MANUAL DE LINEAMIENTOS DE SEGURIDAD DE LA INFORMACIÓN DEL ORGANISMO SUPERVISOR DE LAS CONTRATACIONES DEL ESTADO - OSCE

VERSIÓN 01

Firmado digitalmente por CASTRO LEMA Luis Gerardo FAU 20419026809 soft
Motivo: Doy V° B°
Fecha: 04.10.2024 16:25:59 -05:00

Firmado digitalmente por DIAZ ORTIZ Dan Hilber FAU 20419026809 hard
Motivo: Doy V° B°
Fecha: 04.10.2024 16:29:33 -05:00

Firmado digitalmente por ALCALA NEGRON Christian Nelson FAU 20419026809 soft
Motivo: Doy V° B°
Fecha: 04.10.2024 16:31:21 -05:00

Firmado digitalmente por FLORES VASQUEZ Sandra Patricia FAU 20419026809 soft
Motivo: Doy V° B°
Fecha: 04.10.2024 16:33:10 -05:00

Firmado digitalmente por VERGARA FLORES Franklin Eulolio FAU 20419026809 soft
Motivo: Doy V° B°
Fecha: 04.10.2024 17:12:57 -05:00

ÍNDICE

PRESENTACIÓN

La norma ISO 27001 es el estándar internacional para sistemas de gestión de la seguridad de la información en las organizaciones, tanto para la información física como para la digital. Es parte de la familia de estándares ISO 27000, las cuales ayudan a las organizaciones a mantener seguros sus activos de información.

Al respecto, mediante Resolución Ministerial N° 004-2016-PCM, se aprobó el uso obligatorio de la Norma Técnica Peruana NTP ISO/IEC 27001:2014 a fin de que las entidades del Estado implementen el Sistema de Gestión de Seguridad de la Información - SGSI.

Sobre el particular, con Resolución N° 087-2020-OSCE/PRE se formalizó la aprobación de la "Política Integrada de la Gestión de la Calidad – ISO 9001, Gestión de Seguridad de la Información – ISO 27001 y Gestión Antisoborno – ISO 37001 del Organismo Supervisor de las Contrataciones del Estado - OSCE", mediante la cual la entidad, respecto a la seguridad de la información, asume el compromiso de preservar la confidencialidad, integridad y disponibilidad de la información en cualquiera de sus formas y medios de almacenamiento para el cumplimiento de sus funciones y objetivos.

Por otro lado, la Resolución de Secretaría de Gobierno y Transformación Digital N° 003-2023-PCM/SGTD, establece la implementación y mantenimiento del sistema de gestión de seguridad de la información en las entidades públicas, y en su articulo 1 indica, "Las entidades públicas usan obligatoriamente la Norma Técnica Peruana NTP ISO/IEC 27001 vigente para el análisis, diseño, implementación, operación, mantenimiento y mejora continua del Sistema de Gestión de Seguridad de la Información".

En ese contexto, en el marco de la implementación del SGSI, se ha elaborado el Manual de Lineamientos de Seguridad de la Información que contiene las políticas de seguridad de la información y que tienen por objetivo salvaguardar la confidencialidad, integridad y disponibilidad de la información de la entidad.

En ese sentido, el presente manual es una herramienta que servirá para la mejora continua de del Sistema de Gestión de Seguridad de la Información, tomando como base la Norma Técnica Peruana ISO/IEC 27001:2022.

1. OBJETIVO

El presente documento tiene por objetivo establecer directrices que permitan asegurar la confidencialidad, integridad y disponibilidad de la información del OSCE a través de políticas de seguridad de la información, como parte de la mejora continua del Sistema de Gestión de Seguridad de la Información.

2. ALCANCE

El presente documento es de cumplimiento obligatorio para todo aquel que preste servicios a la institución, indistintamente de su régimen laboral o modalidad contractual.

3. REFERENCIAS NORMATIVAS

En el presente manual se utiliza las siguientes referencias:

3.1 Ley N° 27815, Ley del Código de Ética de la Función Pública.

3.2 Ley N° 29733, Ley de Protección de Datos Personales.

3.3 Decreto Supremo N° 033-2005-PCM, que aprueba el Reglamento de la Ley del Código de Ética de la Función Pública.

3.4 Decreto Supremo N° 003-2013-JUS, que aprueba el Reglamento de la Ley N° 29733, Ley de Protección de Datos Personales.

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

3.6 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.

3.7 Resolución Directoral N° 019-2013-JUS/DGPDP, que aprueba la Directiva de Seguridad de la Información Administrada por los Bancos de Datos Personales.

3.8 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 la seguridad de la información. Requisitos. 3ª Edición. Reemplaza a la NTP-ISO/IEC 27001:2014.

3.9 Resolución de Presidencia N° 177-2019-OSCE/PRE, que aprueba el Reglamento Interno de los/las Servidores/as Civiles - RIS del Organismo Supervisor de las Contrataciones del Estado - OSCE.

3.10 Resolución N° 230-2018-OSCE/SGE, que aprueba la Directiva N° 012-2018-OSCE/SGE "Directiva para regular la implementación del lenguaje inclusivo a nivel escrito, oral y gráfico en el Organismo Supervisor de las Contrataciones del Estado – OSCE".

4. GLOSARIO DE TÉRMINOS

4.1 Términos y Definiciones

- **Active Directory (directorio activo):** Conjunto de servicios que conectan a los usuarios con los recursos de red que necesitan para realizar su trabajo.

- **Activo de Información:** Cualquier información o elemento relacionado con el tratamiento de la misma que, por su importancia para las actividades del OSCE, ha sido declarada como un bien que tiene un valor significativo. Además, es esencial para las actividades de la entidad y, en consecuencia, necesita una protección adecuada.

- **Amenaza:** Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización.

- **Banco de datos personales:** Conjunto organizado de datos personales, automatizado 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.

- **Credenciales:** Información que se requiere para autenticar y verificar la identidad de un usuario. En un entorno digital, puede estar compuesta por "nombre de usuario o ID" y por una "contraseña", u otro factor de autenticación. En un entorno físico, puede ser estar en un fotocheck.

- **Confidencialidad:** Característica de la información de mantener la reserva y no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados.

