
3.4. Ley N° 30096, Ley de Delitos Informáticos y su modificatoria.
3.5. Ley N° 31572, Ley del Teletrabajo y su modificatoria.
3.6. Decreto Legislativo Nº 1353, que crea la Autoridad Nacional de Transparencia y Acceso a la Información Pública, fortalece el régimen de protección de datos personales y la regulación de la gestión de intereses y su modificatoria.
3.7. Decreto Legislativo N° 1412, que aprueba la Ley de Gobierno Digital.
3.8. Decreto de Urgencia Nº 006-2020, que crea el Sistema Nacional de Transformación Digital.
3.9. Decreto de Urgencia N° 007-2020, que aprueba el marco de confianza digital y dispone medidas para su fortalecimiento.
3.10. Decreto Supremo N° 050-2018-PCM, que establece la definición de Seguridad Digital de ámbito nacional.
3.11. Decreto Supremo N° 021-2019-JUS, que aprueba la Ley de Transparencia y Acceso de la Información Pública y su Reglamento.
3.12. Decreto Supremo N° 029-2021-PCM, que aprueba el Reglamento del Decreto Legislativo N° 1412 -Ley de Gobierno Digital.
3.13. Decreto Supremo Nº 157-2021-PCM, que aprueba el Reglamento del Decreto de Urgencia N° 006-2020 que crea el Sistema Nacional de Transformación Digital.
3.14. Decreto Supremo N° 002-2023-TR, Reglamento de la Ley N° 31572 – Ley del Teletrabajo.
3.15. Decreto Supremo N° 016–2024-JUS, que aprueba el Reglamento de la Ley N° 29733, Ley de Protección de Datos Personales y modificatoria.
3.16. Resolución Ministerial Nº 041-2017-PCM, que aprueba el uso obligatorio de la Norma Técnica Peruana "NTP-ISO/IEC 12207:2016- Ingeniería de Software y Sistemas.

Procesos del ciclo de vida del software. 3a Edición", en todas las entidades integrantes del Sistema Nacional de Informática.

3.17. Resolución Ministerial N° 119-2018-PCM, que dispone la creación de un Comité de Gobierno Digital en cada entidad de la administración Pública.
3.18. Resolución Ministerial N° 087-2019-PCM, que aprueba disposiciones sobre la conformación y funciones del Comité de Gobierno Digital.
3.19. Resolución Ministerial N° 320-2021-PCM, que aprueba los lineamientos para la gestión de la continuidad operativa y la formulación de los planes de continuidad operativa de las entidades públicas de los tres niveles de gobierno.
3.20. Resolución Secretarial N° 001-2018-PCM/SEGDI, que aprueba los Lineamientos para el Uso de Servicios en la Nube para entidades de la Administración Pública del Estado Peruano.
3.21. Resolución Directoral N° 022-2022-INACAL/DN que aprueba la Norma Técnica Peruana NTP ISO/IEC 27001:2022 Seguridad de la Información, ciberseguridad y protección de la privacidad. Sistemas de gestión de seguridad de la información. Requisitos. 3ª Edición.
3.22. Directiva N° 001-2022-PCM/SGTD Directiva que establece el Perfil y Responsabilidades del Oficial de Gobierno de Datos.
3.23. Directiva Nº 001-2023-PCM/SGTD Directiva que establece el Perfil y Responsabilidades del Oficial de Seguridad y Confianza Digital.
3.24. 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.
3.25. Resolución de Secretaría de Gobierno y Transformación Digital N° 002-2023-PCM/SGTD que aprueban la Directiva Nº 001-2023-PCM/SGTD, Directiva que establece el perfil y responsabilidades del Oficial de Seguridad y Confianza Digital.
3.26. Política General de Seguridad de la Información, SGSI-POLI-01 del Congreso de la República, aprobada con Resolución N° 080-2022-2023-OM-CR.
3.27. Resolución de Contraloría General N° 320-2006-CG – Normas de Control Interno.
3.28. Resolución Directoral N° 012-2025-DE-UEB/CR, que conforma el Comité de Gobierno y Transformación Digital de la UEB; y designa al Líder de Gobierno y Transformación Digital, así como al Oficial de Seguridad y Confianza Digital.

IV. DIAGNÓSTICO

Mediante la Ley N° 31988, Ley de Reforma Constitucional, se aprueba el restablecimiento de la Bicameralidad en el Congreso de la República del Perú. En dicho marco, a través de la Segunda Disposición Complementaria Final de la Ley N° 32172, se creó la Unidad Ejecutora 1767 "Implementación del modelo de la infraestructura y funcionamiento de la bicameralidad del Poder Legislativo", que se sujeta al presupuesto institucional del Pliego 028, exceptuándose del artículo 68 del Decreto Legislativo N° 1440, Decreto Legislativo del Sistema Nacional de Presupuesto Público.

La UEB, en el marco del Sistema Nacional de Presupuesto Público, es el nivel descentralizado u operativo del Pliego 028: Congreso de la República, y administra los ingresos y gastos públicos, se vincula e interactúa con los órganos rectores de la Administración Financiera del Sector Público y los órganos y unidades orgánicas del Congreso de la República. La UEB cuenta con autonomía normativa, técnica, económica, financiera y administrativa que le permite actuar con flexibilidad en la gestión, independencia operativa y transparencia en la rendición de cuentas. Tiene autonomía funcional y de gestión, dentro de las disposiciones internas aplicables.

La UEB puede aplicar extensivamente, en todo o en parte, las disposiciones (documentos normativos de gestión, disposiciones normativas, otros documentos de gestión u otros) aprobadas por otras instancias del Congreso de la República que sean necesarias para optimizar el ejercicio de sus funciones, considerando la referencia a los órganos y unidades orgánicas indicadas en dichas disposiciones como a las unidades de organización de la UEB que hagan sus veces.

La UEB tiene como parte de sus funciones:

- Planificar, coordinar, ejecutar y supervisar la implementación del modelo de la infraestructura para el funcionamiento de la bicameralidad del Poder Legislativo.
- Planificar, coordinar, ejecutar y supervisar los procesos de contrataciones dentro del ámbito de su competencia.
- Organizar los centros de costos con el propósito de lograr la eficiencia técnica en la producción y entrega de los productos a su cargo.
- Realizar la liquidación y cierre o acciones similares de las intervenciones ejecutadas.
- Formular y aprobar los documentos normativos de gestión, disposiciones normativas y otros documentos de gestión necesarios para optimizar el ejercicio de sus funciones.

Debido a la relevancia de la información que maneja la entidad, es necesario que se implemente y mantenga un Sistema de Gestión de Seguridad de la Información (en adelante SGSI) en los procesos principales y servicios críticos, que permita minimizar los riesgos que afecten la confidencialidad, integridad y disponibilidad de la información que administra, mantener la continuidad de sus servicios y mejorar la confianza de las partes interesadas sobre la adecuada gestión de sus riesgos; en cumplimiento del Decreto Supremo N° 029-2021-PCM, que establece el Reglamento de la Ley de Gobierno Digital.

La presente Política de Seguridad de la Información fue elaborada tomando como referencia la Política General de Seguridad de la Información del Congreso de la República y la Norma Técnica NTP ISO/IEC 27001:2022 Seguridad de la Información, ciberseguridad y protección de la privacidad - Sistemas de gestión de seguridad de la información - Requisitos - 3ª Edición; en donde se mencionan los controles que permitirían mitigar los riesgos de seguridad de la información, los mismos que se podrían aplicar a los activos de información relevantes de la UEB.

V. ALCANCE

La presente política es aplicable a los procesos, servicios, activos de información, recursos tecnológicos y personas responsables en el tratamiento, almacenamiento, administración, transmisión o acceso a información dentro del ámbito de la UEB, sin importar su forma, medio o soporte, y con independencia del modelo de provisión tecnológica (local o en la nube).

El alcance de esta política abarca el tratamiento seguro de la información institucional, incluyendo datos personales, documentos normativos, archivos administrativos, recursos digitales compartidos y toda la infraestructura de tecnología utilizada por la UEB, ya sea de forma interna o a través de servicios contratados en la nube. Esta política es de aplicación obligatoria para todo el personal, incluyendo terceros, y constituye el marco rector del Sistema de Gestión de la Seguridad de la Información (SGSI) de la UEB.

VI. MARCO CONCEPTUAL

La ISO (Organización Internacional para la Estandarización) y la IEC (la Comisión Electrotécnica Internacional) conforman el sistema especializado encargado de crear normas a nivel mundial. En este proceso participan organismos miembros de diferentes nacionalidades. Para el campo de las Tecnologías de Información y Comunicaciones (TIC), han establecido el comité ISO/IEC JTC 1, que se enfoca en el SGSI y la familia de normas o estándares ISO/IEC 27000.

El estándar ISO/IEC 27001:2022 "Seguridad de la Información, ciberseguridad y protección de la privacidad. Sistemas de gestión de seguridad de la información. Requisitos." Especifica los requisitos para la creación, implementación, funcionamiento, supervisión, revisión, mantenimiento y mejora de un SGSI documentado, teniendo en cuenta los riesgos institucionales generales de la organización. Es decir, explica cómo diseñar un SGSI y

establecer los controles de seguridad, de acuerdo con las necesidades y objetivos de una organización, los requisitos de seguridad y sus procesos.

El estándar busca establecer un sistema documentado (política, análisis de riesgos, procedimientos, etc.), donde la alta dirección (Dirección Ejecutiva) colabore activamente y se involucre en el desarrollo y gestión del sistema. Se controlará el funcionamiento del sistema para que opere correctamente y la mejora sea continua, practicándose auditorías internas y revisiones del sistema para verificar que se están obteniendo los resultados esperados. Asimismo, activas acciones encaminadas a solucionar los problemas detectados en las actividades de comprobación (auditorías y revisiones), a prevenir problemas y a mejorar aquellos asuntos que sean susceptibles de ello.

En Perú, el Comité Técnico de Normalización de Codificación e Intercambio Electrónico de Datos presentó a la Dirección de Normalización de INACAL, con fecha 10-11-2021, la propuesta de la PNTP-ISO/IEC 27001:2022 para su revisión y aprobación. No habiéndose presentado observaciones, fue oficializado como Norma Técnica Peruana NTP-ISO/IEC 27001:2022 "Seguridad de la información, ciberseguridad y protección de la privacidad. Sistemas de gestión de seguridad de la información. Requisitos", 3ª Edición.

La NTP-ISO/IEC 27001:2022 "Seguridad de la información, ciberseguridad y protección de la privacidad. Sistemas de gestión de seguridad de la información. Requisitos", 3ª Edición, es una adopción de la norma ISO/IEC 27001:2022. Esta presenta cambios editoriales referidos principalmente a terminología empleada propia del idioma español y ha sido estructurado en concordancia a las Guías Peruanas GP 001:2016 y GP 002:2016.

Con fecha 29 de diciembre del 2022, el Comité Permanente de Normalización aprueba la Norma Técnica Peruana NTP-ISO/IEC 27001:2022 "Seguridad de la información, ciberseguridad y protección de la privacidad. Sistemas de gestión de seguridad de la información. Requisitos", 3ª Edición, con Resolución Directoral N° 022-2022-INACAL- DN.

Asimismo, la Presidencia del Consejo de Ministros, con el Decreto Supremo N° 029- 2021-PCM y la Resolución de Secretaría de Gobierno y Transformación Digital N° 003- 2023-PCM/SGTD, estableció la obligación de implementar en todas las entidades públicas un SGSI teniendo como alcance mínimo sus procesos misionales y aquellos que son relevantes para su operación.

VII. DEFINICIONES Y ACRÓNIMOS[1]

A. Definiciones

- **Activo. -** En seguridad de la información un activo es algo que presenta valor para la organización.
- **Activos de información. -** Cualquier información o sistema relacionado con el tratamiento de la misma que tenga valor para la organización.
- **Anonimización. -** Tratamiento de datos personales que impide la identificación o que no hace identificable al titular de estos. El procedimiento es irreversible.
- **Banco de datos personales. -** Conjunto organizado de datos personales, automatizados o no, independientemente del soporte, sea este físico, magnético, digital, óptico u otros que se creen, cualquiera fuere la forma o modalidad de su creación, formación, almacenamiento, organización y acceso.
- **Centro Nacional de Seguridad Digital – CNSD. -** Gestiona, dirige, articula y supervisa la operación, educación, promoción, colaboración y cooperación de la Seguridad Digital a nivel nacional como componente integrante de la seguridad nacional, a fin de fortalecer la confianza digital.

[1] Fuente: NTP ISO/IEC 27002:2022, Decreto Supremo N° 050-2018-PCM, Decreto Supremo N° 029-2021-PCM, Decreto de Urgencia N° 007-2020 y el artículo 2 de la Ley N° 29733.

- **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.
- **Código fuente**. - Es un archivo o conjunto de archivos que contienen el código escrito en un lenguaje de programación de un sistema de información o aplicativo informático.
- **Confidencialidad de la información. -** Garantizar que la información sea accesible únicamente para quienes tengan acceso autorizado.
- **Controles de seguridad de la información. -** Medida que modifica un riesgo. Incluyen cualquier proceso, política, dispositivo, práctica u otras acciones que modifiquen un riesgo.
- **Datos personales. -** Toda información sobre una persona natural que la identifica o la hace identificable a través de medios que pueden ser razonablemente utilizados.
- **Datos personales sensibles. -** Datos personales constituidos por los datos biométricos que por sí mismos pueden identificar al titular; datos referidos al origen racial y étnico; ingresos económicos, opiniones o convicciones políticas, religiosas, filosóficas o morales; afiliación sindical; e información relacionada a la salud o a la vida sexual.
- **Disponibilidad de la información. -** Garantizar que los usuarios autorizados tengan acceso a la información y activos asociados cuando sea necesario.
- **Función conflictiva. -** Aquellas funciones en que requieren que un mismo individuo puede ejecutar actividades como:
  Iniciar, aprobar o ejecutar un cambio.
  Solicitar, aprobar o implementar derechos de acceso.
  Desarrollar software, probarlo e implementarlo en producción.
  Diseñar, implementar y auditar procesos o controles.
- **Gestión del Riesgo. -** Actividades coordinadas para dirigir y controlar una organización en lo relativo al riesgo.
- **Incidente de seguridad digital. -** Evento o serie de eventos que pueden comprometer la confianza, la prosperidad económica, la protección de las personas y sus datos personales, la información, entre otros activos de la organización, a través de tecnologías digitales.
- **Integridad de la información. -** Salvaguardar la exactitud e integridad de la información y activos asociados.
- **IP - Internet Protocol o Protocolo de Internet. -** La IP es una dirección única que identifica a un dispositivo en Internet o en una red local.
- **Enmascaramiento de datos. -** Es el proceso de ocultar datos personales modificando sus letras y números originales con la finalidad de proteger su confidencialidad.
- **Logueo.-** Acción de ingresar a un sistema de información o servicio informático.
- **Medios de almacenamiento removibles. -** Son aquellos dispositivos que se insertan a los conectores externos de los equipos informáticos para almacenar información, tales como memorias USB, disco duro externo o tarjetas de memoria.
- **Mejora continua. -** Es la actividad recurrente para mejorar el desempeño de los procesos.
- **Propietario del activo o sistemas de información. -** Identifica a la persona o a la entidad que tiene la responsabilidad gerencial aprobada de controlar la producción, desarrollo, mantenimiento, uso y seguridad del activo. Es el dueño o propietario del proceso.
- **Propietario del riesgo. -** Persona o entidad que tiene la responsabilidad y autoridad para gestionar un riesgo, dentro del alcance de sus competencias.
- **Riesgos. -** Probabilidad de que una amenaza pueda explotar una vulnerabilidad de un activo.
- **Seguridad de la Información. -** Preservar la confidencialidad, integridad y disponibilidad de la información; además, también pueden ser involucradas otras características como la autenticación, responsabilidad, no-repudio y fiabilidad.
- **Servicio digital.-** Es aquel servicio provisto de forma total o parcial a través de Internet u otras redes equivalentes, que se caracteriza por ser parcial o totalmente automatizado y utilizar de manera intensiva las tecnologías digitales y datos, permitiendo, al menos una de las siguientes prestaciones: i) Adquirir un bien, servicio, información o contenido,

ii) Buscar, compartir, usar y acceder a datos, contenido o información sobre productos, servicios o personas, iii) Pagar un servicio o bien (tangible o intangible) y, iv) El relacionamiento entre personas.