- **Custodio del activo de información**: Es la/el responsable de resguardar los activos de información que crea, utiliza y/o custodia, así como los medios en los cuales dichos activos residen o se soportan, aplicando los controles de seguridad razonables con la finalidad de minimizar los riesgos respecto a la confidencialidad, disponibilidad e integridad de los mismos en el ámbito de sus funciones en OSCE y en el ámbito del marco contractual en el caso de las/los proveedoras/es de servicios.

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

- **Disponibilidad:** Característica de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada.

- **Dispositivo:** Es un equipo electrónico que almacena y procesa información a través de una aplicación como computadoras personales, laptops, teléfonos inteligentes y tabletas.

- **Encargado de tratamiento de datos personales:** Es toda persona natural, persona jurídica de derecho privado o entidad pública que sola o actuando conjuntamente con otra realiza el tratamiento de los datos personales por encargo del titular del banco de datos

personales en virtud de una relación jurídica que le vincula con el mismo y delimita el ámbito de su actuación.

- **Enmascaramiento:** Es el proceso de ocultar datos modificando sus letras y números originales. Debido a los requisitos normativos y de privacidad, las organizaciones deben proteger los datos confidenciales que recopilan sobre sus clientes y operaciones.
- **Hardware:** Conjunto de elementos físicos o materiales que constituyen una computadora o un sistema informático.

- **Integridad**: Característica de la información relativa a su exactitud y completitud.

- **Incidente de seguridad de la información**: Evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.

- **Lista Blanca:** Es un conjunto de direcciones de correo electrónico, dominios, IP o aplicaciones que han sido verificadas como seguras y, por lo tanto, están autorizadas para acceder a un sistema o red específica.

- **Lista Negra**: Es un tipo de lista de direcciones de correo electrónico, dominios, IP o aplicaciones que han sido identificadas por proveedores de servicios por internet (Internet Service Providers o ISP, por sus siglas en inglés), como no seguras, por lo tanto, no están autorizadas para acceder a un sistema o red específica.

- **Mecanismo Biométrico**: Dispositivo de identificación biométrica que verifica automáticamente la identidad de la persona mediante la medición de alguna de sus características físicas.

- **Medio o mecanismo para el desarrollo de trabajo remoto**: Cualquier equipo o medio informático, de telecomunicaciones y análogos (internet, telefonía u otros), así como de cualquier otra naturaleza que resulte necesario para la prestación de servicios.

- **Memoria USB:** Dispositivo móvil de almacenamiento extraíble que sirve para almacenar y trasladar información.

- **Navegador Web**: Es un programa que permite ver la información que contiene una página web y lo presenta en pantalla permitiendo a la/el usuaria/o interactuar con su contenido.

- **Nivel de Acceso:** Grupos de derechos que las/los usuarias/os necesitan para tratar activos de información.

- **Oficial de Seguridad y Confianza Digital:** Es el/la servidor/a designado/a mediante resolución de Presidencia Ejecutiva, que tiene la responsabilidad de coordinar la implementación, operación, mantenimiento y mejora continua del Sistema de Gestión de Seguridad de la Información (SGSI) en la entidad.

- **Página Web:** Es un documento o conjunto de información que se encuentra en una dirección específica de internet y puede ser accedida a través de un navegador web.

- **Parches:** Archivo que contiene los distintos cambios que se han aplicado a un software para corregir errores, actualizarlo, eliminar secciones antiguas o añadirle funcionalidad.

- **Perfil:** Conjunto de características relacionadas con los roles, privilegios y/o niveles de acceso otorgados a un/a usuario/a sobre un activo de información.

- **Privilegio:** Derecho o permiso para ejecutar un tipo particular de acción o tratar un activo de información.

- **Política**: Intenciones y dirección de una organización, expresada formalmente por su alta dirección.

- **Producto digital:** Herramienta informática, sistema, módulo, aplicación o software desarrollado en el OSCE para disposición de las/los usuarias/os, de manera que pueda atender una problemática o necesidad de usuaria/o o negocio.

- **Propietaria/o de activo de información**: Responsable de la producción, desarrollo, mantenimiento, uso y seguridad del activo de información, según corresponda.

- **Riesgo:** En seguridad de la información, está asociado con el potencial de que las amenazas exploten las vulnerabilidades de un activo de información o grupo de activos de información y, por lo tanto, causen daños a una organización.

- **Rol:** Conjunto de privilegios que se asigna a un/a usuario/a o grupo de usuarias/os.

- **Seguridad de la información:** Es el conjunto de medidas preventivas y reactivas que adopta la organización o sistemas tecnológicos que permiten resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de datos.

- **Sistema de Gestión de Seguridad de la Información:** Conjunto de elementos interrelacionados o interactuantes que utiliza una organización para establecer una política y objetivos de seguridad de la información, basados en un enfoque de gestión del riesgo y la mejora continua.

- **Sitio Web:** conjunto de archivos electrónicos y páginas web referentes a un tema en particular.

- **Software:** Programas informáticos que hacen posible la ejecución de tareas específicas dentro de un equipo de cómputo. Por ejemplo, los sistemas operativos, aplicaciones, navegadores web, juegos o programas.

- **Teletrabajo:** Modalidad especial de prestación de labores, de condición regular o habitual. Se caracteriza por el desempeño subordinado de aquellas sin presencia física de el/la trabajador/a o servidor/a civil en el centro de trabajo, con la que mantiene vínculo laboral. Se realiza a través de la utilización de las plataformas y tecnologías digitales.

- **Tratamiento:** 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 activos de información.

- **Usuarias/os**: Toda persona natural y/o jurídica independientemente de su régimen laboral, modalidad formativa o relación contractual (locadores de servicios y proveedores), que es autorizada por el OSCE para acceder a información y/o hacer uso de los productos digitales, sistemas de información y servicio informáticos de la entidad.

- **VPN (red privada virtual, por sus siglas en inglés):** Conexión protegida al utilizar redes públicas. La VPN cifra su tráfico en internet asegurando la información que se gestiona a través de la misma.

- **Vulnerabilidad:** Debilidad de un activo o control que puede ser explotada por una o más amenazas.

4.2 Abreviaturas

- **CD:** Disco óptico utilizado para almacenar datos en formato digital, consistentes en cualquier tipo de información.

- **DVD:** Disco óptico de mayor capacidad de almacenamiento que un CD, que puede ser usado para guardar datos, incluyendo películas con alta calidad de vídeo y sonido.

- **OSCE:** Organismo Supervisor de las Contrataciones del Estado.