- **Servicios en la nube. -** La provisión de servicios en la nube es un modelo para permitir el acceso por red, de forma práctica y bajo demanda, a un conjunto de recursos de computación configurables (por ejemplo, redes, servidores, almacenamiento, aplicaciones y servicios) que pueden ser suministrados y desplegados rápidamente con una mínima gestión o interacción con el proveedor de servicio. (Definición de Instituto Nacional de Normas y Tecnología del Departamento de Comercio de los Estados Unidos de América [NIST SP800- 145])
- **Sistema de Gestión de Seguridad de la Información (SGSI).-** Es la parte del sistema integral de gestión, basado en un enfoque del riesgo del negocio para establecer, implementar, operar, monitorear, revisar, mantener y mejorar la seguridad de la información.
- **Software. -** Conjunto de reglas o programas que dan instrucciones para que un equipo de cómputo realice tareas específicas. También se conoce como aplicaciones de software, paquetes de software, herramientas de software y programas de software.
- **Tratamiento de datos personales. -** Cualquier operación o procedimiento técnico, automatizado o no, que permite la recopilación, registro, organización, almacenamiento, conservación, elaboración, modificación, extracción, consulta, utilización, bloqueo, supresión, comunicación por transferencia o por difusión o cualquier otra forma de procesamiento que facilite el acceso, correlación o interconexión de los datos personales.
- **Transformación Digital. -** La transformación digital es el proceso continuo, disruptivo, estratégico y de cambio cultural que se sustenta en el uso intensivo de las tecnologías digitales, sistematización y análisis de datos para generar efectos económicos, sociales y de valor para las personas.
- **Seguridad Digital. -** Es el 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 nacional y los objetivos nacionales en dicho entorno.

B. Acrónimos

- **CGTD. -** Comité de Gobierno y Transformación Digital.
- **CNSD.** - Centro Nacional de Seguridad Digital.
- **OGP**.- Oficina de Gestión de Proyectos.
- **PCM. -** Presidencia del Consejo de Ministros.
- **SGSI.** - Sistemas de Gestión de Seguridad de la Información.
- **UEB**. - Unidad Ejecutora 1767 "Implementación del modelo de la infraestructura y funcionamiento de la bicameralidad del Poder Legislativo".
- **UTI**. - Unidad de Tecnologías de la Información.
- **VPN**. - Red Privada Virtual (del inglés Virtual Private Network).

VIII. PRINCIPIOS

La Política de Seguridad de la Información de la UEB se sustenta en los siguientes principios:

8.1. **Principio de Confidencialidad.-** Garantizar que la información sea accesible solo para aquellas personas autorizadas a tener acceso a la misma.
8.2. **Principio de Integridad.-** Salvaguardar la exactitud y totalidad de la información y los métodos de procesamiento.
8.3. **Principio de Disponibilidad.-** Garantizar que los usuarios autorizados tengan accesos a la información y a los recursos necesarios, toda vez que lo requieran.
8.4. **Principio de no repudio.-** Evitar que una entidad que haya enviado o recibido información alegue ante terceros que no la envió o recibió.
8.5. **Principio de auditabilidad.-** Asegurar que los eventos de un sistema deben poder ser registrados para su control posterior.

8.6. **Principio de Legalidad.-** Garantizar el cumplimiento de las leyes, normas, reglamentaciones o disposiciones a las que está sujeta la institución.
8.7. **Principio de Calidad.-** Salvaguardar la veracidad, exactitud y actualización de la información que administra.
8.8. **Principio de Seguridad.-** Adoptar las medidas técnicas, organizativas y legales necesarias para garantizar la seguridad de los datos y la información.
8.9. **Principio de concientización y formación.–** Asegurar la ejecución de acciones de formación, sensibilización y concientización en seguridad de la información a los colaboradores para fortalecer la cultura.
8.10. **Principio de responsabilidad.-** Todas y todos los colaboradores son responsables en su conducta en cuanto a la seguridad de la información, ciñéndose estrictamente a las normas legales vigentes y controles establecidos.
8.11. **Principio de mejora continua.-** Revisar la eficacia de los controles de seguridad establecidos e implementados, a fin de que sigan respondiendo a los cambios y a la constante evolución del riesgo y del entorno tecnológico.

IX. POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN

La UEB, a través de la Dirección Ejecutiva, reconoce a la información como un activo fundamental para la prestación de los servicios y la toma de decisiones eficientes y eficaces, por esta razón, gestiona la seguridad de la información física y digital bajo su responsabilidad y se compromete a:

9.1. Implementar, mantener y mejorar continuamente el Sistema de Gestión de Seguridad de la Información (SGSI) basado en la NTP-ISO/IEC 27001:2022, que garantice la preservación de la confidencialidad, integridad, disponibilidad y trazabilidad de la información, y sus procesos de acuerdo con el marco normativo y regulatorio vigente.
9.2. Fortalecer y promover la cultura institucional basada en la concientización, prevención, gestión del riesgo y mejora continua, a través de programas de formación, monitoreo de cumplimiento y revisión sistemática del desempeño del SGSI.
9.3. Promover la gestión eficaz de sus riesgos, eventos e incidentes de seguridad de la información, con la finalidad de garantizar la disponibilidad de los servicios y recursos informáticos.
9.4. Apoyar los objetivos y disposiciones de seguridad de la información designando los recursos necesarios para la ejecución de sus planes, así como el establecimiento, mantenimiento y mejora continua del Sistema de Gestión de Seguridad de la Información.

X. OBJETIVOS DE SEGURIDAD DE LA INFORMACIÓN

10.1. Fortalecer la cultura en seguridad de la información de los funcionarios, servidores y colaboradores de la UEB.
10.2. Gestionar de manera eficaz los riesgos, eventos e incidentes de seguridad de la información.
10.3. Implementar controles para asegurar la preservación de la confidencialidad, integridad y disponibilidad de la información de la UEB, así como la continuidad de los servicios.
10.4. Asegurar el cumplimiento de requerimientos legales y regulatorios en materia de seguridad y confianza digital.
10.5. Establecer, implementar, operar, evaluar y mejorar el Sistema de Gestión de Seguridad de la Información de la UEB.

XI. POLÍTICAS ESPECÍFICAS

11.1. Dirección de la UEB para la seguridad de la información

Objetivo: Brindar orientación y apoyo de la Dirección Ejecutiva para garantizar la seguridad de la información de acuerdo con las normas institucionales, las leyes y regulaciones pertinentes.

La UEB manifiesta su compromiso, a través del CGTD, de llevar a cabo lo siguiente:

a) Difundir periódicamente las Políticas Específicas de Seguridad de la Información de la UEB entre los colaboradores.
b) Evaluar el cumplimiento de la implementación de los controles de seguridad de la información, como resultado de la aplicación de las Políticas Específicas de Seguridad de la Información.
c) Revisar y actualizar, de ser necesario, las Políticas Específicas de Seguridad de la Información de la UEB en un plazo de un año, contado a partir de la aprobación y publicación de este documento o antes, en caso de producirse cambios significativos que afecten la seguridad de la información.

Las siguientes políticas específicas se encuentran agrupadas en cuatro secciones, de acuerdo a la categorización de controles de seguridad proporcionada en la NTP ISO/IEC 27002:2022 "Seguridad de la información, ciberseguridad y protección de la privacidad. Controles de seguridad de la información", 3ª Edición, Anexo A, Tabla A.1.

11.2. Controles organizacionales

11.2.1. Roles y responsabilidades en seguridad de la información

Objetivo: Establecer una estructura organizativa para la implementación, operación y gestión de la seguridad de la información en la institución.

La responsabilidad de la implementación del SGSI es de la Dirección Ejecutiva, según lo dispone el Decreto Supremo N° 029-2021-PCM y la Resolución de Secretaría de Gobierno y Transformación Digital N° 003-2023-PCM/SGTD. Asimismo, se han establecido los siguientes roles para efectuar la implementación, mantenimiento del SGSI y la operación de los controles de seguridad de la información:

- Dirección Ejecutiva
- Comité de Gobierno y Transformación Digital (CGTD)
- Oficial de Seguridad y Confianza Digital (OSCD)
- Líder de Gobierno y Transformación Digital
- Secretario/a Técnico/a del CGTD
- Oficial de Gobierno de Datos
- Oficial de Datos Personales
- Propietario de la Información
- Custodios de la Información

Las responsabilidades de cada rol se encuentran en el numeral XII, así mismo, las actividades específicas de cada rol se encontrarán en los documentos normativos que designan el rol, disposiciones, directivas y procedimientos.

11.2.2. Segregación de funciones

Objetivo: Segregar los roles y actividades para reducir oportunidades de modificación no autorizada, error, evasión de controles o mal uso de los activos de la organización.

Los propietarios de los procesos deben evaluar las actividades y responsabilidades de cada rol de los colaboradores para asegurar que se encuentran separadas las funciones conflictivas entre diferentes individuos

para mitigar el riesgo de modificación no autorizada, error, evasión de controles o mal uso de los activos de información de la UEB.

11.2.3. Contactos con autoridades

Objetivo: Contar con la información de contacto con autoridades legales, reguladoras y de supervisión y establecer el flujo de comunicación con ellos.

La Unidad de Tecnologías de la Información (UTI) y el Oficial de Seguridad y Confianza Digital, deben mantener la lista actualizada de los contactos con autoridades que permita reportar oportunamente los eventos e incidentes de seguridad de la información.

Para el caso del reporte de los incidentes de seguridad física, corresponde a la Oficina de Administración mantener el Directorio de los actores involucrados en el Sistema Nacional de Gestión del Riesgo de Desastres.

11.2.4. Contactos con grupos especiales de interés

Objetivo: Contar con la información de contacto con grupos especializados que puedan apoyar la atención de consultas e incidentes relacionados a la seguridad de la información.

La UTI, el Oficial de Seguridad y Confianza Digital, y los propietarios de los procesos, en caso corresponda, deben mantener actualizada una Lista de los Grupos o Foros de Interés en los que participan a fin de realizar consultas o recibir alertas tempranas sobre vulnerabilidades relacionadas a seguridad de la información.

11.2.5 Inteligencia de amenazas

Objetivo: Permitir la recopilación de la información de las amenazas relacionadas a seguridad de la información y su análisis para realizar acciones para su adecuada mitigación.

La UTI debe recopilar información de las amenazas existentes y emergentes para tomar acciones que conlleven a reducir su impacto o evitar que causen daño, entre estas acciones está el comunicar la información de las amenazas a las partes relevantes y su inclusión en los procesos de gestión de riesgos de seguridad de la información.

11.2.6 Seguridad de la información en la gestión de proyectos

Objetivo: Identificar desde etapas iniciales y a lo largo de todo el proyecto, los riesgos asociados a la seguridad de la información, a fin de establecer las medidas necesarias para su tratamiento.

Corresponde a los Jefes de cada unidad de organización, identificar los riesgos relacionados con la seguridad de la información e informarlos a la OGP, para que esta elabore la propuesta de mitigación.

11.2.7 Inventario de información y otros activos asociados

Objetivo: Identificar los activos de información de la institución y los propietarios, así como definir responsabilidades para una protección apropiada.

Las Unidades de Organización comprendidos en el alcance de la presente Política, deben:

a) Identificar e inventariar la información y otros activos asociados con el tratamiento de la información; así como las instalaciones de procesamiento y almacenamiento de la información.
b) Determinar la importancia de los activos de información en términos de seguridad de la información.
c) Asignar a un propietario y un custodio del activo de la información.
d) Identificar la clasificación de los activos de información.
e) Mantener actualizado el inventario de activos de información.

Los usuarios deben:
a) Proteger la información que utilizan o acceden evitando su exposición o divulgación; en concordancia con su clasificación.
b) Usar los activos de información sólo y exclusivamente para fines laborales en cumplimiento con el marco normativo y las políticas de seguridad de la información, para evitar daños operativos, a la imagen o a otros intereses de la institución.
c) Los activos de información, independientemente de su formato o soporte de almacenamiento no pueden ser retirados de la institución sin autorización del propietario.
d) Todo activo que contiene información no debe ser desatendido, y debe quedar resguardado o se deben utilizar bloqueos especiales para evitar el acceso de personas no autorizadas a la información que contiene.

11.2.8. Uso aceptable de la información y otros activos asociados

Objetivo: Asegurar que se definen e implementan las reglas y procedimientos para el manejo de los activos de información y otros activos asociados.

Corresponde a la UTI, y a los propietarios de los procesos definir e implementar las normas y procedimientos para el uso y manejo de la información y los activos asociados dentro del alcance de sus competencias.

Todo el personal de la UEB, en general, es responsable del uso de la información y los activos de información a los cuales tienen acceso para cumplir sus funciones.

El Oficial de Seguridad y Confianza Digital debe efectuar el seguimiento anual al cumplimiento de las disposiciones sobre el uso aceptable de activos de información.

11.2.9. Devolución de activos

Objetivo: Proteger los intereses de la entidad cuando se realice un desplazamiento de personal (rotación, encargos o designaciones temporales, entre otros), traslado de unidad de organización o finalización de la relación laboral de los colaboradores.

El personal, al término de su relación laboral con la UEB, debe:
a) Poner a disposición de su jefe inmediato (o a quien este designe formalmente) todos los documentos físicos o en formato digital que le fueron entregados o hayan sido generados, como parte del cumplimiento de sus actividades.
b) En el caso de los equipos informáticos como computadoras, laptop, entre otros que utilizaba para el desempeño de sus funciones deberá ser

entregado al Jefe de la UTI de acuerdo al procedimiento o disposición establecido para tal fin.

c) Otros activos relacionados con el tratamiento de la información que le fueron entregados, de acuerdo a las disposiciones establecidas.

También corresponde a los jefes de cada unidad de organización tomar las acciones necesarias para asegurar la transferencia del conocimiento del personal que ya no labora.

11.2.10. Clasificación de la información

Objetivo: Asegurar que se aplique un nivel de protección adecuado a la información.

Los propietarios de activos de la información en posesión de la UEB son los responsables de:

a) Clasificar su información de acuerdo con lo establecido en Texto Único Ordenado de la Ley de Transparencia y Acceso a la Información Pública: secreta, reservada, confidencial y/o pública.
b) Clasificar toda información producida, transferida o recibida o bajo su control dentro del ámbito de sus responsabilidades, ya sea lógica (información que se genera y que se encuentra almacenada en Internet o medio electrónico como disco duro, USB, CD, DVD, entre otros) o física (información contenida en papel).

El Oficial de Seguridad y Confianza Digital, debe verificar los controles, supervisar su correcta implementación y recomendar mejoras de los controles requeridos en concordancia con su clasificación.

Los responsables de las Unidades de Organización deben asegurar que la información sea tratada y protegida en concordancia con su clasificación.

Para la Información clasificada como Secreta o Reservada:

a) Se debe ubicar en un ambiente que cuente con acceso seguro o de acceso restringido con resguardo de un personal asignado por el órgano que custodia la información.
b) En su almacenamiento y/o transmisión se debe aplicar algún tipo de mecanismo de seguridad y ser cifrado (preferentemente con la última versión tecnológica existente), según corresponda.
c) No se debe obtener copias físicas o electrónicas en ninguna circunstancia, caso contrario se deberá implementar los controles adecuados para su reserva.
d) Para la difusión o divulgación de la información clasificada como "Secreta o Reservada" se requiere la autorización expresa del Propietario de la Información.

Para la Información clasificada como Confidencial:

a) Se debe ubicar en un ambiente que cuente con acceso restringido, registrándose los accesos a estos ambientes.
b) Su almacenamiento debe ser mínimamente bajo llave (o algún otro mecanismo de seguridad similar) y ser cifrado (con la última versión tecnológica compatible con los sistemas institucionales), según corresponda.
c) Se debe controlar las copias físicas o electrónicas registrándose, como mínimo, la fecha de la copia y de la persona que lo recibe.

d) Su comunicación digital se debe dar por canales seguros de transmisión, cifrados con la última tecnología vigente y a direcciones de correos electrónicos institucionales autorizados por el propietario del activo. Para el caso de documentos enviados por el Sistema de Gestión Documental, estos deben ser marcados como confidencial y cifrados para evitar el acceso a personas no autorizadas.
e) Para la difusión o divulgación de la información clasificada como "Confidencial" se requiere el consentimiento previo, informado, expreso e inequívoco del Propietario de la Información.

11.2.11. Etiquetado de la información

Objetivo: Facilitar la comunicación de la clasificación de la información.

Los propietarios de activos de la información en posesión de la UEB son los responsables de etiquetar la información clasificada como secreta, reservada o confidencial ya sea almacenada en papel o medio electrónico.

Los responsables de las unidades de organización Orgánicas deben:

a) Asegurar que la información sea etiquetada en concordancia con su clasificación.
b) Para el etiquetado se puede utilizar sellos, etiquetas físicas, encabezados y pies de página, metadatos, marca de agua, entre otros.
c) Todos los documentos físicos o digitales que son considerados confidencial o reservados o secreto deben ser etiquetados (marcados), siempre y cuando los activos sean de propiedad de la UEB.
d) La información, documentos o activos que no tienen la clasificación de confidencial o reservado o secreto, no amerita etiquetado.
e) Se excluye de etiquetar la salida de información de los sistemas de información.

11.2.12. Transferencia de información

Objetivo: Mantener la seguridad de la información intercambiada dentro de la institución y con cualquier otra entidad.

La UTI debe proteger el intercambio de información por medio electrónico, en concordancia con su clasificación.

Corresponde al propietario de la información analizar, evaluar y definir el alcance de la transferencia de la información que realizarán con otras entidades para darle los controles de seguridad, al transferir información que no sea de carácter público.

Los responsables de las Unidades de Organización de la UEB deben:

a) Verificar la implementación de controles de seguridad de la información propuestos por la UTI, para la transferencia de la información según su clasificación.
b) Asegurar el uso de un acuerdo o cláusula de confidencialidad y no divulgación previa a la transferencia de información que no sea de carácter público ya sea dentro de la UEB o con otra entidad externa.
c) Entregar la información digital por medios magnéticos, de forma personal al destinatario, en un sobre cerrado y lacrado; o haciendo uso de técnicas criptográficas que protejan la información de la intercepción y permitan la autenticación del destinatario y el no repudio; su entrega debe quedar registrada.

d) Incorporar al acuerdo de transferencia de información lo siguiente:
- Responsabilidades para controlar y notificar la transmisión, el despacho y la recepción.
- Actividades para garantizar la capacidad de seguimiento y no repudio.
- Normas técnicas mínimas para el empaque y transmisión.
- Uso del etiquetado acorde con la clasificación de la información.
- Responsabilidades en caso de incidentes de seguridad de la información, tales como la pérdida de los datos.
- Cualquier control especial necesario para proteger información sensible, como criptografía.
- Mantener una cadena de custodia para la información durante el tránsito.
- Niveles de control de acceso.

e) Considerar para el acceso de terceros a información secreta, reservada o confidencial, los siguientes requisitos:
- Firma de un acuerdo o acta que indique la información que se protegerá, la duración esperada del acuerdo, las responsabilidades de cada parte y las acciones de los firmantes para evitar la divulgación de información no autorizada.
- El uso permitido de la información y los derechos del firmante para utilizar la información.
- El procedimiento para notificar e informar sobre la divulgación no autorizada o la fuga de información confidencial.
- Procedimiento a seguir para el retorno de la información o su destrucción al término del acuerdo.
- Medidas que se tomarán en caso de un incumplimiento del acuerdo.

El personal de la UEB debe:
a) Evitar que los documentos con información que no sea de carácter público sean expuestos a personas no autorizadas mientras permanezca bajo su custodia (incluye el proceso de impresión).
b) Cumplir los lineamientos o políticas de uso del correo electrónico institucional y servicio de internet emitidas por la UTI.
c) Cuidar que la información a la cual tienen acceso para cumplir sus funciones y cuya clasificación no es pública, solo sea compartida entre los usuarios autorizados por el propietario de la información y su tratamiento se realice en concordancia con su clasificación.

11.2.13. Control de acceso

Objetivo: Asegurar el acceso de usuarios autorizados y prevenir el acceso no autorizado a los sistemas, servicios e instalaciones de procesamiento de información.

Todo acceso otorgado a los sistemas de información, servicios informáticos debe considerar la premisa de mínimo privilegio ("Todo está prohibido a menos que esté expresamente permitido"), los principios de necesidad de saber ("sólo acceso a la información necesaria para sus actividades") y necesidad de uso ("sólo acceso a la infraestructura que requiere para sus actividades").

La UTI debe establecer las normas para el control de acceso en concordancia con los requisitos de seguridad de la información de cada proceso. El acceso a plataformas, sistemas de información, servicios informáticos, instalaciones físicas y en general cualquier recurso de información de la UEB, debe ser

definido y asignado de acuerdo con los documentos de gestión de la UEB, así como a las normas legales o leyes aplicables.

La autorización para el acceso a los sistemas de información debe ser definida y aprobada por el propietario de la información, y se debe otorgar de acuerdo con el nivel de clasificación de la información identificada en los documentos de gestión de la UEB, según la cual se deben determinar los controles y privilegios de acceso que se pueden otorgar a los colaboradores de acuerdo a sus funciones.

Los requerimientos y atenciones de acceso a los sistemas de información y servicios informáticos de la UEB deben ser registrados en los formatos establecidos en los procedimientos para este propósito.

Corresponde a la Oficina de Administración establecer disposiciones para el control de acceso físico a la Institución y sus ambientes.

11.2.14. Gestión de identidades

Objetivo: Permitir la identificación única de las personas que acceden a la información, sistema de información y servicios informáticos.

La UTI debe considerar en las disposiciones y procedimientos referido al acceso a los sistemas de información y servicios informáticos lo siguiente:

a) Solo una identidad específica se pueda asignar a una persona.
b) En el caso se requiera asignar una identidad a más de una persona (identidades compartidas), esta debe ser justificada y autorizada por el jefe de la unidad de organización propietaria del proceso en los formatos establecidos.
c) De requerirse asignar identidades a entidades no humanas, estás deben ser aprobadas por el Jefe de la UTI y supervisadas por el Oficial de Seguridad y Confianza Digital.
d) Guardar todos los eventos relacionados al uso y gestión de identidades de usuario.

11.2.15. Información de autenticación

Objetivo: Asegurar la autenticación adecuada evitando fallas en los procesos de autenticación.

La UTI debe asegurar que el procedimiento, los sistemas de información y servicios informáticos consideren lo siguiente:

a) La asignación de contraseñas únicas y secretas durante el proceso de inscripción o creación de una identidad. Los usuarios serán forzados a cambiar su contraseña antes de su primer uso o inicio de sesión con contraseñas de no menos de doce (12) caracteres, combinando letras mayúsculas, minúsculas, números e incluir un carácter especial.
b) Procedimientos automáticos para reiniciar la contraseña del usuario previa verificación de su identidad.
c) Enviar la información de autenticación, incluyendo la temporal, de manera segura.
d) Permitir el acuse de recibo de los usuarios del envío de la información.
e) Permitir a los usuarios cambiar su contraseña cuando lo requieran.
f) Restringir la reutilización de contraseñas.
g) No mostrar la visualización de las contraseñas en la pantalla mientras el usuario la ingresa.

h) Almacenar y transmitir la contraseña en forma segura.
i) Cambiar la clave de manera obligatoria cada treinta (30) días calendario.
j) Bloquear la cuenta del usuario por un lapso de quince (15) minutos luego de cinco (5) intentos fallidos de acceso.
k) Registrar los intentos fallidos y exitosos de acceso.
l) Establecer mecanismos que permitan dos o más factores de autenticación incluyendo algo que conoce, tiene o es parte de la identidad del usuario, por ejemplo, códigos remitidos al correo electrónico o equipos móviles, uso de preguntas secretas y lectura de datos biométricos.
m) Mantener evidencia de los eventos significativos relacionados con la asignación y gestión de la información de la autenticación.

Los usuarios de los sistemas de información y de los servicios informáticos de la UEB, deben:

a) Mantener en secreto la información de autenticación a los sistemas de información y servicios informáticos, así como cambiarla en un periodo no mayor a los treinta (30) días calendario.
b) En el caso de uso de identidades asignadas a múltiples personas, solo la información de autenticación debe ser compartida entre estos usuarios.
c) Cambiar las contraseñas de acceso antes del primer inicio de sesión o en caso de detectarse algún indicio que vulnere la seguridad de la misma.
d) Seleccionar una contraseña, con las siguientes características:
   - Debe estar conformada por doce caracteres como mínimo, debiendo ser una combinación de letras mayúsculas, minúsculas, números y/o caracteres especiales.
   - En su construcción se deberá evitar coincidencias con palabras de diccionario, nombre de la institución, datos del usuario tales como nombres, apellidos, fecha de nacimiento; entre otros.
   - Evitar el uso de la contraseña en otros servicios, por ejemplo, aplicaciones o correo electrónico de uso personal o redes sociales.
e) Evitar mantener anotadas las contraseñas en cualquier medio físico o electrónico, salvo que sea registrada debidamente encriptada.

11.2.16. Derechos de acceso

Objetivo: Asegurar que el acceso a la información, al sistema de información y a otros activos asociados esté definida y autorizada de acuerdo con los requisitos del negocio.

Los responsables de las Unidades de Organización de la UEB son formalmente los gestores de accesos a los sistemas de información y a los servicios informáticos del cual son propietarios.

Los gestores de accesos son los responsables, en los sistemas de información que se les asigne, de gestionar y autorizar las acciones de crear, actualizar y dar de baja a las cuentas de usuario y sus accesos a los sistemas de información y servicios informáticos, previa autorización del responsable de la unidad orgánica en el que labora el usuario, cualquiera que sea la modalidad de contractual (incluido proveedores y terceros); y del responsable de la Unidad Orgánica propietaria del sistema de información y servicio informático.

Los responsables de las Unidades de Organización propietarias de un sistema de información y servicio informático, debe coordinar que los gestores de acceso mantengan un inventario actualizado de las identidades y accesos a los sistemas de información y servicios informáticos del cual son propietarios, así como se guarde el registro de la autorización de acceso de los usuarios (activación, modificación o bajas de cuentas de acceso).

La Unidad de Recursos Humanos debe comunicar a la UTI la relación de los colaboradores que finalizan su relación laboral, tienen una licencia mayor o igual a tres (3) meses o un desplazamiento de personal, en un plazo máximo de un (01) día hábil de acontecido el evento, a través del procedimiento establecido.

La Unidad de Logística debe comunicar a la UTI la relación de los proveedores o terceros que finalizan su relación contractual en un plazo máximo de un (01) día hábil, a través del procedimiento establecido.

Para el caso de la baja de las cuentas de acceso a los sistemas de información que utilizaban los colaboradores y/o proveedores o terceros que laboraron o prestaron servicios o tienen una licencia mayor o igual a tres (3) meses, corresponde al jefe de la Unidad Orgánica en el que trabajaron, solicitar la baja de las cuentas a la Unidad Orgánica propietaria del sistema de información en un plazo máximo de un (01) día hábil.

La UTI debe atender la solicitud de inactivación o cancelación de las cuentas de acceso a la red de datos y a los servicios tecnológicos de la UEB que administra en un plazo de un (01) día hábil a partir de la comunicación.

Corresponde a los propietarios de los sistemas de información, a través de sus gestores de accesos, atender las solicitudes de cancelación o inactivación de las cuentas de acceso a los sistemas de información bajo su responsabilidad en un plazo de un (01) día hábil, a partir de la comunicación.

También, corresponde al responsable de la Unidad de Organización en el que laboró el personal, remover los accesos físicos, por ejemplo: llaves de puertas o de armarios, accesos con lectores biométricos.

El Responsable del órgano propietario del sistema de información, debe revisar trimestralmente la gestión de las cuentas de acceso de los usuarios de los sistemas de información realizada por el gestor de accesos.

El Oficial de Seguridad y Confianza Digital debe revisar trimestralmente, a nivel de muestra, las cuentas de acceso a los sistemas de información y servicios informáticos.

11.2.17. Seguridad de la información en las relaciones con los proveedores

Objetivo: Gestionar los riesgos de seguridad de la información en las relaciones con los proveedores.

Los responsables de las Unidades de Organización que requieran la contratación de bienes y servicios relacionados con el acceso, procesamiento, almacenamiento, transferencia y otro tipo de tratamiento de la información, deben:

a) Verificar que los proveedores o terceros y su personal cumplan con los requisitos requeridos para el servicio contratado y firmen una cláusula o acuerdo confidencialidad y de no divulgación.
b) Coordinar que los proveedores o terceros reciban la sensibilización y capacitación en seguridad de la información, que les sean aplicables, por ejemplo, cuando tengan acceso a información confidencial, reservada o secreta deben conocer las políticas y procedimientos de seguridad.
c) Identificar, evaluar y gestionar los riesgos de seguridad de la información asociados con el uso de los activos de información dentro del servicio.

d) Solicitar a la empresa o institución proveedora que proporcione a la UEB, antes de realizar un servicio, la relación de personas, perfiles, funciones y responsabilidades asociadas al servicio provisto, disponer se informe cualquier cambio (alta, baja, sustitución o cambio de funciones o responsabilidades) que se produzca en dicha relación.
e) Elaborar los acuerdos de intercambio de la información con proveedores, que cumplan los requisitos definidos en la sección de transferencia de información del presente documento, incluyendo el retorno de los activos una vez terminado el servicio.
f) Asegurar que los proveedores y terceros que accedan a las instalaciones de tratamiento de información sensible solo usen el material estrictamente necesario para llevar a cabo las actividades acordadas.
g) Gestionar la transferencia de conocimiento, información y los activos asociados.

11.2.18. Abordar la seguridad de la información dentro de los acuerdos con proveedores

Objetivo: Mantener el nivel de seguridad de la información y entrega de servicios de acuerdo a las condiciones preestablecidas.

Los responsables de las unidades de organización deben asegurar el cumplimiento de los requerimientos de seguridad de la información considerados en las especificaciones técnicas y/o términos de referencia.

Se pueden considerar como parte de los requisitos de seguridad en los términos de referencia del servicio lo siguiente:

a) La incorporación de requerimientos de seguridad de la información (organizativos, legales y técnicos) en las especificaciones técnicas y/o términos de referencia; para ello podrá solicitar el apoyo de la UTI y/o del Oficial de Seguridad y Confianza Digital de la UEB.
b) Establecer en los acuerdos contractuales cláusulas de confidencialidad, declaración de responsabilidades con respecto a la seguridad de la información, cláusulas respecto a las leyes de derecho de autor o protección de datos personales; según corresponda. Dichos acuerdos contractuales deben estar vigentes hasta la finalización del contrato; según sea necesario.
c) Derecho a auditar los procesos y controles del proveedor relacionados con la seguridad de la información dentro del marco del contrato.
d) Procedimientos para la autorización y revocación de accesos y uso de información de la UEB y otros activos asociados.
e) Procedimientos para la notificación y gestión de incidentes de seguridad de la información.
f) Cumplimiento de las Políticas y normas referidas a seguridad de la información de la UEB por parte del proveedor.

De haber algún cambio en la provisión de servicios por parte de los proveedores se debe realizar una reevaluación de los riesgos de seguridad de la información, tomando en cuenta la criticidad de la información, sistemas y procesos involucrados.

11.2.19. Gestión de la seguridad de la información en la cadena de suministro de las TIC

Objetivo: Gestionar los riesgos de seguridad de la información en la cadena de suministro de productos y servicios TIC.

La UTI, cuando requiera la contratación de bienes y servicios TIC, debe:

a) Incorporar requerimientos o requisitos de seguridad de la información en los Términos de referencia del bien o servicio.
b) Solicitar que los proveedores de servicios de tecnología de la información y comunicaciones, que requieran subcontratar a otros proveedores, cumplan los requisitos de seguridad.
c) Validar que los productos y servicios TIC cumplan con los requisitos de seguridad establecidos, así como la funcionalidad solicitada.
d) Implementar medidas para garantizar que los componentes de los productos o servicios no sean alterados o modificados sin autorización de la UTI, por ejemplo: etiquetas anti-manipulación, verificaciones hash criptográficas o firmas digitales.
e) Gestionar el ciclo de vida de los componentes TIC, incluyendo riesgos de seguridad como la obsolescencia.

11.2.20. Seguimiento, revisión y gestión de cambios en servicios de proveedores

Objetivo: Monitorear, revisar, evaluar y gestionar periódicamente los cambios en la prestación de servicios.

Para los servicios críticos, los responsables de las unidades de organización deben:

a) Identificar y monitorear los cambios realizados por los proveedores incluyendo las mejoras a los servicios, el desarrollo de nuevas aplicaciones y sistemas, modificaciones a los procedimientos utilizados por el proveedor, controles para atender incidentes de seguridad de la información, cambio de personal o sub contrataciones, uso de nuevas tecnologías o productos o versiones.
b) Coordinar la ejecución de auditorías o verificaciones de la seguridad de la información en los servicios y verificar la atención de los hallazgos.

11.2.21. Seguridad de la información en el uso de servicios en la nube

Objetivo: Gestionar la seguridad de la información en el proceso de adquisición, uso, administración y finalización de los servicios en la nube.

La UTI debe asegurar que se identifican los requisitos mínimos cuando se contrate un servicio en la nube, para alinear la contratación con el cumplimiento de la normatividad vigente, así como la relacionada con la seguridad de la información y, cuando corresponda, con la protección de datos personales, de modo que se resguarde la información que sea almacenada o gestionada en la nube.

La UTI, debe considerar los siguientes aspectos en la contratación del servicio en la nube:

a) Establecer Acuerdos de Niveles de Servicio - ANS con el proveedor de servicios en la nube, en la que se defina las responsabilidades de la UEB y el proveedor, así como los tiempos de atención.
b) Cumplir con las medidas de seguridad aplicables para las entidades del Estado, como la NTP ISO/IEC 27001:2022 (o en su versión vigente) y las disposiciones señaladas en la Directiva de Seguridad emitida por la Autoridad Nacional de Protección de Datos Personales del Ministerio de Justicia (cuando corresponda).

c) Cumplir la Política de Seguridad de la Información de la UEB y demás documentos normativos de la institución que les aplique. La UEB deberá solicitar al proveedor una declaración de aplicabilidad de las medidas, certificaciones o acreditaciones en materia de seguridad de la información.
d) La disposición de monitorear, revisar y evaluar el uso de los servicios para administrar los riesgos de seguridad de la información.
e) El verificar del cumplimiento de las medidas de seguridad por parte del proveedor.