- **OSCD:** Oficial de Seguridad y Confianza Digital.

- **OTI:** Oficina de Tecnología de la Información.

- **OAD:** Oficina de Administración.

- **SGSI:** Sistema de Gestión de Seguridad de la Información.

- **UABA:** Unidad de Abastecimiento.

- **UAST:** Unidad de Arquitectura y Soporte de Tecnologías de la Información y Comunicación.

- **UGDS:** Unidad de Gestión de Desarrollo de Software.

- **UOYM:** Unidad de Organización y Modernización.

- **UREH:** Unidad de Recursos Humanos.

5. POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

Las políticas de seguridad de la información establecidas en el presente manual son de cumplimiento obligatorio para las/los usuarias/os, sujetándose a las acciones correspondientes frente a su incumplimiento.

5.1 POLÍTICA: CONTROL DE ACCESOS

A. Propósito

Establecer lineamientos a fin de que el acceso físico y lógico a los activos de información por parte de las/los usuarias/os sea gestionado, controlado y debidamente autorizado por las/los propietarias/os de los activos de información, salvaguardando su seguridad ante accesos no autorizados.

B. Responsabilidades de la/el usuaria/o:

- Proteger sus credenciales de acceso, tanto física como digitales, a fin de evitar accesos no autorizados.

- Mantener visibles sus credenciales físicas durante su tránsito dentro de la entidad, para facilitar su identificación.

- Cambiar sus contraseñas luego del primer inicio de sesión, así como ante algún indicio de vulnerabilidad y periódicamente, por prevención.

- Seleccionar contraseñas que cuenten con un nivel adecuado de complejidad, siguiendo las siguientes consideraciones:
    - Longitud mínima de ocho (8) caracteres.
    - Combinación de letras mayúsculas, letras minúsculas, números y caracteres especiales.
    - Evitar el uso de palabras comunes o datos personales.

- Asegurar la confidencialidad de sus contraseñas no compartiéndolas y evitando registrarlas en medios físicos o electrónicos.

- Cualquier acción realizada sobre un activo de información, tanto en entornos físicos como en digitales, es responsabilidad de la/lo usuaria/o cuyas credenciales permitió ejecutar la acción.

- Reportar a la/el OSCD ante cualquier hecho que pueda afectar la seguridad de la información, a través del instrumento establecido para la gestión de incidencias de seguridad de la información.

C. Responsabilidades de la/el propietaria/o de activo de información:

- Definir y establecer los perfiles, roles, privilegios y/o niveles de acceso de sus activos de información, de acuerdo a su necesidad.

- Administrar y/o gestionar el acceso a los activos de información, en coordinación con el/los custodio/s de los activos de información.

- Definir como se gestionarán las credenciales de acceso de los los/las usuarios/as a sus activos digitales.

- Autorizar la activación, desactivación o modificación de perfiles, roles, privilegios y/o niveles de acceso a los activos de información.

- Gestionar oportunamente la desactivación de las credenciales de acceso, previo a la finalización del período contractual, cese de personal o cambio de puesto de trabajo, según corresponda.

- En coordinación con el OSCD, gestionar la implementación de controles de seguridad de los activos de información.

- Autorizar las solicitudes de acceso a los activos de información, previa autorización de las/los jefas/es del órgano o unidad orgánica a la cual pertenece la/el usuaria/o.

D. Responsabilidades de la OTI

- Atender las solicitudes de creación o desactivación de credenciales de acceso, de los productos y servicios digitales que gestionan, requeridos mediante los procedimientos y/o formatos establecidos.

- Crear las credenciales de accesos, teniendo en cuenta lo siguiente:
    - El nombre de usuario o ID de la credencial asignada a el/la servidor/a del OSCE debe estar compuesta por caracteres relacionados a su nombre y/o apellidos.
    - El nombre de usuario o ID de la credencial asignada a un/a proveedor/a o tercero, puede estar compuesto por caracteres relacionados con una denominación genérica relacionada al servicio que brinda.

- Desactivar las credenciales de acceso, teniendo en cuenta lo siguiente:
    - Las credenciales de acceso a la red (Active Directory) y del SGD deben ser desactivadas temporalmente cuando el/la servidor/a programe su descanso vacacional, para lo cual la UREH comunicará (vía SGD) a la UAST, las fechas de inicio y fin de dicha desactivación.
    - Cuando el/la servidor/a se desvincule del OSCE, se deben desactivar las credenciales de acceso asignadas a más tardar el último día de labores conforme a lo comunicado por la UREH en el documento de desvinculación.
    - Cuando la/el jefa/e del órgano o la unidad orgánica solicite desactivar las credenciales de acceso asignados a un/a proveedor/a o tercero.

- Contar con un registro de usuarios, que contenga por lo menos nombre de usuario o ID, nombres y apellidos, órgano o unidad orgánica, fecha creación, fecha de cese y estado.

- Bloquear las credenciales de acceso, teniendo en cuenta lo siguiente:
    - Por un lapso mínimo de quince (15) minutos luego de cinco (5) intentos de acceso fallidos, previa evaluación técnica.

- Registro de los intentos de acceso fallidos y exitosos por las/los usuarias/os, previa evaluación técnica.

- Para las contraseñas, tener en cuenta lo siguiente:
  - Cambio de contraseña: al primer inicio de sesión, cada sesenta (60) días y/o cuando lo requieran las/los usuarias/os.
  - Longitud mínima de ocho (8) caracteres.
  - Combinación de caracteres como son: letras mayúsculas, letras minúsculas, números y/o caracteres especiales.
  - Mantener un mínimo de cinco (5) contraseñas en el historial de contraseñas.

- Establecer la programación del bloqueo automático en los dispositivos informáticos luego de un tiempo determinado de inactividad.

E. Lineamientos Generales

- Los requerimientos y atenciones de acceso a los activos de información, tanto para el alta como para la baja, deben se solicitados por la/el jefa/jefe del órgano o unidad orgánica de la/el usuaria/o.

- Los requerimientos y atenciones de acceso a los activos de información deben ser solicitados de acuerdo a lo establecido en los instrumentos correspondientes.

- El servicio de seguridad debe solicitar las credenciales físicas a el/la servidor/a del OSCE para ingresar a los ambientes de la institución.

- El ingreso a los sectores restringidos, requiere el uso de su tarjeta de identificación personal a fin de registrar su ingreso y salida, empleando, de ser el caso, mecanismos biométricos.