11.2.22. Planificación y preparación de la gestión de incidentes de seguridad de la información

Objetivo: Asegurar un enfoque consistente y efectivo para la gestión de incidentes de seguridad de la información.

La UTI debe establecer los procedimientos y responsabilidades para asegurar una respuesta rápida, efectiva y ordenada a los incidentes de seguridad de la información. Este procedimiento debe considerar:

a) El monitoreo y reporte de los eventos de seguridad de la información para decidir si son clasificados como incidentes de seguridad de la información.
b) Clasificar, priorización y análisis de los incidentes de seguridad de la información, determinando mínimamente su causa raíz, impacto, probabilidad de ocurrencia, la solución a la causa raíz, responsable de la atención y el periodo de implementación de la solución.
c) Seguimiento de la atención de los incidentes hasta su conclusión, incluyendo el escalamiento requerido y la comunicación a las partes interesadas.
d) Que el Jefe de la UTI, informe al Oficial de Seguridad y Confianza Digital todo incidente de seguridad digital crítico que afecte los procesos misionales y servicios que brinda la entidad, de forma inmediata.
e) Informar al Oficial de Seguridad y Confianza Digital las debilidades y eventos de seguridad de la información que podrían comprometer la continuidad de los servicios informáticos de la UEB.
f) Identificación y registro de las lecciones aprendidas y mejoras a los controles de seguridad de la información.

11.2.23. Evaluación y decisión sobre eventos de seguridad de la información

Objetivo: Asegurar una categorización y priorización de los eventos de seguridad de la información.

Los usuarios/Jefes/Direct deben reportar los eventos y/o debilidades de seguridad de la información relacionada a los servicios informáticos a la UTI, de acuerdo con los procedimientos establecidos. Asimismo, para el caso de los eventos relacionados a la seguridad física de las instalaciones de la UEB deberán reportarlo a la a la Oficina de Administración de la UEB.

Dichas unidades de organización deben dar tratamiento a los eventos y/o debilidades de seguridad de la información reportadas, asimismo, evaluar, clasificar, priorizar el evento y determinar si es un incidente; en caso afirmativo deberá comunicar al Oficial de Seguridad y Confianza Digital de acuerdo a los procedimientos establecidos.

11.2.24. Respuesta a incidentes de seguridad de la información

Objetivo: Asegurar una respuesta eficiente y eficaz a los incidentes de seguridad de la información.

La UTI debe comunicar los procedimientos establecidos para el reporte y la atención de los incidentes de seguridad de la información en forma rápida, efectiva y ordenada.

11.2.25. Aprendizaje de los incidentes de seguridad de la información

Objetivo: Reducir la probabilidad o las consecuencias de los futuros incidentes de seguridad de la información.

Corresponde a la UTI, en coordinación con el Oficial de Seguridad y Confianza Digital, considerar en el procedimiento de gestión de incidentes de seguridad de la información la cuantificación de los tipos, volúmenes y costos de los incidentes de seguridad de la información que permita:

a) Mejorar los protocolos de atención de los incidentes.
b) Identificar incidentes recurrentes o graves y sus causas para analizarlos e incluirlos en la evaluación de riesgos de seguridad de la información y así reducir la probabilidad o las consecuencias de futuros incidentes similares.
c) Mejorar los programas o planes de concienciación en seguridad de la información del usuario.

El Oficial de Seguridad y Confianza Digital, debe:
a) Comunicar a la UTI los incidentes de seguridad digital que le fueron reportados.
b) Comunicar al Oficial de Datos Personales los incidentes de seguridad de la información relacionados a bancos de datos personales a fin que, de considerarlo, pueda comunicarlo a la Autoridad de Protección de Datos Personales.
c) Revisar trimestralmente el proceso de gestión de incidentes de la UTI.

La UTI debe comunicar al CNSD los incidentes identificados a través de los medios que indique la plataforma Facilita (https://facilita.gob.pe/t/1025).

11.2.26 Recolección de evidencia

Objetivo: Asegurar una gestión eficaz de la evidencia relacionada con los incidentes de seguridad de la información que puedan implicar acciones disciplinarias y legales.

La UTI deberá definir un procedimiento para la identificación, recolección y conservación de la información que puede servir como evidencia para propósitos de acción disciplinaria y legal.

11.2.27 Seguridad de la información durante una interrupción

Objetivo: Mantener la seguridad de la información a un nivel apropiado durante una disrupción.

La UTI y la Oficina de Administración, dentro de ámbito de sus competencias, en coordinación con las demás unidades de organización de la UEB, deben

determinar los requisitos de seguridad para implementar los controles durante y después de una disrupción o falla; de tal manera que se proteja la información, se asegure la continuidad operativa y se restaure la seguridad de la información al nivel y en los plazos requeridos.

11.2.28. Preparación de las TIC para la continuidad del negocio

Objetivo: Mantener la disponibilidad de la información, sistemas de información y servicios tecnológicos de la UEB.

La Oficina de Administración a través de sus Unidades, deben establecer, implementar, probar, revisar y evaluar los planes, procesos, procedimientos y controles, para la continuidad de los procesos y servicios TIC de la UEB en caso de situaciones adversas. Asimismo, debe asegurar que reúna al menos los siguientes elementos:

a) Analizar y determinar los riesgos que puedan afectar la continuidad de los procesos y la seguridad de la información, en términos de probabilidad de ocurrencia de las amenazas e impacto, incluyendo la identificación y la determinación de la prioridad de los activos para cada proceso.
b) Identificar los requisitos de continuidad de las TIC (resultado del análisis de impacto en el negocio) y los controles preventivos o correctivos que permitirán la reducción de la probabilidad o impacto del riesgo. Entre estos controles se deben considerar:
   - Copias de seguridad de los sistemas y aplicaciones críticas y pruebas de restauración.
   - Monitoreo de los servicios TIC y revisión periódica de los logs.
c) Identificar los recursos financieros, organizacionales, técnicos y ambientales suficientes para tratar los riesgos identificados.
d) Formular, documentar, probar y actualizar periódicamente los planes y procedimientos de respuesta y recuperación ante una disrupción de los servicios TIC, como el Plan de Recuperación de Servicios Informáticos.

Los propietarios de los activos de información de la UEB deben identificar al personal crítico y asignarles, ante incidentes, la responsabilidad, la autoridad y la competencia necesaria para administrar un incidente y mantener la seguridad de la información.

La UTI en coordinación con las unidades de organización propietarios de los sistemas de información, deben efectuar revisiones y pruebas del plan de recuperación de servicios informáticos para verificar la eficacia de los controles, por lo menos dos veces al año.

11.2.29. Requisitos legales, estatutarios, regulatorios y contractuales

Objetivo: Evitar infracciones de las obligaciones legales, estatutarias, regulatorias o contractuales relacionadas con la seguridad de la información.

Los Unidades de organización de la UEB deben:
a) Identificar todos los requisitos legislativos, estatutarios, regulatorios y contractuales relevantes.
b) Implementar procedimientos para asegurar el cumplimiento de lo señalado en las normas legales, estatutarias, regulatorias o documentos contractuales relacionados con el tratamiento de la información, derechos de propiedad intelectual y uso de producto de software propietario.

Corresponde a la UTI implementar los controles criptográficos en cumplimiento con todos los acuerdos, legislación y regulación vigente.

El Oficial de Seguridad y Confianza Digital debe verificar la implementación de los controles para recomendar mejoras. Para el caso de los controles de seguridad en los bancos de datos personales de la UEB debe coordinar con el Oficial de Datos Personales.

11.2.30. Derechos de propiedad intelectual

Objetivo: Evitar infracciones de las obligaciones legales, estatutarias, regulatorias o contractuales relacionadas con los derechos de propiedad intelectual.

Los derechos de propiedad intelectual incluyen derechos de autor de software o documentos, derechos de diseño, marcas registradas, patentes y licencias de código fuente.

La UTI debe:

a) Llevar un registro de licencias de software y mantener las evidencias de las licencias adquiridas.
b) Implementar controles que aseguren que el número máximo de usuarios permitidos con licencias no sea excedido e impedir que los usuarios instalen software que atente contra los derechos de propiedad intelectual.
c) Realizar revisiones para verificar que solo se ha instalado software autorizado y/o con licencia.
d) Solicitar la inscripción y/o registro en Indecopi a nombre de la UEB, el software desarrollado (incluido el desarrollado por terceros), en el registro intelectual respectivo. Ello, con el objeto de acogerse a los resguardados que estipula la normativa relacionada a la Propiedad Intelectual.

11.2.31. Protección de registros

Objetivo: Proteger los registros ante la pérdida, destrucción, falsificación, acceso no autorizado y liberación no autorizada.

Las Unidades de organización de la UEB deben proteger la autenticidad, confiabilidad, integridad y usabilidad de los registros, por lo tanto, deben incorporar en los lineamientos y procedimientos de operativos o de tratamiento de información, las normas a seguir para el almacenamiento, custodia y eliminación de los registros de acuerdo con el esquema de clasificación.

11.2.32. Privacidad y protección de la información de identificación personal

Objetivo: Evitar infracciones al cumplimiento de las normas legales y regulatorias relacionados con la seguridad de la información de los datos personales.

Las unidades de organización de la UEB deben:

a) Identificar, documentar y registrar ante la Autoridad Nacional de Protección de Datos Personales, los bancos de datos personales existentes en el ámbito de sus responsabilidades.
b) Los propietarios de los sistemas de información deben efectuar el tratamiento de datos personales de acuerdo con las normas legales vigentes, debiendo:
c) Obtener el consentimiento libre, previo, expreso, informado e inequívoco del titular para el tratamiento de sus datos con el fin de recolectar, transferir, almacenar, usar, circular, suprimir, compartir, actualizar o transmitir dichos datos personales en el marco de las actividades de la institución.

d) Gestionar la implementación de los controles de tratamiento y de protección de los datos personales que administran según las directivas emitidas por la Autoridad de Protección de Datos Personales y los documentos normativos de la institución.
e) Implementar las medidas de seguridad definidas por el emisor o exportador de datos personales. La aceptación de la implementación de las medidas de seguridad debe realizarse por escrito mediante cláusulas contractuales u otro instrumento jurídico.
f) Disponer de cláusulas contractuales u otro instrumento jurídico para los terceros en los que se establezca la obligación de cumplir las normas legales y regulatorias vigentes respecto al tratamiento de los datos personales a los que pueda tener acceso en la ejecución del servicio.

La UTI debe implementar los controles de seguridad de la información para la protección de los bancos de datos localizados en el Micro Centro de Datos.

El Oficial de Seguridad y Confianza Digital, en coordinación con el Oficial de Datos Personales, debe verificar los controles, supervisar la correcta implementación, recomendar mejoras de los controles requeridos para la seguridad y gestión de los bancos de datos de la UEB.

11.2.33. Revisión independiente de la seguridad de la información

Objetivo: Verificar que la seguridad de la información, incluyendo personas, procesos y tecnología, está implementada y es operada de acuerdo con las políticas y normas de seguridad de la información.

El Oficial de Seguridad y Confianza Digital debe:
a) Elaborar y proponer al Comité de Gobierno y Transformación Digital para su aprobación, el programa de auditoría interna o externa al menos una vez por año, de los procesos que forman parte del alcance del SGSI.
b) Coordinar la ejecución de las auditorías internas o externas por personas independientes a los procesos o unidades orgánicas a revisar.
c) Realizar revisiones de la seguridad de la información al menos una vez al año, a los controles de seguridad de la información implementadas en la UTI. La revisión incluye los procesos relacionados con el procesamiento de la información, como son desarrollo de software, base de datos, redes, entre otros y debe realizarse tomando como criterios los controles del Anexo A de la NTP ISO/IEC 27001:2022 NTP Seguridad de la Información, ciberseguridad y protección de la privacidad. Sistemas de gestión de seguridad de la información. Requisitos. 3ª Edición.
d) Informar al Comité de Gobierno y Transformación Digital los resultados de las revisiones y auditorías.

El Comité de Gobierno y Transformación Digital, debe revisar los informes de los resultados de la auditoría interna, externa o de las revisiones realizadas o coordinadas por el Oficial de Seguridad y Confianza Digital.

11.2.34. Cumplimiento con políticas, reglas y normas de seguridad de la información

Objetivo: Verificar el cumplimiento de la Política de seguridad de la información de la UEB y los procedimientos o normas referidos a seguridad de la información.

Los Jefes de las unidades de organización de la UEB deben asegurar que el personal y los terceros dentro de la unidad orgánica que lideran, cumplen la política de la seguridad de la información. De existir incumplimientos, deben

reportarlo, analizar las causas, implementar las acciones correctivas y verificar la efectividad de las acciones tomadas.

El Oficial de Seguridad y Confianza Digital debe:

a) Revisar las políticas, disposiciones y procedimientos de seguridad de la información al menos una vez al año o cuando existan cambios en las normas o procesos de la institución.
b) Revisar, a nivel de muestra, que el personal y los terceros cumplan la política de la seguridad de la información al menos una vez al año.

11.2.35. Procedimientos operativos documentados

Objetivo: Asegurar que las operaciones de instalaciones de procesamiento de la información, como el Micro Centro de Datos de la UEB, se realicen en forma correcta y segura.

La UTI debe elaborar procedimientos documentados como mínimo para las actividades operativas que represente un riesgo de no realizarse de manera correcta. Estos procedimientos deben:

a) Establecer las actividades y responsabilidades para la gestión y operación de los medios de procesamiento y almacenamiento de la información, por ejemplo: monitoreo de la capacidad y desempeño de los recursos informáticos, instalación y configuración de los sistemas, entre otros.

b) Asegurar la segregación de funciones en la operación para reducir el riesgo de un mal uso.

Corresponde a la UTI, registrar, controlar e identificar el impacto de los cambios que se realicen en los procesos de tecnología de la información y comunicaciones y las instalaciones de procesamiento de la información que afecten la seguridad de la información.

11.3. Controles de Personal

11.3.1. Selección

Objetivo: Asegurar que se incorporen requisitos de seguridad en el proceso de selección de personal.

La Unidad de Recursos Humanos debe comprobar los antecedentes del personal que ingresa a laborar en la institución, de acuerdo con las leyes y regulaciones vigentes, independientemente de su modalidad de contratación.

11.3.2. Términos y condiciones del empleo

Objetivo: Asegurar que se incluyan en los contratos las responsabilidades del personal respecto a seguridad de la información.

La Unidad de Recursos Humanos debe:

a) Establecer en los acuerdos contractuales de empleo, cláusulas de confidencialidad, declaración de responsabilidades con respecto a la seguridad de la información, cumplimiento a la política de seguridad de la información y documentos normativos institucionales, cláusulas respecto a las leyes de derecho de autor o protección de datos personales; según corresponda. Dichos acuerdos contractuales deben estar vigentes hasta la finalización del contrato; según sea necesario.

b) Comunicar que el incumplimiento de la Política de Seguridad de la información podrá ser objeto de sanción administrativa disciplinaria, previo procedimiento administrativo disciplinario.

El personal debe:
a) Cumplir con lo dispuesto en las Políticas de Seguridad de la Información; así como con toda normativa relacionada con la seguridad de la información emitida por la UEB.
b) Informar las vulnerabilidades detectadas y violaciones de seguridad de la información al Oficial de Seguridad y Confianza Digital de la UEB o a través de la UTI.

11.3.3 Toma de conciencia, educación y entrenamiento sobre la seguridad de la información

Objetivo: Asegurar que los colaboradores conozcan, sean conscientes y cumplan con sus responsabilidades de seguridad de la información.

La Unidad de Recursos Humanos, en coordinación con la Unidad de Tecnologías de la Información, así como las unidades de organización deben:
a) Liderar la sensibilización y/o concientización de la implementación del SGSI en la UEB.
b) Incluir en el Plan de inducción aspectos de seguridad de la información, en concordancia con las políticas y procedimientos establecidos en la normativa vigente.
c) Incluir en el Plan de Desarrollo de las Personas acciones de capacitación, orientadas al fortalecimiento de los conocimientos sobre las políticas y procedimientos de la institución, así como en las normas legales y mejores prácticas referidas a la seguridad de la información.
d) Difundir mensajes de sensibilización sobre la importancia de la seguridad de la información y de las consecuencias de no cumplir con las políticas de seguridad vigentes.

11.3.4. Proceso disciplinario

Objetivo: Asegurar que los colaboradores comprendan las consecuencias de no cumplir con las políticas y normas de seguridad de la información.

La Unidad de Recursos Humanos debe difundir, a través de la Secretaría Técnica del Procedimiento Administrativo Disciplinario o quien haga sus veces, que el incumplimiento de la Política de Seguridad de la Información podrá ser objeto de sanción administrativa disciplinaria, previo procedimiento administrativo disciplinario; como también los medios de presentación de la denuncia para reportar tal incumplimiento.