- Las credenciales de usuarias/os tienen carácter personal, intransferible y confidencial.

5.2 **POLÍTICA**: DISPOSITIVOS MÓVILES INSTITUCIONALES

A. Propósito

Establecer lineamientos que permitan el uso y protección adecuado de los dispositivos móviles institucionales asignados a las/los usuarias/os, a fin de salvaguardar la seguridad de la información.

B. Responsabilidades de la/el usuaria/o:

- Mantener el acceso al dispositivo protegido mediante controles de seguridad adecuados, tanto a nivel de software y hardware.

- Mantener actualizado el software instalado en el dispositivo, únicamente mediante los medios autorizados y con versiones provenientes de la/el fabricante del software.

- Conectar los dispositivos solo a redes inalámbricas seguras, no utilizar redes inalámbricas públicas.

- Verificar tener instalado y actualizado software antivirus, software de prevención de intrusiones (malware), software para administración u otro similar, caso contrario, comunicar al equipo de Soporte de la UAST.

- Instalar software, de ser requerido, únicamente con autorización de la/el jefa/e del órgano y/o unidad orgánica, y visto bueno de la UAST.

- Comunicar inmediatamente al equipo de soporte de la UABA, ante la pérdida o robo de su dispositivo, para las acciones correspondientes.

- Utilizar los dispositivos asignados, únicamente para las actividades propias de sus funciones en la institución.

- Mantener la configuración de seguridad de los dispositivos, no realizar ningún tipo de modificación.

C. Responsabilidades de la OTI:

- Definir las características de las capacidades de los dispositivos informáticos en función a la importancia de la información procesada o almacenada.

- Mantener actualizado el software antivirus de los dispositivos institucionales.

- Configurar e implementar en los dispositivos institucionales controles para el bloqueo automático del mismo, cuando se deje de utilizar por algún tiempo.

- Configurar algún método de seguridad (por ejemplo, contraseñas, mecanismos biométricos, patrones, reconocimiento de voz), para el control de accesos al dispositivo.

5.3 POLÍTICA: TELETRABAJO

A. Propósito

Definir los lineamientos para las/los usuarias/os sin presencia física en el OSCE que tengan acceso a información mediante el uso de recursos tecnológicos institucionales (redes, carpetas compartidas, productos digitales), así como para los mecanismos informáticos que permitan salvaguardar la confidencialidad, integridad y disponibilidad de la información del OSCE.

B. Responsabilidades de la/el usuaria/o:

- Acceder a la red del OSCE (productos digitales, carpetas compartidas, repositorios, entre otros) únicamente a través de la conexión VPN a fin de salvaguardar la seguridad de la información de la entidad; utilizando los instrumentos correspondientes para su instalación y uso adecuado.

- Acceder a la VPN desde dispositivos conectados a redes confiables, no públicas y/o gratuitas, que cuenten con una contraseña de acceso.

- Comunicar al equipo de soporte de la UAST, en caso se presente un desperfecto con la conexión VPN.

- Cumplir con los requisitos técnicos definidos por la OTI, para una adecuada ejecución del teletrabajo.

- Almacenar información confidencial únicamente en dispositivos del OSCE, nunca en los equipos de cómputo personales.

C. Responsabilidades de la OTI

- Brindar acceso remoto a través de la VPN, de acuerdo a lo solicitado y autorizado por las/los jefas/es de los órganos y/o unidades orgánicas.

- Efectuar regularmente el monitoreo de las conexiones VPN prestando especial atención a los intentos de conexión sospechosa.

- Habilitar el acceso remoto utilizando canales de comunicación seguros (cifrados) previa autenticación.

- Deshabilitar los accesos a la VPN cuando culminen las actividades relacionadas con el teletrabajo, previa comunicación de la UREH y UABA, para el personal del OSCE y proveedoras/es o terceros, respectivamente.

D. Lineamientos Generales

- El teletrabajo solo aplica para las/los usuarias/os autorizadas/os por la/el jefa/e del órgano y/o unidad orgánica.

5.4 **POLÍTICA**: ESCRITORIO LIMPIO Y PANTALLA LIMPIA

A. Propósito

Establecer los lineamientos que permitan salvaguardar la confidencialidad, integridad y disponibilidad de la información a través del escritorio limpio y pantalla limpia.

B. Responsabilidades de la/el usuaria/o sobre Escritorio Limpio

- Custodiar y proteger de forma segura los documentos impresos y soportes de almacenamiento de datos (CD, DVD, disco duro externo, memoria USB, y medios removibles en general) que contengan información confidencial. No dejarlos expuestos sobre los escritorios para evitar accesos no autorizados.

- Almacenar los documentos impresos, así como de los soportes de almacenamiento que contengan información confidencial, en lugares, espacios y/o mobiliario que cuenten con mecanismos físicos de seguridad. No dejarlos expuestos sobre los escritorios, fotocopiadoras o impresoras.

- La información confidencial impresa debe ser destruida y desechada de manera segura, a fin de que no se permita su reconstrucción total o parcial.

- Los documentos físicos que contengan información confidencial no deben ser reciclados.

C. Responsabilidades de la/el usuaria/o sobre Pantalla Limpia

- Bloquear su dispositivo de cómputo asignado o dispositivo móvil, al ausentarse de su puesto de trabajo, para impedir el acceso de personas no autorizadas.

- Bloquear su dispositivo de cómputo asignado al término del horario laboral.

- Proteger los archivos con información confidencial almacenada en sus dispositivos, no almacenándola, ni creando atajos, en el escritorio del sistema operativo, a fin de dificultar su acceso en caso de alguna intrusión no autorizada.

5.5 **POLÍTICA**: ACCESO A LA INFORMACIÓN DEL OSCE A TRAVÉS DE DISPOSITIVOS NO INSTITUCIONALES

A. Propósito

Establecer lineamientos para las/los usuarias/os autorizados por el OSCE que acceden a información institucional a través de dispositivos no institucionales para el desarrollo de sus funciones o actividades dentro y/o fuera de las instalaciones de la entidad, a fin de salvaguardar la seguridad de la información.

B. Lineamientos Generales

- La/El jefa/e del órgano y/o unidad orgánica autoriza a la/el usuaria/o el acceso a la información institucional gestionada a través de dispositivos no institucionales, para el desarrollo de sus funciones o actividades asignadas. Para ello la/el propietaria/o del dispositivo no institucional debe suscribir el compromiso relacionado al cumplimiento de la presente política. En caso, la/el propietaria/o no suscriba el referido compromiso, no contará con la autorización para gestionar información a través de su propio dispositivo.