11.3.5. Responsabilidades después del cese o cambio de empleo

Objetivo: Proteger los intereses de la UEB durante el proceso de cambio o finalización de empleo por parte de los colaboradores.

El personal, al término de su relación laboral con la UEB, debe poner a disposición de su jefe inmediato (o a quien este designe formalmente), todos los documentos físicos o en formato digital que le fueron entregados o hayan sido generados, como parte del cumplimiento de sus actividades; así como otros activos relacionados con el tratamiento de la información que le fueron entregados.

11.3.6. Acuerdos de confidencialidad o no divulgación

Objetivo: Proteger la información de accesos no autorizados.

Corresponde a los jefes de las unidades de organización identificar a los colaboradores que acceden a información confidencial, reservada o secreta para supervisar la aplicación de los controles de seguridad en el tratamiento de la información a la que acceden, entre ellos, la firma de un acuerdo de confidencialidad.

11.3.7. Trabajo remoto

Objetivo: Proteger la información y los servicios informáticos que utilizan los colaboradores cuando trabajan de forma remota.

La UTI es responsable de habilitar el acceso remoto a la red de datos de la UEB a través de un software VPN, previa autorización del Jefe de la unidad orgánica del colaborador. También debe implementar las medidas necesarias para:

a) Capacitar y concientizar a los usuarios sobre las medidas de seguridad y confianza digital que deben tener para la protección de la información a la que acceden, como la protección de sus credenciales de acceso a los recursos de información y los cuidados en los equipos de cómputo asignados.

b) Verificar que los equipos de trabajo remoto tengan instalado el software VPN, el software antivirus o antimalware, el firewall activado y el sistema operativo actualizado.

Es responsabilidad de los usuarios:
a) Asegurarse que en el sitio donde realizarán el trabajo remoto o teletrabajo sea un ambiente en donde se reduzca la probabilidad de accesos no autorizados a información o recursos.
b) Utilizar redes privadas para el acceso a internet.
c) Verificar que el Sistema Operativo y el antivirus o antimalware del equipo asignado cuente con las últimas actualizaciones.
d) Verificar que los equipos cuenten con bloqueo automático por inactividad.
e) No utilizar otra herramienta de comunicación o de videoconferencia a la establecida por la UEB.
f) Guardar confidencialidad de la información proporcionada por la UEB para la prestación de las labores.

11.3.8. Reporte de eventos de seguridad de la información

Objetivo: Establecer un mecanismo o canal de comunicación para que los usuarios reporten, de manera oportuna, los eventos de seguridad de la información observados o bajo sospecha.

Corresponde a la UTI establecer el canal y el procedimiento para el reporte de los eventos o debilidades de seguridad de la información.

Los colaboradores y proveedores tienen prohibido probar vulnerabilidades de seguridad sospechosas en los servicios informáticos, sistemas de información

y la plataforma tecnológica de la UEB sin la autorización expresa del Jefe de la UTI.

11.4. Controles físicos

11.4.1. Perímetros de seguridad física

Objetivo: Evitar el acceso físico no autorizado, el daño y la interferencia a la información que hace uso la UEB en sus procesos y servicios.

La Oficina de Administración a través de la Unidad de Logística coordina los accesos a fin de prevenir actos ilícitos o incidentes que puedan generar riesgos contra la integridad de los colaboradores, usuarios y patrimonio de la UEB y lo establecido en las disposiciones de control de acceso de personas y vehículos a la UEB, emitidas para tal fin.

11.4.2. Ingreso físico, asegurar oficinas, salas e instalaciones

Objetivo: Evitar el acceso físico no autorizado a las áreas donde se almacena y/o procesa información.

La Oficina de Administración a través de la Unidad de Logística debe dar cumplimiento a las disposiciones de Control de Acceso de Personas y Vehículos vigente con la finalidad de garantizar la seguridad de los colaboradores, usuarios y los bienes patrimoniales de la sede central de la UEB.

El personal de la UEB, proveedores y el personal de terceros autorizados, deben portar siempre su identificación (fotocheck o pase especial de ingreso) en un lugar visible al permanecer en las instalaciones de la UEB, incluyendo el Micro Centro de Datos. Corresponde a los responsables de las unidades de organización verificar que las personas dentro de las instalaciones bajo su responsabilidad cumplan con portar su identificación.

11.4.3. Supervisión de la seguridad física

Objetivo: Monitorear continuamente las áreas o instalaciones de almacenamiento y/o procesamiento de información para detectar o disuadir el acceso no autorizado e identificar riesgos que puedan afectar los activos.

La Oficina de Administración de la UEB, en coordinación con la UTI y las unidades de organización responsables de las instalaciones de procesamiento y/o almacenamiento de información, deben tomar las acciones para instalar controles que permitan monitorear las actividades dentro de las instalaciones de procesamiento de información como por ejemplo sistemas de video vigilancia.

11.4.4. Protección contra amenazas físicas y ambientales

Objetivo: Disminuir la probabilidad y/o el impacto de las consecuencias originadas por amenazas físicas o ambientales a la infraestructura.

La Oficina de Administración, así como las unidades de organización responsables de las instalaciones de procesamiento y/o almacenamiento de información, deben tomar las acciones para:

a) Realizar evaluaciones de riesgo a las instalaciones de procesamiento y/o almacenamiento de información que permita identificar las amenazas físicas y ambientales a las que están expuestas, por ejemplo, incendio, inundación, disturbios civiles, entre otras, según lo establecido en los planes correspondientes de la UEB.
b) Implementar los controles adecuados para el tratamiento de los riesgos identificados e informar para la actualización del plan o situaciones no contempladas en el mismo.
c) Realizar pruebas periódicas y/o revisiones a los controles ambientales implementados como sensores de humedad, detectores de humo, entre otros.

11.4.5. Trabajo en áreas seguras

Objetivo: Implementar medidas de seguridad que permitan trabajar en áreas protegidas contra daños e interferencias no autorizadas.

La Oficina de Administración, a través de la Unidad de Logística de la UEB, debe:

a) Verificar la operatividad de los extintores (de acuerdo al tipo de material que existan en el ambiente) y sistema de alarma contra incendios.
b) Dar cumplimiento a lo establecido en las disposiciones de control de acceso de personas y vehículos a la UEB, de tal manera que se minimice el riesgo de ingreso de material o equipo peligroso a las instalaciones o la salida de un activo de información sin autorización.

Los responsables de las unidades de organización de la UEB deben:
a) Asegurar que los proveedores y terceros que accedan a las instalaciones de tratamiento de información sensible solo usen el material estrictamente necesario para llevar a cabo las actividades acordadas, así como no ingresen sin la presencia del personal a cargo o su representante.
b) Asegurar que las puertas y ventanas exteriores e interiores estén protegidos contra accesos no autorizados, sobre todo en horas no laborables.
c) Asegurar que los ambientes de procesamiento de la información sensible, posean una infraestructura física adecuada, que impida el vandalismo, sabotaje y robo.
d) Evaluar periódicamente los riesgos internos y externos de los ambientes u oficinas donde se custodien y conserven el acervo documental producido y/o recibido como partes de sus funciones y actividades, y reportarlo de acuerdo a los procedimientos establecidos.
e) Deben requerir, a la Oficina de Administración, la implementación y mantenimiento del sistema de detección y/o extinción de incendio, del tipo adecuado a los materiales combustibles o inflamables que existan o se manipulen en los ambientes u oficinas de tratamiento de información.

La UTI en coordinación con la Oficina de Administración, en el marco de sus competencias, son responsables de programar la limpieza y mantenimiento necesario para asegurar la correcta funcionalidad de cada uno de los elementos del Micro Centro de Datos de la Entidad. Para el caso de los repositorios archivísticos dichas actividades de programación corresponden a la Oficina de Administración también en coordinación con las unidades de organización de la UEB.

11.4.6. Escritorio y pantalla limpios

Objetivo: Reducir los riesgos de acceso no autorizado, pérdida y daño a la información ubicada en los escritorios, pantallas y en otros lugares accesibles.

La UTI debe implementar controles que permitan que:

Pantalla Limpia y escritorio limpio

a) El usuario (persona autorizada) al ausentarse de su estación de trabajo o del equipo portátil asignado, bloquee la pantalla (haciendo uso de las teclas CRTL + ALT + SUPR o Tecla Windows + L), para impedir el acceso de personas no autorizadas a los sistemas de información que maneja, la cual se podrá desbloquear solo con su contraseña.
b) Si el usuario se ausenta por un periodo superior a los cinco (05) minutos, la política de pantalla limpia llevará a la estación de trabajo o equipo portátil al modo "bloqueado", que será desbloqueado solo con su contraseña.
c) Si el usuario se ausenta por un periodo superior a los treinta (30) minutos, la política de pantalla limpia lleva a la estación de trabajo o equipo portátil a modo "suspendido" y "bloqueado". Se podrá desbloquear solo con su contraseña.
d) Las estaciones de trabajo y equipos portátiles deben usar el fondo de pantalla institucional.
e) Las impresoras, escáneres y fotocopiadoras deben estar protegidas de uso no autorizado.

Es responsabilidad de los usuarios:

a) Cuando no se encuentre en su lugar de trabajo, su escritorio no deberá exponer documentos impresos, así como los soportes de almacenamiento de datos (CD, DVD, Disco Duro Externo, USB, y medios removibles en general), que contengan información reservada o confidencial. También estos deben ser retirados del escritorio o de otros lugares (impresoras, fotocopiadoras, escáneres, etc.), para evitar el acceso no autorizado a los mismos.
b) Los documentos impresos y soportes deben ser custodiados de forma segura, de acuerdo con la forma de clasificación de la información que corresponda.
c) Las pizarras que contengan información reservada y/o confidencial deben borrarse.
d) Asegurar que el escritorio del sistema operativo (Windows) no contenga iconos con acceso directo a documentos o carpetas en donde se tenga información con clasificación confidencial, reservada o secreta.
e) Reiniciar los equipos de cómputo y accesorios asignados periódicamente.

11.4.7. Ubicación y protección de los equipos

Objetivo: Reducir los riesgos de accesos no autorizados y daños a los equipos, así como amenazas físicas y ambientales.

La UTI debe implementar controles que permitan:
a) Evitar la apertura de los equipos informáticos. Solo el personal de soporte técnico de la UTI podría hacerlo en caso corresponda.
b) La apertura de equipos debe estar controlada con etiquetas o algún tipo de hardware de seguridad.

Para el caso de los equipos ubicados en el Micro Centro de Datos de la UEB corresponde a la UTI monitorear las condiciones ambientales como la temperatura y humedad que puedan afectar el funcionamiento de los equipos.

11.4.8. Seguridad de los activos fuera de las instalaciones

Objetivo: Reducir los riesgos de pérdidas, daños y robos de los equipos fuera de las instalaciones de la UEB.

La Unidad de Logística debe mantener los registros de control de los equipos de cómputo que son retirados de las instalaciones de la UEB.

La UTI debe aplicar controles de seguridad de la información en los equipos a utilizarse fuera de las instalaciones de la institución como mecanismos que permitan el cifrado de la información confidencial, reservada o secreta contenida en los equipos de cómputo.

Es responsabilidad de los usuarios:
a) No dejar sus equipos de cómputo y medios de almacenamiento sin vigilancia o en lugares públicos.
b) No exponer los equipos de cómputo a altas temperaturas o condiciones ambientales que puedan afectar su funcionamiento.

11.4.9. Medios de almacenamiento

Objetivo: Garantizar que la información de los medios de almacenamiento es usada, modificada, eliminada o destruida de acuerdo con su clasificación.

Es responsabilidad de los usuarios:
a) Almacenar los medios de almacenamiento en un área segura de acuerdo con la clasificación de la información.
b) Realizar y/o solicitar a la UTI, la copia de respaldo de la información contenida en los medios de almacenamiento para evitar su pérdida.
c) En caso de reutilizar los medios de almacenamiento, solicitar a la UTI el borrado seguro de la información antes de su reutilización.
d) Antes de la eliminación o desecho de un medio de almacenamiento solicitar a la UTI, el borrado seguro.

11.4.10. Servicios de suministro de apoyo

Objetivo: Reducir los riesgos de pérdida o daño de la información, así como la interrupción de servicios de la UEB relacionadas a la falla o corte de servicios de electricidad, telecomunicaciones, entre otros.

La Oficina de Administración, dentro del marco de sus competencias y en coordinación con la UTI, debe:
a) Coordinar los mantenimientos de los equipos de respaldo de energía eléctrica (UPS) para asegurar el funcionamiento de los componentes del Micro Centro de Datos, ante la pérdida del servicio de suministro eléctrico.
b) Asegurarse que los equipos de respaldo de energía eléctrica se inspeccionen y prueben periódicamente para garantizar su correcto funcionamiento.

La UTI debe solicitar la contratación de un servicio de conexión a Internet de contingencia que permita la operatividad de los servicios informáticos de la UEB ante la interrupción del servicio de conexión principal.

11.4.11. Seguridad del cableado

Objetivo: Reducir los riesgos de pérdida, daño o robo de la información, así como la interrupción de servicios de la UEB relacionadas al cableado de comunicaciones y/o datos.

La UTI debe implementar controles que permitan asegurar que los cables que transportan datos se encuentren debidamente protegidos contra la interceptación, interferencia o posibles daños.

11.4.12. Mantenimiento de equipos

Objetivo: Reducir los riesgos de pérdida o daño de la información, así como la interrupción de servicios de la UEB relacionadas a la falta de mantenimiento de los equipos.

La UTI debe:

a) Programar y realizar en forma periódica mantenimientos preventivos de los equipos informáticos de los colaboradores de la institución de acuerdo con las recomendaciones del fabricante y las buenas prácticas.
b) Asegurar que se efectúe el mantenimiento de los equipos informáticos que conforman la infraestructura de tecnología del Micro Centro de Datos de la UEB como son equipos de servidores, switches, UPS, sistema de aire acondicionado de precisión, entre otros.

11.4.13. Eliminación segura o reutilización de equipos

Objetivo: Evitar la fuga de información de los equipos que se eliminarán o reutilizarán en la UEB.

La UTI debe:

a) Asegurar que la información clasificada como no pública, almacenada en los medios de almacenamiento que van a ser reutilizados, reemplazados o puestos a disposición (baja), sea borrada de manera segura; así como también en el caso que contengan software propietario.
b) Retirar las etiquetas y marcas, que identifican a la UEB, de los equipos o medios de almacenamiento antes de ser puestos a disposición para donación o eliminación.
c) De acuerdo a una evaluación de riesgos de acceso a información no pública, determinar si los medios de almacenamiento deberían destruirse físicamente.

Corresponde los responsables de las unidades de organización que, en el caso que se requiera eliminar documentos físicos que ya no se utilicen, estos deben ser destruidos, por ejemplo, triturados, para evitar que puedan ser reconstruidos.

11.5. Controles tecnológicos

11.5.1. Dispositivos terminales del usuario

Objetivo: Proteger la información almacenada, procesada o accesible desde los equipos de cómputo asignados a los usuarios.

La UTI debe:

a) Mantener un inventario actualizado de los equipos de cómputo de la UEB detallando sus características, el software instalado, el usuario asignado y la ubicación del equipo.

b) Restringir la instalación de software en los equipos de cómputo sólo a los usuarios Administradores.
c) Implementar los procedimientos y herramientas que permitan proteger la información y los equipos de cómputo, como:

- Controles de acceso mediante métodos de autenticación como contraseñas, acceso biométrico, entre otros.
- Actualización periódica del sistema operativo y el software instalado en los equipos.
- Cifrado de la información confidencial o reservada.
- Software de protección contra malware.
- Bloqueo automático por tras un periodo de inactividad de cinco (5) minutos.
- Restricción de acceso a los usuarios a servicios o páginas en Internet de dudosa procedencia, violencia, terrorismo, entre otras.
- Restricción en el uso de dispositivos de almacenamiento externo, entre otros.

Corresponde al Oficial de Seguridad y Confianza Digital:
a) Dar a conocer las políticas y procedimientos de seguridad establecidos en la UEB, así como las responsabilidades de los usuarios en seguridad de la información.
b) Concientizar a los usuarios sobre las amenazas más comunes a la seguridad de la información.

Uso de dispositivo personales (o BYOD por sus siglas en ingles Bring Your Own Device)

Todo dispositivo personal que se utilizará para el tratamiento de la información laboral de la institución, con conexión a la red de datos de la UEB, acceso a los sistemas de información o servicios informáticos, debe tener la autorización del Jefe de la Unidad de organización al que pertenece el usuario y del Jefe de la UTI. También debe cumplir las políticas de seguridad de la información de la UEB que se indican para los equipos de cómputo de usuario final de la UEB.

Adicionalmente el usuario deberá:

a) Evitar la conexión del equipo de cómputo a redes de datos públicas para acceder a sistemas de información o servicios informáticos de la UEB.
b) No dejar el equipo de cómputo desatendido.
c) No instalar aplicaciones o software que pongan en riesgo la información confidencial o los servicios de la UEB.
d) No utilizar aplicaciones que generen un alto consumo de los servicios de la UEB, como el servicio de internet, entre otros.