- La información institucional que se almacena, transfiera o procesa en los dispositivos no institucionales, es de titularidad del OSCE.

C. Responsabilidades de la/el usuaria/o

- Proteger los dispositivos no institucionales mediante métodos de autenticación como claves y/o contraseñas, y/o patrón de seguridad y/o lectores biométricos, u otros que se consideren necesarios para salvaguardar la seguridad de la información del OSCE.

- Tener instalado software antivirus y/o software de prevención de intrusiones (malware) y/o software para administración de dispositivos móviles, u otro similar, cuya funcionalidad permita salvaguardar la seguridad de la información del OSCE.

- Proteger las contraseñas de las credenciales de acceso asignadas por el OSCE.

- Mantener actualizado el dispositivo con los últimos parches de seguridad de los sistemas operativos.

- Proteger la información del OSCE en sus dispositivos, no permitir el acceso a personas no autorizadas.

- Descargar, almacenar y/o transferir solo información que haya sido autorizada por el OSCE, en el marco de sus actividades y/o funciones asignadas.

- Reportar todo evento o incidente de seguridad de la información presentada en el dispositivo no institucional, mediante los mecanismos definidos.

- Reportar la pérdida del dispositivo no institucional, que contenga información del OSCE, ya sea por extravío, robo o hurto.

D. Responsabilidades de la OTI

- Brindar acceso a la red del OSCE, solo a los dispositivos no institucionales de la/el usuaria/o que haya suscrito el compromiso de la presente política y que cuente con los requisitos mínimos de seguridad como:
    - Método de autenticación seguro para su acceso
    - Software antivirus, o similar, instalado y actualizado
    - Sistema Operativo licenciado, con soporte vigente y con las últimas actualizaciones de seguridad.
    - Otros que considere pertinentes la OTI, para garantizar la seguridad de la red.

- Verificar que los dispositivos no institucionales que se conectarán a la red del OSCE, cuenten con métodos de autenticación como claves y/o contraseñas, y/o patrón de seguridad y/o lectores biométricos u otros que consideren necesarios para salvaguardar la seguridad de la información del OSCE.

- Verificar que los dispositivos no institucionales que se conectarán a la red del OSCE, tengan instalado software antivirus y/o software de prevención de intrusiones (malware) y/o software para administración de dispositivos móviles u otro similar, cuya funcionalidad permita salvaguardar la seguridad de la información del OSCE.

- Implementar herramientas y/o soluciones adecuadas, que permitan mitigar cualquier riesgo de seguridad digital, ante la conexión de los dispositivos no institucionales, a la red del OSCE.

5.6 POLÍTICA: TRANSFERENCIA DE LA INFORMACIÓN

A. Propósito

Establecer los lineamientos que permitan salvaguardar la seguridad de la información durante su transferencia, ya sea al interior del OSCE, con otras instituciones y/o con un tercero.

B. Lineamientos Generales

- Toda transferencia de información del OSCE es respaldada por un requerimiento formal y, cuando corresponda, por un convenio o contrato que incluya cláusulas de confidencialidad y/o no divulgación de la información.

- La transferencia de la información confidencial se debe realizar utilizando mecanismos o medios que salvaguarden la seguridad de la información, tanto dentro como fuera de la entidad.

C. Responsabilidades de la/el usuaria/o:

- Determinar el alcance de la transferencia de la información, en coordinación con el OSCD, a fin de gestionar la implementación de controles de seguridad, teniendo en cuenta la clasificación de la misma.

- Gestionar la autorización de transferencia de información a la/el propietaria/o del activo de información, a través de la/el jefa/e del órgano o unidad orgánica.

- Utilizar los canales tecnológicos de la entidad, previa autorización de la/el propietaria/o del activo de información.

- Autenticar la identidad de las/los destinatarios/as previo a la transferencia de información.

- Utilizar canales tecnológicos que aseguren la transferencia de información de manera segura.

D. Responsabilidades de la/el propietaria/o de activo de información:

- Autorizar las solicitudes de transferencia de información, relacionadas a sus activos de información, verificando previamente el requerimiento formal y el sustento de la solicitud.

- Solicitar al custodio del activo de la información, que remita la información solicitada, aplicando los controles de seguridad adecuados de acuerdo a su clasificación.

E. Responsabilidades de la OTI

- Configurar en el correo electrónico el pie de página correspondiente a la advertencia en cuanto a uso y autorización de la información.

- Orientar y apoyar a los órganos y/o unidades orgánicas en la autenticación de las/los usuarias/os previa a la transferencia de información.

- Proponer e implementar mecanismos o medios que salvaguarden la seguridad de la información durante la transferencia de la misma.

- Implementar y utilizar canales tecnológicos que aseguren la transferencia de información de manera segura.

- Proponer e implementar mecanismos de cifrado de información para la trasferencia de la información de manera segura, de acuerdo a la viabilidad tecnológica.

- Implementar medidas de seguridad adecuadas para la transferencia de información mediante servicios digitales, implementando controles de autenticación y cifrado de información.

- Implementar los requisitos de seguridad solicitados por otras entidades, en el marco de convenios vigentes, para el intercambio de su información por medios digitales.

5.7 **POLÍTICA**: SEGURIDAD DE LA INFORMACIÓN PARA LA RELACIÓN CON LAS/LOS PROVEEDORAS/ES

A. Propósito:

Establecer los lineamientos que permitan salvaguardar la protección de los activos de información a los que acceden las/los proveedoras/es, en el marco de los servicios que brindan al OSCE.

B. Lineamientos Generales:

- El acceso a la información de las/los proveedoras/es debe limitarse a lo indispensable para cumplir con el servicio que brindan.

- La información proporcionada por el OSCE es de su propiedad, sin importar el tiempo trascurrido.

- Las obligaciones de confidencialidad continuarán vigentes aún culminado el contrato de prestación de servicios.

- En el supuesto en que las condiciones de mercado establezcan excepciones a la cláusula de confidencialidad, la Oficina de Administración deberá solicitar al órgano o unidad orgánica usuaria del servicio, realizar una evaluación técnica correspondiente.

- El OSCE se reserva el derecho de implementar mecanismos de control y auditoría que verifiquen el cumplimiento de las políticas de seguridad de la información, así como realizar auditorías extraordinarias adicionales, siempre que se den las causas específicas que lo justifiquen.

- Los órganos o unidades orgánicas que requieren la contratación de bienes y servicios relacionados con el tratamiento de activo(s) de información, cumplen lo siguiente:
    - Deben evaluar y definir los requerimientos de seguridad en los términos de referencia, de ser necesario en coordinación con el OSCD. Esta evaluación y determinación de requisitos de seguridad, pueden ser determinados con una evaluación de riesgos.
    - Asegurar que el/la proveedor/a conozca las políticas de seguridad de la información que le son aplicables, y que firme un acuerdo de confidencialidad y de no divulgación.

- Comunicar a la/el Oficial de Seguridad y Confianza Digital, los incidentes de seguridad de la información reportados por las/los proveedoras/es.

C. Responsabilidades de el/la proveedor/a

- Asegurar el cumplimiento de las restricciones legales respecto del uso del material protegido por normas de propiedad intelectual.

- Utilizar los activos de información autorizados por la entidad únicamente para el desarrollo de los servicios contratados.

- Considerar a la información como confidencial por tiempo indefinido.

- Designar un/a responsable de gestionar la información que necesite en función al contrato con el OSCE.

- En caso corresponda, el/la proveedor/a es responsable de transmitir y hacer cumplir las políticas de seguridad de la información de la entidad a terceros subcontratados.

- Asegurar que a la terminación del servicio o ante el pedido efectuado en cualquier momento por la entidad, cesará inmediatamente el uso de toda información proporcionada, debiendo entregar toda la información que obre en su poder y destruir toda copia que se haya realizado, entregando una confirmación por escrito de ello con la calidad de declaración jurada.

- Comunicar de manera oportuna al órgano o unidad orgánica usuario del servicio, cuando vayan a realizar cambios en el personal que brindará el servicio.

- Respecto al personal que brinda el servicio, en los casos que implique acceso a la información o sistemas de información de la entidad, deben cumplir con lo siguiente:
    - Verificar los antecedentes profesionales, penales y policiales del personal asignado al servicio.
    - Asegurar la baja inmediata del personal asignado al servicio que incumpla las políticas de seguridad de la información.

- Cuando conozca de cualquier pérdida, uso no autorizado o revelación de la información proporcionada o de propiedad de la entidad, debe comunicarlo inmediatamente a la/el responsable del servicio del área usuaria.

D. Prohibiciones del el/la proveedor/a

- Usar los recursos proporcionados por la entidad para actividades no relacionadas con el propósito del servicio.

- Efectuar la conexión a la red del OSCE de dispositivos y/o aplicaciones que no estén especificados como parte del software propio o bajo supervisión de la entidad.

- Intentar y/u obtener, sin autorización explícita, otros derechos o accesos distintos a los que la entidad haya asignado.

- Intentar y/o acceder, sin autorización explícita, a áreas restringidas de la entidad.

- Revelar, modificar, destruir o dar mal uso a la información a la que tenga acceso.

- Utilizar la información de la entidad para beneficio propio o de terceros.

5.8 POLÍTICA: RESPALDO

A. Propósito:

Establecer lineamientos que permitan generar y mantener de manera segura las copias de seguridad (respaldo) de la información, mitigando situaciones relacionadas con la pérdida parcial o total de la información que podrían afectar la continuidad operativa de los servicios que brinda el OSCE a través de sus productos digitales.

B. Responsabilidades de la OTI

- Realizar periódicamente las copias de respaldo de la información almacenada en los Centros de Cómputo del OSCE.

- Implementar y mantener actualizadas las políticas de backups consideradas en la administración y monitoreo de la plataforma tecnológica.

- Efectuar periódicamente pruebas aleatorias de restauración de la información y como consecuencias de las mismas, documentar las incidencias que se hayan puesto de manifiesto durante su desarrollo.

- Asegurar que las copias de respaldo se resguarden en una ubicación externa a la entidad, que reúna las condiciones adecuadas de acondicionamiento, temperatura y humedad, siendo trasladadas con los elementos de seguridad adecuados, a fin de prevenir intentos de acceso no autorizados y mantener un inventario actualizado de dichas copias de respaldo.

- Conservar la información en custodia por el período de retención definido por la/el propietaria/o de la información en concordancia con la matriz de activos de información.

- Contar con un programa de mantenimiento preventivo y correctivo para el hardware de respaldo, a efectos de asegurar su correcto funcionamiento.

- Revisar periódicamente la vigencia tecnológica del hardware y software utilizados en la generación de las copias de respaldo y la restauración de las mismas.

C. Responsabilidades de la/el propietaria/o de activo de información:

- Solicitar a la OTI que realice el respaldo de sus activos de información más críticos.

- Definir, en tiempo, la máxima de cantidad de datos e información que el activo puede aceptar como pérdida considerable ante una contingencia.

5.9 POLÍTICA: CONTROLES CRIPTOGRÁFICOS

Establecer lineamientos que permitan asegurar el uso efectivo de controles criptográficos para proteger la confidencialidad, autenticidad y/o integridad de la información.

A. Lineamientos Generales

- La información confidencial de la entidad debe ser protegida en su almacenamiento y transporte. Para ello se pueden utilizar controles criptográficos, previa evaluación técnica.

- Se deben usar algoritmos de cifrados confiables y verificados.

- Se deben utilizar controles criptográficos para el establecimiento de canales seguros, incluyendo el uso y gestión de llaves criptográficas y certificados digitales.

- Las llaves criptográficas deben estar clasificadas como confidencial y ser protegidas contra divulgación, uso indebido o sustitución no autorizada.

- La generación de llaves criptográficas debe utilizar mecanismos seguros, no predecibles ni al azar.

- Las llaves criptográficas deben tener un ciclo de vida con su respectivo período de expiración.

B. Responsabilidades de la OTI

- Implementar medidas de seguridad que garanticen la confidencialidad de las llaves criptográficas usadas por la entidad.

- Autorizar formalmente los métodos de encriptación a utilizar en los productos digitales y en los componentes de la plataforma tecnológica.

- Asegurar que los controles criptográficos cumplan con la normativa nacional y/o estándares internacionales.

- Definir y gestionar los recursos necesarios para la implementación y protección de los controles criptográficos.