La UTI debe verificar el cumplimiento de las políticas de seguridad de la información en los dispositivos personales antes de brindarle acceso a los servicios informáticos de la UEB, así como realizar verificaciones inopinadas del cumplimiento de las políticas.

11.5.2. Derechos de acceso privilegiados

Objetivo: Mantener el control de la asignación y el uso de derechos de acceso privilegiados a los activos de información.

La UTI debe establecer un procedimiento para la asignación y uso de cuentas de acceso privilegiadas. Este procedimiento debe considerar:

a) Que cada responsable o custodio de los activos de información mantenga un inventario actualizado de los usuarios con acceso privilegiado o de usuario administrador.
b) Mantener evidencia de la asignación de accesos privilegiados, así como de la comunicación de sus responsabilidades y el cumplimiento de las políticas de seguridad de la información.
c) Que no se comparta o vincule una identidad o cuenta de acceso privilegiado con varias personas.
d) Proteger la información de autenticación de las cuentas de acceso privilegiado para asegurar su uso ante una indisponibilidad de un usuario administrador de un activo crítico.
e) Requerir, si el servicio así lo permite, dos o más factores de autenticación para una cuenta de acceso privilegiado a un activo de información crítico, por ejemplo, directorio activo, base de datos.
f) Se debe considerar que las cuentas de acceso privilegiadas son solo para las tareas de administración de los activos de información. Para las actividades diarias como revisión del correo electrónico, uso de aplicativos o sistemas de información o navegación en internet, el personal deberá contar con otra cuenta de acceso.

Corresponde al Oficial de Seguridad y Confianza Digital, verificar el cumplimiento del procedimiento de asignación de accesos privilegiados, así como revisar trimestralmente las cuentas de acceso de los administradores de los sistemas de información.

11.5.3. Restricción de acceso a la información

Objetivo: Evitar accesos no autorizados a la información y/o activos de la UEB.
La UTI debe asegurar que se implementen los controles de acceso a la información como:

a) Accesos a los sistemas de información y servicios informáticos de la UEB mediante mecanismos de autenticación.
b) No permitir el acceso a información sensible mediante los sistemas de información o servicios a identidades de usuario desconocidas o de forma anónima.
c) Permitir la restricción de accesos a los datos o información, así como a las acciones que puede realizar sobre ellos.
d) Mecanismos para proteger la información contra cambios, copias y distribución no autorizada, como uso de credenciales fuertes, restringir accesos por periodos de tiempo o ubicación, uso del cifrado para información confidencial, registro de quien accede a la información, cuando y desde donde, entre otros.

11.5.4. Acceso al código fuente

Objetivo: Evitar accesos no autorizados, cambios no intencionales y/o maliciosos en el código fuente de los aplicativos o sistemas de información de la UEB, así como proteger la disponibilidad del código fuente.

La UTI debe incluir, de ser el caso, en las disposiciones de desarrollo de software lo siguiente:

a) Restringir el acceso al código fuente, así como a la documentación del proyecto solo al personal y/o terceros involucrados en la construcción del sistema de información o aplicativo, previa autorización del Jefe de la UTI.
b) Se debe almacenar el código fuente en una herramienta centralizada que permita:

c) Controlar los accesos a modo de lectura o escritura y mantener registros de auditoría de todos los accesos y de todos los cambios realizados al código fuente.
d) Controlar las versiones del código fuente y de sus componentes asociados como manuales técnicos y documentos del proyecto.
e) Mantener copias de seguridad del código fuente de acuerdo a la programación aprobada por la UTI.

11.5.5. Autenticación segura

Objetivo: Garantizar la autenticación segura de un usuario a los sistemas, aplicaciones y/o servicios que brinda la UEB.

La UTI debe asegurar la implementación de tecnologías o controles de autenticación a los sistemas de información y/o servicios, bajo su gobierno, que considere:

a) El uso de un mecanismo de autenticación fuerte o más de un factor de autenticación, si la tecnología lo permite, para verificar la identidad del usuario con métodos de autenticación adicionales a la contraseña, como el uso de certificados digitales de autenticación, tarjetas inteligentes, tokens o medios biométricos, sobre todo para el acceso a los sistemas críticos de la UEB o aquellos que permiten el acceso a datos personales.
b) De utilizar autenticación biométrica incluir alguna técnica de autenticación alternativa que permita la disponibilidad del acceso en caso de falla.
c) Para los sistemas críticos o que contienen información confidencial, verificar que cuenten con controles para la restricción de acceso a los sistemas de información y servicios por ubicación, IP o por tiempo.
d) En el inicio de sesión a los aplicativos y/o sistemas de información de la UEB no se debe:
    - Brindar mensajes que permitan identificar el dato incorrecto.
    - Mostrar información confidencial o del sistema antes de la autenticación exitosa para evitar exponer información a un usuario no autorizado.
    - Mostrar el texto de la contraseña sin enmascarar mientras esté siendo ingresada por el usuario.
e) Implementar medidas de seguridad para proteger los aplicativos y/o sistemas de información de intentos de inicio de sesión por fuerza bruta, como el uso de captcha, requiriendo el restablecimiento de contraseña después de cinco (5) intentos fallidos o bloqueando al usuario después de diez (10) errores.
f) Almacenar la información de autenticación, tanto de los intentos exitosos como de los fallidos.
g) Configurar el envío de alertas de seguridad al usuario y administradores ante algún incumplimiento de los controles de inicio de sesión.
h) Finalizar las sesiones después de cinco (5) minutos de inactividad del usuario, sobre todo para los sistemas de información públicos o externos a la institución.
i) Transmitir las contraseñas cifradas por la red para evitar que esta sea capturada por ciberdelincuentes.

En el caso de los servicios tecnológicos se deben configurar el uso de mecanismos de autenticación fuertes, si la tecnología lo permite, y otros controles dependiendo de la herramienta y la información que contiene.

11.5.6. Gestión de capacidad

Objetivo: Asegurar que los recursos necesarios para el procesamiento de información como infraestructura tecnológica, recursos humanos, instalaciones, entre otros, satisfagan las necesidades actuales y futuras.

La UTI debe analizar la demanda de capacidad de sus recursos administrados, por ejemplo, monitorear el consumo de recursos de procesadores, memorias, servicios de almacenamiento, servicios de impresión, anchos de banda, servicio de internet, servicios externos requeridos a otras instituciones, tráfico de las redes de datos, entre otros, y realizar proyecciones de crecimiento de manera periódica, con el fin de asegurar el desempeño y capacidad de la plataforma tecnológica.

La UTI debe realizar pruebas de estrés de los sistemas y servicios, previa al pase a producción, para verificar que estos cumplen los requisitos de rendimiento requeridos.

Corresponde a los responsables de las unidades de organización de la UEB, comunicar a la UTI la demanda, incluyendo sus variaciones, de los servicios informáticos de entidades externas como CONGRESO, SUNARP, RENIEC, SUNAT, entre otras, incluyendo la cantidad de usuarios que acceden a un sistema de información.

11.5.7. Protección contra programas maliciosos (malware)

Objetivo: Proteger la información sensible y otros activos de la UEB contra malware o software malicioso.

La UTI debe implementar reglas y controles que detecten el uso de software no autorizado, el acceso a sitios web maliciosos y detección de malware. Estos controles deben considerar:

a) Asegurar que los equipos informáticos cuenten con herramientas de seguridad contra códigos maliciosos y se actualicen periódicamente.
b) Realizar charlas de concientización apropiada a los usuarios y colaboradores, sobre los riesgos a los que estamos expuestos en Internet y cómo afrontar un evento u ocurrencia de infección de virus o malware.
c) Todo equipo que no cuente con una herramienta de protección contra software malicioso, no podrá ser conectado a la red de datos de la UEB.
d) Todo contrato de arrendamiento de equipos informáticos, debe incluir el requisito de una herramienta de protección contra software malicioso.
e) Mantener los sistemas operativos y software, con las últimas actualizaciones de seguridad disponibles (probar dichas actualizaciones en un entorno de prueba previamente si es que constituyen cambios críticos a los sistemas).
f) La plataforma de comunicaciones debe contar con equipamiento de seguridad que otorgue la protección necesaria ante amenazas y controle el tráfico de entrada y de salida para la red de datos de la UEB.

No está permitido por el personal de la UEB:
a) La desinstalación y/o desactivación de software y herramientas de seguridad implementadas por la UTI.
b) Instalar y ejecutar programas ya sean propios u obtenidos a través de internet, correo u otro medio, en los equipos de la institución sin la debida autorización de la UTI.

11.5.8. Gestión de vulnerabilidades técnicas

Objetivo: Prevenir la explotación de vulnerabilidades técnicas. La UTI debe:

a) Mantener un inventario de los activos de información de la infraestructura tecnológica identificando los equipos y sistemas críticos.
b) Programar y realizar el análisis de vulnerabilidades técnicas de los sistemas de información y servicios informáticos críticos, por lo menos una vez al año.
c) Planificar y ejecutar las acciones necesarias para mitigar los riesgos identificados en el análisis de vulnerabilidades, así efectuar la comprobación de la implementación exitosas de estas medidas.

11.5.9. Gestión de la configuración

Objetivo: Que el software, hardware, los servicios y las redes funcionen correctamente y con la configuración de seguridad requerida.

La UTI debe revisar periódicamente y actualizar la configuración del hardware, software, servicios y redes de acuerdo con las buenas prácticas de seguridad definida por los proveedores o las organizaciones de seguridad como el Centro Nacional de Seguridad Digital de la Presidencia del Consejo de Ministros. En la revisión y actualización se debe considerar las nuevas amenazas, debilidades, así como su viabilidad y aplicabilidad de la actualización de las versiones de acuerdo a contexto de la UEB.

Solo los administradores del hardware, software, servicios y redes de la UTI, son los responsables de realizar una actualización en la configuración siguiendo el procedimiento de gestión de cambio.

11.5.10. Eliminación de información

Objetivo: Que la información almacenada en los sistemas de información, dispositivos o cualquier otro medio de almacenamiento, cuando ya no se requiera, sea eliminada de manera segura y de acuerdo a las normas legales vigentes.

Los responsables de cada Unidad de organización, en coordinación con la UTI y la Oficina de Administración, deben asegurar que la eliminación de la información clasificada como confidencial o reservada o secreta se realice de manera segura guardando evidencia de la actividad y resultados de la eliminación: información del lugar, fecha, hora, personas que intervinieron, método y herramienta utilizada; conforme a lo establecido en el marco normativo respecto de los documentos archivísticos.

Corresponde a la UTI:
a) Identificar el tipo de eliminación de información (digital) apropiada para cada tipo de medio de almacenamiento, por ejemplo, uso de un software de eliminación segura, desmagnetizado de unidades de disco duro o de disco de almacenamiento externo.
b) Asegurarse que la información confidencial o reservada almacenada en la nube se elimine de forma segura cuando no se requiera.

11.5.11. Enmascaramiento de datos

Objetivo: Proteger y limitar la exposición a los datos secretos, reservados y confidenciales, como los datos personales y sensibles de acuerdo con las normas legales y regulatorias.

Los responsables de las unidades de organización Orgánicas deben proteger la información, incluyendo datos personales y sensibles, a la que acceden de

acuerdo con su clasificación, considerando mecanismos de enmascaramiento, anonimización o disociación.

La UTI debe proteger la información secreta, reservada y confidencial que custodian como los datos de la configuración y direcciones de publicación en Internet de los sistemas de información y servicios informáticos mediante técnicas de enmascaramiento o cifrado.

11.5.12. Prevención de fuga de datos

Objetivo: Detectar y prevenir el acceso, divulgación y extracción de información por personas no autorizadas.

Los responsables de las unidades de organización deben identificar, clasificar y registrar en el inventario de activos la información contenida en los procesos y sistemas de información del cual son propietarios.

La UTI debe implementar herramientas que permitan monitorear y/o prevenir la fuga de datos en servicios como el correo electrónico, transferencia de archivos a través servicios de almacenamiento en la nube, discos de almacenamiento externo, entre otros.

11.5.13. Copia de seguridad de la información

Objetivo: Protección contra la pérdida de datos/información. La UTI debe:

a) Realizar periódicamente copias de respaldo de la información almacenada en los equipos informáticos del Micro Centro de Datos de la UTI; así como efectuar las pruebas de restauración de la información en concordancia con su plan o programa o procedimiento correspondiente y como consecuencias de las mismas, documentar las incidencias que se hayan puesto de manifiesto durante su desarrollo.
b) Asegurar que las copias de respaldo de la información de los equipos informáticos del Micro Centro de Datos de la UEB, sean resguardados en una ubicación externa y lejana a la institución o contratar los servicios de un proveedor de almacenamiento de respaldo de información, que reúna las condiciones adecuadas de acondicionamiento, temperatura y humedad (para asegurar la continuidad de las operaciones); siendo trasladada con los elementos de seguridad adecuados y manteniendo un inventario actualizado de la información almacenada externamente.
c) Realizar las copias de respaldo de la información de los equipos de los usuarios, a solicitud de estos y en la medida de que la capacidad de almacenamiento lo permita.
d) Definir en el plan o programas o procedimiento de copias de respaldo, la periodicidad de respaldo de los sistemas de información, en coordinación con el propietario del sistema de información.
e) Establecer con el propietario de la información, en coordinación con la Oficina de Administración, en lo que respecta al período de retención de la información esencial para la institución, considerando cualquier tipo de requisito para archivar copias que se deberían retener de manera permanente o temporal, de acuerdo con las leyes y normas vigentes y el uso del espacio disponible para el almacenamiento.
f) Definir el periodo de existencia para las copias de seguridad y los procedimientos a seguir para su destrucción definitiva una vez concluido tal período, de acuerdo a lo establecido por el propietario de la información.
g) En coordinación con el propietario de la información y la Oficina de Administración, se debe destruir o eliminar de manera segura la información

de la UEB, cuando ésta deja de ser necesaria y de acuerdo a lo establecido en el marco normativo respecto de los documentos archivísticos.

h) Contar con un programa de mantenimiento preventivo y correctivo para los equipos de respaldo, a efectos de asegurar su correcto funcionamiento.
i) Estimar anticipadamente la cantidad necesaria de recursos requeridos para efectuar las copias de respaldo; en caso de no contar con ello, solicitar su oportuna adquisición.
j) Revisar periódicamente la vigencia tecnológica de los equipos y software utilizados para el respaldo y recuperación de la información e informar algún riesgo identificado al Jefe de la UTI.

Corresponde a los propietarios de los procesos y sistemas de información:

a) Revisar de forma periódica, el valor y la utilidad de la información almacenada para coordinar con la UTI la destrucción o eliminación de la información que ya no es necesaria de acuerdo a las normas legales vigentes.
b) Identificar la información necesaria para sus procesos y servicios a fin de solicitar a la UTI el respaldo de la misma.
c) Corresponde a los Jefes de las unidades de organización, autorizar de manera formal si algún personal bajo su cargo requiere compartir información fuera de la entidad.

Los usuarios:

a) Deben utilizar responsablemente los repositorios de información y recursos compartidos institucionales almacenados en la nube (Microsoft 365) administrados por la UTI, la cual es la plataforma oficial de la UEB.
   - OneDrive: Para almacenamiento temporal y personal institucional (únicamente de carácter laboral), accesible desde el explorador de archivos o vía web.
   - SharePoint Online: Para archivos compartidos entre equipos, áreas o proyectos.

b) No deben almacenar información de trabajo en los discos duros locales (ejemplo C: o D:) de los equipos asignados.
c) No deben utilizar dispositivos externos (discos duros portátiles o memorias extraíbles o similares) como medio principal o de uso permanente para guardar documentos de trabajo.
d) No deben almacenar información personal en los repositorios institucionales (Microsoft 365).

11.5.14. Redundancia de las instalaciones de procesamiento de información

Objetivo: Asegurar la disponibilidad de las instalaciones y procesamiento de la información de acuerdo a los requisitos establecidos.

Los propietarios de los sistemas de información y procesos, en coordinación con la UTI, deben establecer los requisitos de disponibilidad de la información y servicios informáticos y sistemas de información, en el caso de la materialización de situaciones adversas.

La UTI debe:

a) Asegurar la redundancia de los principales componentes tecnológicos (servidores, switches, base de datos y otros), que permitan la continuidad de los sistemas de información que se considere crítico para la institución.
b) Determinar la infraestructura alterna de tecnología de información, la cual debe localizarse geográficamente en un lugar diferente a la sede principal, asegurando que presente seguridad en los siguientes aspectos: calidad de

suelos y del entorno, riesgo de inundación, calidad de la construcción, disponibilidad de servicios básicos, entre otros.

c) Elaborar un plan de recuperación de servicios informático que permita definir las actividades a seguir para la activación de los componentes tecnológicos redundantes, incluyendo las instalaciones de procesamiento alterno. Dicho Plan debe ser probado cada seis meses y sus resultados se deben documentar.

d) Contar con dos proveedores diferentes de los servicios críticos para la continuidad de los sistemas de información, por ejemplo, el servicio de Internet.