- Implementar la encriptación de la información, salvaguardando su integridad y confidencialidad, desde la transmisión hasta la recepción, previa evaluación técnica de los componentes de la plataforma tecnológica y de los productos digitales.

- Implementar los mecanismos necesarios para la creación, cambio y/o eliminación de las llaves criptográficas.

5.10 POLÍTICA: DESARROLLO SEGURO

A. Propósito

Establecer lineamientos de desarrollo seguro de software, así como principios de ingeniería de sistemas seguros, que deben ser considerados en la implementación y mantenimiento de productos digitales del OSCE.

B. Lineamientos generales:

- La presente política aplica a los productos digitales que se implementan y modifican en la entidad.

- La infraestructura tecnológica que soporte el ambiente de desarrollo y pruebas debe estar separada del ambiente de producción, contando con controles de acceso adecuados para cada uno de ellos.

- Los contratos suscritos con los terceros para la implementación o mantenimiento de productos digitales, deben contar con una cláusula que resguarde la propiedad intelectual del OSCE, la confidencialidad y reserva absoluta en el manejo de la información y documentación a la que tengan acceso.

C. Responsabilidades de la OTI:

- Establecer los requisitos de seguridad para la implementación y mantenimiento de productos digitales.

- Mantener control de la versión de los productos digitales de acuerdo a la factibilidad técnica.

- Gestionar la asignación de recursos para la implementación y modificación de los productos digitales.

- El equipo de desarrollo no debe tener acceso a los ambientes de producción.

- Autorizar, cuando corresponda y previa evaluación técnica, utilizar software de código abierto debidamente documentado.

- El equipo de desarrollo, previa evaluación técnica, podrá modificar el código fuente de software de código abierto. Las modificaciones autorizadas son a través de parches.

- Realizar, al menos una vez al año, un escaneo selectivo de las aplicaciones, servicios y sistemas operativos en busca de vulnerabilidades, manteniendo un registro de los resultados y las acciones correctivas tomadas.

- Asegurar que las actualizaciones de los componentes de la plataforma tecnológica del OSCE no interrumpan la funcionalidad de los sistemas de información adquiridos o desarrollados.

- Asegurar la integridad de las copias de respaldo del repositorio del código fuente de los productos digitales, así como de la documentación almacenada en otros repositorios.

- Implementar el doble factor de autenticación de usuarios en los productos digitales del OSCE, previa evaluación de factibilidad técnica.

- Implementar pistas de auditoría en los productos digitales, en función a los requerimientos de los órganos y unidades orgánicas responsables de los productos digitales.

- Garantizar la integridad y disponibilidad de datos históricos de los productos digitales.

- Segregar las funciones en la implementación y mantenimiento de productos digitales, de acuerdo a la disponibilidad de recursos.

- Implementar una codificación segura que garantice lo siguiente:
    - Validación de datos de entrada
    - Estilo de programación estandarizado
    - Manejo de log de cambios
    - Prácticas criptográficas cuando corresponda
    - Manejo de errores y logs
    - Manejo de archivos y versionamiento del código fuente
    - Inspección de código por fases, cuando corresponda
    - Estandarización y reutilización de funciones de seguridad.

- Elaborar documentación técnica de los productos digitales y los componentes de la plataforma tecnológica de la entidad.

- Ejecutar acciones de control de calidad previo a la puesta en producción.

- Ejecutar pruebas de seguridad en los productos digitales, así como en los componentes de la plataforma tecnológica.

D. Responsabilidades de la/el propietaria/o de activo de información:

- Definir los roles y privilegios en los servicios y sistemas de información del OSCE, relacionados a sus procesos.

- Definir y aprobar el alcance de los requerimientos a implementarse en los servicios y sistemas de información del OSCE, relacionados a sus procesos.

- Evaluar y, de corresponder, solicitar la implementación de pistas de auditoría en los productos digitales relacionados a sus procesos.

- Participar de las pruebas funcionales de los servicios y sistemas de información del OSCE, relacionados a sus procesos.

- Autorizar la puesta en producción de la implementación de los requerimientos en los servicios y sistemas de información del OSCE, relacionados a sus procesos.

5.11 POLÍTICA: INTELIGENCIA DE AMENAZAS

A. Propósito

Establecer lineamientos para la recopilación y análisis de la información relacionadas con las amenazas a la seguridad de la información, para adoptar acciones de mitigación adecuadas.

B. Lineamientos generales:

- Identificar, examinar y seleccionar fuentes de información internas o externas para obtener información relevante de amenazas. Estas fuentes pueden ser de las/los proveedoras/es de soluciones tecnológicas, datos de foros, blogs y sitios web, registros y metadatos de los dispositivos de seguridad y de la red interna, así como resultado de análisis de vulnerabilidades, entre otras.

- Informarse de las últimas amenazas y mejores prácticas para mantener los servicios informáticos seguros y proteger la información confidencial de la entidad.

C. Responsabilidades del OSCD:

- Consultar de forma periódica la "Alerta Integrada de Seguridad Digital" del Centro Nacional de Seguridad Digital de la PCM a través del siguiente enlace: https://www.gob.pe/institucion/pcm/colecciones/791-alerta-integrada-de-seguridad-digital-del-cnsd

- Identificar la información recopilada de las amenazas y verificar su autenticidad, para evaluar su impacto en la entidad, según el caso, y proceder a su registro en el formato "Inteligencia de Amenazas".

- Reportar a los dueños de los procesos que puedan verse afectados por las amenazas identificadas, para que puedan registrarlas en su matriz de riesgos de seguridad de la información y se proceda a su evaluación, y de ser el caso, aplicar las medidas de tratamiento.

D. Responsabilidades de la OTI:

- Analizar la información de las amenazas reportadas en el formato "Inteligencia de Amenazas", para identificar las acciones a realizar.

- Identificar si la amenaza reportada compromete las operaciones de la entidad, a efectos de adoptar las acciones necesarias para la resolución de la amenaza reportada; actualizando la información en el formato "Inteligencia de Amenazas".

- Informar al OSCD sobre las amenazas que comprometan las operaciones de la entidad, así como las acciones para mitigar los riesgos que generen.

5.12 POLÍTICA: USO DE SERVICIOS EN LA NUBE

A. Propósito

Establecer directrices para el uso de servicios en la nube que permita asegurar la protección de la información y el cumplimiento con los estándares de seguridad del OSCE.