11.5.15. Registro

Objetivo: Registrar la información de los eventos (logs) de seguridad de los sistemas de información y servicios informáticos de la UEB con la finalidad de identificar brechas a la seguridad y proponer mejoras.

La UTI, en coordinación con las unidades de organización propietarias de los sistemas de información, debe implementar mecanismos que permitan:

a) Registrar, mantener y revisar periódicamente los eventos (logs) de intentos de accesos exitosos y rechazados, cambios de configuración del sistema, uso de programas privilegiados, desactivación de algunos controles como antivirus, modificación de cuentas privilegiadas, actividades de usuarios con privilegio de administrador, eliminación de información crítica.

b) Registrar para cada evento el usuario, fecha y hora del evento (log), identificación del dispositivo de acceso (dirección Mac), dirección de red o IP de origen, tipo de acción realizada por el usuario, entre otros.

c) Implementar controles que aseguren que los eventos (log) no sean manipulados, tal como la activación de registros de auditoría.

d) Realizar copias de seguridad de estos eventos periódicamente.

e) Implementar controles de protección de privacidad de los datos personales almacenados en los registros de eventos de los sistemas de información.

La UTI debe revisar y analizar, a nivel de muestra, los registros almacenados de los eventos para identificar actividades inusuales o sospechosas que puedan poner en riesgo la información o los servicios de la UEB.

11.5.16. Actividades de Monitoreo

Objetivo: Detectar eventos anómalos o posibles incidentes de seguridad de la información en los sistemas de información, servicios informáticos y las redes.

La UTI debe:

a) Identificar los recursos informáticos críticos que deben ser monitoreados, estableciendo una línea base de comportamiento del recurso, la frecuencia de monitoreo y el periodo de retención de las evidencias.

b) Se debe implementar una herramienta que permita monitorear y enviar alertas automáticas de:

- El tráfico de la red y los sistemas de información, entrante y saliente.
- El acceso a los sistemas de información, equipos de la red de datos y demás servicios críticos.
- Uso de recursos como CPU, disco duro, memoria y ancho de banda, incluyendo su rendimiento.
- Así como almacenar y revisar los registros del monitoreo para realizar proyecciones de futuros requisitos de capacidad, que aseguren el

desempeño requerido por los servicios informáticos y sistemas de información.

11.5.17. Sincronización de reloj

Objetivo: Apoyar el análisis de los eventos relacionados con la seguridad y el registro de datos, así como las investigaciones de los incidentes de seguridad de la información.

La UTI debe sincronizar los relojes de todos los sistemas de procesamiento de información y servicios informáticos tomando como referencia una única fuente confiable de transmisión del tiempo, basándose en protocolos estándares de sincronización reconocidos como el Protocolo de Tiempo de Red (PTR o NTP Network Time Protocol) o el Protocolo de Tiempo de Precisión (PTP).

11.5.18. Uso de programas de utilidad privilegiados

Objetivo: Garantizar el uso seguro de los programas o software de utilidad (privilegiados) en la UEB, para minimizar los riesgos de acceso no autorizado, daño a los sistemas, uso inapropiado y divulgación de información sensible.

Toda instalación de programas de utilidad privilegiados en los equipos informáticos de la red de datos de la UEB debe contar con la autorización del Jefe de la Unidad Orgánica en la que labora el usuario y del Jefe de la UTI.

La UTI debe:

a) Mantener un inventario actualizado de los programas privilegiados instalados en la UEB.
b) Establecer controles de acceso en los equipos y servicios informáticos para limitar la instalación y uso de programas privilegiados solo a los usuarios autorizados.

Corresponde a los usuarios que cuentan con la autorización de uso de programas de utilidad privilegiados:

a) Utilizar los programas solo para las actividades autorizadas.
b) Mantener la confidencialidad de la información a la que puedan acceder con dichos programas privilegiados.

11.5.19. Instalación de software en sistemas operativos

Objetivo: Proteger la integridad de los Sistemas Operativos evitando la explotación de vulnerabilidades técnicas.

La UTI debe:

a) Controlar la instalación de sistemas operativos, mediante la restricción de privilegios para evitar incidentes de seguridad de la información y violaciones de derechos de propiedad intelectual.
b) Mantener actualizado los sistemas operativos sobre todo con las actualizaciones referidas a seguridad, evitando el uso de software comercial sin soporte del proveedor.
c) Ejecutar evaluaciones o pruebas antes de instalar actualizaciones de los sistemas operativos.

11.5.20. Seguridad de redes

Objetivo: Proteger la información, los sistemas de información y la infraestructura de redes.

La UTI debe:

a) Gestionar, proteger y conservar la seguridad de los datos en las redes de la UEB.
b) Mantener actualizada la documentación técnica de la red, como los diagramas de red, el inventario de los equipos que conforman la infraestructura tecnológica y la información de su configuración.
c) Establecer controles y medidas especiales para salvaguardar la disponibilidad, confidencialidad e integrar los datos que se transfieren a través de redes públicas, incluyendo los sistemas de información, por ejemplo, implementando equipos como firewall, sistemas de detección y prevención de intrusiones, entre otros.
d) Detectar, restringir y autenticar la conexión de equipos y dispositivos a la red.
e) Implementar sistemas de autenticación a la red que requieran más de un factor de autenticación de usuario.
f) Implementar procedimientos que permitan reducir las vulnerabilidades técnicas en las redes, como, deshabilitar los protocolos de red vulnerables y el endurecimiento (hardening) de red y servidores.
g) Registrar las acciones o vulnerabilidades que puedan afectar la seguridad de la información de las redes y realizar su atención.

El Oficial de Seguridad y Confianza Digital deberá verificar la atención a las vulnerabilidades de red identificadas.

11.5.21. Seguridad de servicios de red

Objetivo: Garantizar el uso seguro de los servicios de red. La UTI debe:

a) Implementar procedimientos de autorización y controles de autenticación para acceder a las redes y servicios en red.
b) La conexión a la red de datos y servicios de red de la UEB de manera remota se debe realizar a través de una Red Privada Virtual (VPN) u otro mecanismo que permita establecer una línea segura y cifrada entre la red de datos de la UEB y el equipo de cómputo del usuario.
c) Monitorear, revisar y auditar regularmente todos los servicios de red incluyendo los provistos por terceros.
d) Analizar las vulnerabilidades y aplicar las correcciones de seguridad de manera oportuna.
e) Planificar y autorizar los cambios en los servicios de red, incluyendo los que proveen terceros, considerando los riesgos que podrían generar, en el marco de la normativa aplicable.
f) Identificar e incluir en los acuerdos de servicios de red y/o los términos de referencia (para los servicios tercerizados) los mecanismos de seguridad, niveles de servicio y requisitos de gestión de los servicios de red.
g) Verificar la implementación de los mecanismos de seguridad, niveles de servicio y requisitos de gestión de los servicios de red.

Los usuarios de la red deben:

a) Utilizar los recursos de red de manera responsable y ética, evitando acciones que puedan poner en riesgo la seguridad de las redes.
b) Reportar a la UTI, a través de los procedimientos establecidos, cualquier incidente de seguridad, vulnerabilidad o sospecha de actividad maliciosa.

11.5.22. Segregación de redes

Objetivo: Segregar las redes y controlar el tráfico entre ellas en función de las necesidades de la UEB y la seguridad de la información.

La UTI debe:

a) Segregar las redes en función de los niveles de confianza, criticidad y sensibilidad de la información, sistemas y servicios que contienen.
b) Configurar firewalls, routers y otros dispositivos para limitar el acceso entre las diferentes zonas de la red, por ejemplo, el acceso a los recursos y datos sensibles que permitan reducir el impacto potencial de un incidente de seguridad.

11.5.23. Filtrado de la web

Objetivo: Controlar el acceso a los sitios web externos o no autorizados para proteger la información y los sistemas de información de malware.

La UTI debe:

a) Establecer niveles para el acceso a los sitios web, en función a lo que necesitan para la atención a sus funciones.
b) Implementar restricciones de acceso a los usuarios a sitios web que tienen la función de carga de información, que contienen información ilegal o son conocidos como sospechosos, por ejemplo, aquellos que distribuyen malware, phishing o que son declarados como peligrosos por el CNSD de la PCM.
c) Implementar filtro de contenidos y software antispam.

La UTI en coordinación con el Oficial de Seguridad y Confianza Digital, deben capacitar y concientizar a los servidores y terceros de la UEB en el uso seguro y responsable del Internet.

Los usuarios deben:

a) Utilizar responsablemente el servicio de internet institucional, evitando la navegación en páginas web de contenido malicioso, pornográfico, terrorismo, violencia, ocio, entre otras que no sean acorde al desempeño de sus funciones y perjudique o degrade o sature o consuma en exceso el servicio de internet.
b) Utilizar los navegadores web instalados por la UTI, por lo que está prohibido el uso de complementos o extensiones o addons que genere un salto a los controles de filtrado web.

11.5.24. Uso de criptografía

Objetivo: Asegurar el uso apropiado y efectivo de la criptografía para proteger la confidencialidad, autenticidad e integridad de la información de acuerdo a las normas legales vigentes.

El personal de la UEB debe remitir de manera encriptada la información electrónica cuya clasificación no sea pública, en el caso de ser requerida; previa autorización de su propietario. Para ello puede solicitar el apoyo técnico de la UTI, de ser necesario.

El uso de certificados digitales se debe realizar cumpliendo las normas legales vigentes y las condiciones de uso establecidas por la Entidad de Certificación Digital.

La UTI debe:

a) Asegurar que los controles criptográficos cumplan con estándares nacionales e internacionales, evitando el uso de controles con algoritmos de encriptación considerados como débiles, obsoletos o inseguros.
b) Implementar métodos criptográficos que permitan la integridad y confidencialidad de la información desde su transmisión hasta su recepción, como la publicación de servicios y sistemas de información a través de un certificado digital SSL (Secure Sockets Layer).
c) Previa evaluación de riesgos, determinar la necesidad de encriptar la información que no sea de carácter público, incluyendo la referida a datos personales, almacenados en las bases de datos de la UEB.

11.5.25. Ciclo de vida de desarrollo seguro

Objetivo: Garantizar que la seguridad de la información se diseñe e implemente en el ciclo de vida de desarrollo de los sistemas de información y aplicaciones de la UEB.

La UTI debe incluir en los lineamientos o metodología de desarrollo de software, controles que permitan el desarrollo seguro de los sistemas de información y aplicaciones en cada una de las etapas del ciclo de vida del software. Entre estos controles se debe considerar:

a) La segregación de funciones en la asignación de los roles para cada una de las etapas del clico de vida del software.
b) Implementar repositorios seguros para resguardar y controlar los cambios en el código fuente, la documentación de desarrollo y gestión del proyecto generada e en cada etapa del ciclo de vida del software.
c) Realizar el análisis de las vulnerabilidades técnicas para detectar problemas de seguridad en los sistemas de información y aplicaciones antes del pase a producción.
d) Incluir en todos los programas críticos, la generación de registros de eventos de auditoría.
e) Capacitar a los desarrolladores en cómo prevenir, encontrar y corregir vulnerabilidades en el desarrollo de software.

11.5.26. Requisitos de seguridad de la aplicación

Objetivo: Asegurar que los requisitos de seguridad se identifiquen, especifiquen y atiendan en el desarrollo o adquisición de sistemas de información o aplicaciones.

La UTI en coordinación con el Oficial de Seguridad y Confianza Digital, debe:

a) Incluir en los requisitos de los nuevos sistemas de información o en las propuestas de mejoras de los sistemas de información existente; aquellos relacionados con la seguridad de la información, desde las etapas iniciales del proyecto y conforme al alcance de la UTI.
b) Proteger la información involucrada en los servicios de aplicaciones a través de redes públicas.
c) Proteger la información involucrada en las transacciones de servicios de las aplicaciones, para prevenir transmisión incompleta, ruteo incorrecto, alteración o divulgación no autorizada de mensajes, ya sea interna o externa a la UEB.

d) Verificar que los cambios solicitados formalmente por los propietarios de la información no causen riesgos de seguridad y de ocurrir un incidente de seguridad en la implementación de un cambio, debe deshabilitarse para su posterior subsanación.
e) Determinar las pruebas de calidad y seguridad de software a aplicar de acuerdo a la criticidad del sistema y del cambio.

11.5.27. Arquitectura de sistemas seguros y principios de ingeniería

Objetivo: Asegurar que los sistemas de información o aplicaciones se diseñen, implementen y operen de manera segura.

La UTI debe:

a) Establecer, documentar y aplicar principios de ingeniería segura en el desarrollo de los sistemas de información.
b) Diseñar la seguridad en todas las capas de la arquitectura de un sistema de información (negocios, datos, aplicaciones y tecnología).
c) En caso de uso de nueva tecnología, se deben analizar e identificar los riesgos de seguridad.

11.5.28. Codificación segura

Objetivo: Garantizar que el software se escriba de forma segura, reduciendo la cantidad de posibles vulnerabilidades de seguridad de la información en los sistemas de información implementados en la UEB.

La UTI debe establecer pautas para la codificación segura. Dentro de estos deben incluir que:

a) Los desarrolladores y analistas sigan las mejores prácticas de codificación segura y estándares de seguridad reconocidos para el desarrollo y mantenimiento de software, por ejemplo, el uso de frameworks y librerías de seguridad reconocidas para mitigar las vulnerabilidades comunes como las difundidas por la Open Web Application Security Project - OWASP y su publicación de los diez riesgos de seguridad más importantes (Top 10).
b) Implementar controles de validación y sanitización de datos de entrada para prevenir ataques de inyección de código.

11.5.29. Pruebas de seguridad en desarrollo y aceptación.

Objetivo: Validar que los sistemas de información y aplicaciones cumplen los requisitos de seguridad definidos antes de su implementación.

La UTI debe:
a) En caso corresponda, validar los sistemas de información y aplicaciones durante todas las etapas del desarrollo de software.
b) Considerar pruebas unitarias, pruebas calidad funcional y no funcional (por ejemplo: validación de datos y rendimiento), pruebas de seguridad y pruebas de aceptación por el usuario.
c) En las pruebas de seguridad incluir pruebas de autenticación de usuario, restricción de acceso, codificación y configuración segura.
d) Determinar el alcance y los tipos de pruebas en la etapa de análisis en función a la importancia, la naturaleza del sistema y el impacto del cambio.

e) De preferencia implementar herramientas automatizadas para identificar vulnerabilidades.
f) Verificar la corrección de los defectos relacionados con la seguridad.

11.5.30. Desarrollo subcontratado

Objetivo: Asegurar que los lineamientos de seguridad de la información definidos por la UEB para el desarrollo e implementación de los sistemas de información y aplicaciones se implementan también en los servicios contratados.

Los proveedores de desarrollo, según corresponda, deben cumplir con las normas y requisitos de seguridad de la información establecidos por la UEB, así como colaborar en la identificación y atención de riesgos de seguridad de la información durante el proceso de desarrollo.

La UTI debe:
a) Incluir en los términos de referencia de los sistemas desarrollados o modificados por terceras partes, que deben cumplir con lo establecido en esta política de seguridad y la normativa de la UEB.
b) Establecer acuerdos previos con todos los terceros, que resguarde la propiedad intelectual y asegure los niveles de confidencialidad de la información manejada en los proyectos.
c) Implementar un proceso de supervisión, revisión y aprobación de los entregables para asegurar la calidad y seguridad de los sistemas y aplicaciones entregados.

El Oficial de Seguridad y Confianza Digital, en coordinación con los propietarios del sistema y los desarrolladores, deben evaluar los riesgos asociados al desarrollo tercerizado para verificar que se cuentan con los controles de seguridad adecuados.

11.5.31. Separación de los entornos de desarrollo, prueba y producción

Objetivo: Proteger los entornos de desarrollo, prueba y producción. La UTI debe:
a) Mantener separados, en la medida que las capacidades técnicas lo permitan, los ambientes de desarrollo, pruebas y producción.
b) Establecer las actividades a seguir para el despliegue del software desde el ambiente de desarrollo, prueba hasta el ambiente de producción.
c) No permitir la ejecución de pruebas en entornos de producción, salvo excepciones aprobadas por el Jefe de UTI y el propietario del sistema.
d) No utilizar en los ambientes de desarrollo y pruebas, datos confidenciales o personales similares al ambiente de producción. De ser necesario se deben aplicar procedimientos de enmascaramiento o anonimización,
e) Implementar en los ambientes de desarrollo y pruebas las actualizaciones de seguridad del software utilizado y controlar el acceso solo a personal autorizado por el Jefe de la UTI.
f) Proteger el acceso a la información de producción de acuerdo a su clasificación.

11.5.32. Gestión de cambios

Objetivo: Preservar la seguridad de la información al ejecutar cambios en los sistemas de información y la infraestructura tecnológica.

La UTI debe:

a) Establecer e implementar un procedimiento para controlar el ingreso de nuevos sistemas o las actualizaciones o cambios en los sistemas existentes. Dicho procedimiento debe tener actividades de identificación, evaluación, autorización, implementación, revisión de los cambios (incluyendo la documentación) y comunicación de su implementación a las partes pertinentes.
b) Requerir que todo cambio tenga documentación que indique la descripción detallada del cambio, el impacto esperado, los riesgos asociados, los recursos necesarios y las actividades y condiciones a seguir en caso sea necesario realizar su reversión.
c) Establecer el procedimiento a seguir en caso de cambios de emergencia ante una contingencia.
d) Ejecutar el respaldo de la versión o solución anterior, previo a la implementación de un cambio.

11.5.33. Información de las pruebas

Objetivo: Garantizar la relevancia del proceso y resultados de las pruebas, así como la protección de los datos e información utilizada en ellas.

La UTI debe:
a) Realizar las pruebas de los sistemas de información en un ambiente controlado y con los datos seleccionados para tal fin.
b) Implementar medidas de confidencialidad para proteger la información de prueba de acuerdo a su clasificación, como la encriptación de datos sensibles y la restricción de acceso solo a personal autorizado.
c) El personal que participa en la ejecución de las pruebas no debe ser el mismo que participó en su desarrollo.
d) Documentar los resultados de las pruebas realizadas.

11.5.34. Protección de los sistemas de información durante las pruebas de auditoría

Objetivo: Minimizar el impacto de las actividades de auditoría y aseguramiento en los sistemas operativos, sistemas de información y servicios informáticos de la UEB.

Toda auditoría y revisión a los sistemas operativos, sistemas de información y servicios informáticos debe ser coordinada con la UTI en cuanto al alcance, tipo de evaluaciones y herramientas a utilizar. Asimismo, toda auditoría y revisión debe limitarse sólo a lectura de datos y no está permitido realizar adecuaciones o cambios en la configuración de los sistemas o la infraestructura tecnológica.

La UTI debe:
Coordinar la ejecución de las pruebas de auditoría o revisiones que puedan afectar la disponibilidad de los sistemas fuera del horario laboral y en coordinación con el propietario del sistema o proceso afectado.

XII. RESPONSABILIDADES

12.1. Dirección Ejecutiva

a) Implementar el SGSI en la UEB.
b) Aprobar con Resolución Directoral las Políticas y Objetivos de Seguridad de la Información y sus modificatorias.
c) Designar al Comité de Gobierno y Transformación Digital
d) Designar al Oficial de Seguridad y Confianza Digital de la UEB.

e) Promover la implementación del SGSI de la UEB.

12.2. Comité de Gobierno y Transformación Digital

a) Informar semestralmente al/a la titular de la UEB los avances y dificultades en la operación u operación del SGSI.
b) Asegurar el cumplimiento de las políticas, objetivos, planes, procedimientos y marco normativo en materia de seguridad y confianza digital en la entidad pública.
c) Apoyar al Oficial de Seguridad y Confianza Digital en las actividades relacionadas al SGSI, como la concienciación a los usuarios, dentro del alcance del Órgano y/o Unidad Orgánica al que pertenece.
d) Otras relacionadas con el Gobierno y Transformación Digital de la entidad.

12.3. Líder de Gobierno y Transformación Digital

a) Ejercer el liderazgo del proceso de transformación digital de la entidad.
b) Participar activamente en el Comité de Gobierno Digital.
c) Promover el uso de tecnologías digitales al interior de la entidad para el logro de los objetivos estratégicos.
d) Promover el uso de metodologías de innovación, ágiles u otras para coadyuvar al proceso de transformación digital.
e) Promover una cultura digital al interior de la entidad para el aprovechamiento de las tecnologías digitales y su adaptación al proceso de transformación digital.
f) Otras responsabilidades que se deleguen mediante lineamientos de la Secretaría de Gobierno Digital.

12.4. Oficial de Seguridad y Confianza Digital

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.

12.5. Secretario/a Técnico/a del CGTD

a) Coordinar y articular con el Oficial de Seguridad y Confianza Digital, la implementación, operación, mantenimiento y mejora continua del SGSI del Órgano y/o Unidad Orgánica al que pertenece.
b) Realizar la verificación de los controles de seguridad de la información, así como el cumplimiento de la Política de Seguridad de la Información de la UEB y demás documentos normativos de referidos a seguridad de la información de acuerdo a la programación.
c) Presentar los informes de implementación del SGSI al CGTD
d) Coordinar la implementación y mantenimiento del SGSI en la entidad dentro del alcance de los órganos/unidades orgánicas de su competencia, bajo la dirección del Oficial de Seguridad y Confianza de la UEB.

12.6. Directivo/Jefe

a) Implementar las Políticas de Seguridad de la Información y demás documentos relacionados, dentro de sus áreas de responsabilidad, monitoreando su cumplimiento y reportando al Comité de Gobierno y Transformación Digital periódicamente.
b) Asegurarse que los colaboradores estén informados de sus roles y responsabilidades de seguridad de la información antes que se le conceda acceso a la información y otros activos asociados.

c) Informar a la UTI sobre las deficiencias e incidentes que identifiquen en materia de seguridad de la información tecnológica.
d) Informar a la Oficina de Administración sobre deficiencias o incidentes generadas por fenómenos naturales y/o acción humana.
e) Gestionar que se provean los recursos adecuados para la implementación de los procesos y controles de seguridad de la información.
f) Mantener en el personal las habilidades y calificaciones en seguridad de la información requeridas para cada puesto dentro de su unidad orgánica.

12.7. Oficina de Administración

Planificar, desarrollar, implantar y gestionar el sistema de información, infraestructura tecnológica y telecomunicaciones, para que brinden el soporte de las funciones desarrolladas por las diferentes unidades orgánicas estableciendo políticas, estándares y procedimientos.

12.8. Oficial de Gobierno de Datos

a) Asegurar el uso ético de las tecnologías digitales y datos en la entidad.
b) Garantizar el proceso de toma de decisiones basadas en datos.
c) Gestionar el uso y publicación de datos de la entidad en la Plataforma Nacional de Datos Georreferenciados (GEOPERÚ) para el análisis y toma de decisiones basadas en datos en el territorio.
d) Gestionar la publicación de los datasets más importantes de la entidad en la Plataforma Nacional de Datos Abiertos.
e) Proponer al Comité de Gobierno y Transformación Digital iniciativas de innovación basadas en datos y gestionar y/o coordinar su implementación.
f) Impulsar el intercambio de datos e interoperabilidad entre las entidades.
g) Garantizar el impulso de una cultura basada en datos en la entidad.
h) Promover la implementación de herramientas y soluciones digitales que garanticen la trazabilidad de los datos.
i) Articular y gestionar el uso de datos gubernamentales.
j) Asegurar la calidad e integridad de los datos que contribuya a la creación de valor público.
k) Impulsar y coordinar el modelamiento, procesamiento, análisis y desarrollo de servicios de información de datos gubernamentales y datos abiertos con los responsables de los procesos correspondientes.
l) Coordinar la implementación del Modelo de Referencia de Datos de la entidad.
m) Promover el intercambio de conocimientos en materia de gobierno de datos.
n) Apoyar la gestión de almacenes de datos, procesamiento analítico e implementación y uso de herramientas de procesamiento de grandes volúmenes de datos.
o) Promover el diseño de herramientas computacionales para obtener resultados a partir de los modelos matemáticos propuestos y los datos del problema bajo evaluación.
p) Impulsar la analítica de datos en todas las unidades de organización de la entidad en coordinación con la Unidad de Analítica Avanzada de la Secretaría de Gobierno y Transformación Digital.
q) Coordinar las acciones relacionadas con los proyectos del Centro Nacional de Innovación Digital e Inteligencia Artificial y el Centro Nacional de Datos aplicados en la entidad.
r) Reportar semestralmente a la Secretaría de Gobierno y Transformación Digital de la Presidencia del Consejo de Ministros la implementación y aplicación de las normas en materia de gobernanza y gestión de datos.

12.9. Jefe/a de Oficina de Planeamiento y Presupuesto

Orientar al Oficial de Seguridad y Confianza Digital de la UEB para asegurar una adecuada articulación con los instrumentos de gestión institucional comprendidos en los sistemas administrativos de presupuesto público, planeamiento estratégico, programación multianual y gestión de inversiones.

12.10. Oficial de Datos Personales

a) Es el rol responsable de velar por el cumplimiento de las normas en materia de protección de datos personales en la UEB emitidas por la Autoridad Nacional de Protección de Datos Personales.
b) Comunicar a la Autoridad Nacional de Protección de Datos Personales los incidentes de seguridad de la información de los bancos de datos personales.
c) Coordinar y/o realizar las capacitaciones y concientización sobre el tratamiento y la protección de datos personales gestionados por la UEB.

12.11. Propietario de la Información o activos de información/Dueños de los procesos

a) Clasificar la información de los procesos bajo su responsabilidad y establecer su nivel de criticidad y disposición final. A su vez deberá determinar cuando la información ya no es necesaria el tiempo de retención en coordinación con la Oficina de Administración, en lo que respecta a documentos archivísticos en los diferentes soportes, de acuerdo a lo establecido en el marco normativo respectivo; y en coordinación con la UTI determinar los métodos de destrucción de la información.
b) Participar en la identificación y gestión de los riesgos de información asociados con los activos.
c) Ser responsable por la calidad, consistencia y disponibilidad de los datos, por lo que deberá tomar medidas para minimizar el riesgo por pérdida o exposición de la seguridad de la información bajo su responsabilidad.
d) Autorizar accesos a la información y ratificar periódicamente las decisiones sobre los mismos, así como dar cumplimiento las disposiciones sobre accesos a los sistemas de información.
e) Revisar la clasificación de la información y los accesos de los procesos bajo su responsabilidad periódicamente.
f) Apoyar en la gestión de los incidentes de seguridad de la información según corresponda.

12.12. Jefe de la Unidad de Tecnologías de la Información

a) Informar al Oficial de Seguridad y Confianza Digital de la UEB todo incidente de seguridad digital crítico que afecte los procesos misionales y servicios que brinda la entidad, de forma inmediata.
b) Articular con el Oficial de Seguridad y Confianza Digital de la UEB la implementación de controles de seguridad de la información.
c) Coordinar la gestión de incidentes de seguridad digital.

12.13. Custodios de la Información

a) Preservar y proteger la información que le ha sido confiada en custodia.
b) Cumplir con las Políticas de Seguridad de la Información de la UEB y los especificados por el propietario de la información.

c) Realizar conjuntamente con los propietarios de la información, pruebas de contingencia y asegurar que todos los empleados y/o usuarios involucrados conozcan sus responsabilidades.

12.14. Personal de la UEB

a) Cumplir las Políticas de Seguridad de la Información de la UEB y documentos relacionados a la Seguridad de la Información de la UEB.
b) Asegurar la protección de los activos de la información involucrados en las labores que realizan.
c) Informar a su inmediato superior y a la UTI sobre las deficiencias e incidentes en materia de seguridad digital.
d) Informar a su inmediato superior y a la Oficina de Administración sobre deficiencias o incidentes generadas por fenómenos naturales y/o acción humana.

XIII. ANÁLISIS DE RIESGOS

El análisis de Riesgos permite determinar las vulnerabilidades de los activos de información de la institución y asimismo clasificarlos por su criticidad. También facilita la implementación de controles para tratar los riesgos asociados a los activos de información.

Se deben clasificar los activos de información de la institución, e identificar las amenazas y vulnerabilidades para luego determinar el nivel de riesgo asociado al activo de información.

El nivel de riesgo identificado tiene una valoración cualitativa de acuerdo a una escala. el riesgo es calculado en base a la probabilidad de ocurrencia de la amenaza y la probabilidad que la amenaza explote la vulnerabilidad.

Los riesgos con niveles Medio, Bajo y Muy Bajo están dentro del nivel de riesgo aceptable por la UEB.

XIV. CUMPLIMIENTO Y CONFORMIDAD

El cumplimiento de la Política de Seguridad de la Información es obligatorio para las unidades de organización de la UEB. En el caso de incumplimiento, la UEB aplicará a los responsables las medidas necesarias según el Reglamento Interno de Servidores Civiles de la UEB o la normativa legal aplicable, de ser el caso.

XV. FINANCIAMIENTO

Cada una de las unidades de organización deberán destinar los recursos necesarios (humanos y económicos) para la implementación, según les corresponda, de los controles de seguridad de la información y de las políticas específicas indicadas en el presente documento.

XVI. VIGENCIA

La Política de Seguridad de la Información de la UEB entra en vigencia a partir de su aprobación y deberá ser revisada, y actualizada en caso corresponda, una vez al año o en caso de producirse modificaciones a las normas legales o cambios significativos en la organización o en los procesos que afecten la seguridad de la información.

XVII. MONITOREO, SEGUIMIENTO Y EVALUACIÓN

La Política de Seguridad de la Información de la UEB, será monitoreada en forma permanente con la revisión de los controles de seguridad, de acuerdo a lo establecido en el numeral XI. Política Específicas.

El seguimiento a la Política de Seguridad de la información se realizará con la medición del cumplimiento de los objetivos de seguridad de la información a través de los indicadores y metas indicados en el numeral XXI. Indicadores y metas del SGSI. Los resultados de esta medición se plasmarán en los informes semestrales realizados por el Oficial de Seguridad y Confianza Digital de la UEB.

La evaluación de la Política de Seguridad de la Información se realizará en forma anual por la Oficina de Administración de la UEB, así como se informará del progreso de la implementación del SGSI.

XVIII. DISPOSICIONES FINALES

Las disposiciones no contempladas en la presente política se regirán de acuerdo a la normativa vigente sobre la materia.

XIX. CONTROL DE CAMBIOS

N°	Texto modificado	Versión	Fecha	Responsable
1	Primera versión de la Política de Seguridad de la Información de la UEB.	01	13.06.20255	Jefe de la Unidad de Tecnologías de la Información

XX. ALINEAMIENTO A LOS OBJETIVOS ESTRATÉGICOS INSTITUCIONALES

		IX. Políticas generales de seguridad de la información				XI. Políticas específicas de seguridad de la información				
Objetivo Estratégico Institucional - PEI	**Acción estratégica**	**9.1**	**9.2**	**9.3**	**9.4**	**11.1 Dirección de la UEB para la seguridad de la información**	**11.2 Controles organizacionales**	**11.3 Controles de personal**	**11.4 Controles físicos**	**11.5 Controles tecnológicos**
OEI 04 Modernizar la gestión institucional del Congreso de la República	AEI 04.04 Gestión administrativa y técnica eficaz en el Congreso de la República.	X	X	X	X	X	X	X	X	X

		IX. Políticas generales de seguridad de la información				XI. Políticas específicas de seguridad de la información				
Actividad Operativa - POI	**Tarea**	**9.1**	**9.2**	**9.3**	**9.4**	**11.1 Dirección de la UEB para la seguridad de la información**	**11.2 Controles organizacionales**	**11.3 Controles de personal**	**11.4 Controles físicos**	**11.5 Controles tecnológicos**
A03 Operación, mantenimiento y mejora del Sistema de Gestión de Seguridad de la Información en la UE 1767	Tarea 1. Realizar la operación, mantenimiento y mejora del Sistema de Gestión de Seguridad de la Información en la UE 1767.	X	X	X	X	X	X	X	X	X

XXI. INDICADORES Y METAS DEL SGSI

Ítem	Objetivo	Acciones para alcanzar los objetivos	Indicador	Propósito del indicador	Método de Cálculo	Frecuencia de medición	Meta	Responsable	Recursos
1	Fortalecer la cultura en seguridad de la información de los funcionarios, servidores y colaboradores de la UEB	Realizar capacitaciones sobre el sistema de gestión de seguridad de la información. Difundir comunicados sobre Seguridad de la Información.	Nivel de cobertura de colaboradores que recibieron cursos, charlas o comunicados de seguridad de la información	>=50%	(# de colaboradores que recibieron cursos, charlas o comunicados de seguridad de la información / # de colaboradores dentro del alcance del SGSI) * 100	Anual	>=50%	Oficial de Seguridad y Confianza Digital	Boletines digitales remitidos por correo electrónico. Charlas / Talleres de Seguridad de la Información.
2	Implementar controles para asegurar la preservación de la confidencialidad, integridad y disponibilidad de la información de acuerdo al Plan de Implementación SGSI de la UEB, así como la continuidad de los servicios.	Realizar seguimiento a la implementación de los controles de seguridad de la información de acuerdo con el Plan de Implementación SGSI.	Nivel de implementación de los controles de seguridad de la información dentro del alcance Plan de Implementación del SGSI	Medir el grado de avance en la implementación de los controles de seguridad de la información	(# de controles implementados en el periodo/ # de los controles que se planearon implementar en el periodo) * 100	Anual	>=20%	Oficial de Seguridad y Confianza Digital	Plan de Implementación del SGSI