B. Responsabilidades de la/el usuaria/o:

- Utilizar adecuadamente los accesos y controles de seguridad para el servicio de nube asignado.
- Utilizar doble factor de autentificación, si se encuentra habilitado.
- Acceder a los servicios en la nube desde dispositivos seguros y mantener los dispositivos actualizados.
- Evitar el uso innecesario de recursos en la nube para prevenir el almacenamiento excesivo de la información.
- Informar de inmediato cualquier actividad sospechosa o incidente de seguridad de la información, de acuerdo al instrumento establecido.
- Mantener seguras las credenciales de acceso y no compartirlas con terceros.
- Utilizar los servicios en la nube únicamente para fines relacionados con las funciones asignadas y conforme a las políticas de seguridad de la información que le sean aplicables.

C. Responsabilidades de la OTI

- Establecer requisitos de seguridad de la información asociados al servicio en la nube y criterios de selección de el/la proveedor/a.
- Realizar evaluaciones de riesgos de seguridad de la información relacionados al servicio en la nube.
- Determinar con qué certificaciones de seguridad debe contar el/la proveedor/a de servicio en la nube.
- Establecer qué controles de seguridad de la información gestiona el/la proveedor/a de servicios en la nube y cuáles gestiona el OSCE como cliente del servicio en la nube.
- Gestionar los recursos y servicios en la nube (IaaS, PaaS y SaaS).
- Implementar controles de accesos robustos para limitar el acceso a la gestión de los servicios en la nube solo a personas autorizadas.
- Establecer los parámetros de configuración, operación, monitoreo, gestión de incidencias y auditorias del servicio en la nube.

- Monitorear continuamente el rendimiento y uso de servicios en la nube, para ello el/la proveedor/a debe realizar como mínimo lo siguiente:
    - Soporte operacional sobre la infraestructura
    - Monitoreo 7x24.

- Garantizar que como parte del servicio de operaciones, se realice como mínimo lo siguiente:
    - Gestión de infraestructura aprovisionada
    - Gestión de backups sobre plataformas IaaS / PaaS, según la configuración de cada recurso.

- Proveer capacitación regular a los/las usuarios/as sobre las mejores prácticas de seguridad para el uso de servicios en la nube.

- Asegurar que el servicio en la nube esté disponible según el acuerdo de nivel de servicios (SLA).

D. Lineamientos Generales:

- Los accesos y controles de seguridad para el servicio de nube asignado son limitados, controlados y brindados al personal autorizado.

5.13 POLÍTICA: MONITOREO DE SEGURIDAD FÍSICA

A. Propósito

Establecer lineamientos para un adecuado monitoreo de la seguridad física en las instalaciones del OSCE a fin de detectar accesos físicos no autorizados.

B. Lineamientos generales:

- El personal de vigilancia debe controlar la entrada y salida de personas que ingresan a las instalaciones del OSCE.

- En el caso de las oficinas de Alta Dirección, u otros ambientes en donde se procese información confidencial, se debe contar con medidas de protección físicas para su adecuado monitoreo.

- Contar con dispositivos que permiten almacenar videos en formatos digitales para revisarlos en caso de emergencia y/o como evidencia en caso de algún incidente.

- El tiempo de retención de los videos grabados es por un período de hasta tres (3) meses, dependiendo de la factibilidad técnica.

C. Responsabilidades del Órgano o Unidad Orgánica encargada de la seguridad física:

- Gestionar la implementación de un servicio cerrado de videovigilancia para poder supervisar los ambientes del OSCE.

- Implementar un monitoreo del circuito cerrado de televisión que reciba la información captada desde las cámaras que están distribuidas de forma estratégica en el OSCE. El objetivo principal es reaccionar de forma inmediata ante accesos no autorizados en zonas o ambientes protegidos.

- Garantizar que se monitoreen los ambientes donde se procese información confidencial del OSCE, así como el centro de cómputo, mediante cámaras de videovigilancia y/o sensores para detectar de manera oportuna eventos inesperados y accesos no autorizados.

- Contar con un plan de trabajo para el mantenimiento de las cámaras de videovigilancia.

5.14 POLÍTICA: GESTIÓN DE LA CONFIGURACIÓN

A. Propósito

Garantizar que los componentes de configuración asociados a hardware, software, redes y servicios de tecnologías se gestionen de manera adecuada, a fin de que no se vea alterada por cambios no autorizados o incorrectos.

B. Lineamientos generales:

- Contar con información documentada sobre configuración del hardware, software, redes y servicios de tecnologías.

- Almacenar en lugares seguros la información documentada sobre las configuraciones, garantizando su acceso solo a personal autorizado.

C. Responsabilidades de la OTI

- Documentar las configuraciones de hardware, software, redes y servicios utilizados en los sistemas del OSCE, incluyendo versiones, ajustes y parámetros de seguridad de la información.

- Implementar un proceso formal de control de cambios que requiera autorización previa para modificar la configuración de los sistemas, asegurando la trazabilidad.

- Establecer un sistema de versionamiento para llevar un registro histórico de las configuraciones, facilitando la restauración a estados anteriores.

- Actualizar la documentación de las configuraciones de hardware, software, redes y servicios de TI utilizados en los sistemas del OSCE, la cual debe contar con elemento, descripción, configuración actual y responsables.

- Proteger y controlar el acceso a la documentación de las configuraciones de hardware, software, redes y servicios de TI utilizados en los sistemas del OSCE.

5.15 POLÍTICA: ELIMINACIÓN DE LA INFORMACIÓN

A. Propósito

Establecer las directrices de uso y manejo para eliminación de información en los dispositivos suministrados por la entidad, que hagan uso de los servicios de información y red del OSCE.

B. Lineamientos generales

- Los órganos o unidades orgánicas identificarán en sus procesos, de forma periódica, si cuentan con información obsoleta, innecesaria o sensible que debe ser eliminada de los sistemas y/o archivos del OSCE.

- Los órganos o unidades orgánicas deberán coordinar, con el órgano o unidad orgánica responsable del archivo general, los mecanismos adecuados de eliminación de documentos físicos.

C. Responsabilidades de la OTI

- Aplicar medidas específicas de eliminación segura, garantizando un tratamiento adecuado de los datos críticos.

- Implementar métodos para la eliminación segura de la información, incluyendo, el formateo seguro de dispositivos y borrado definitivo de datos electrónicos.

- Mantener un registro detallado de los procesos de eliminación de información, incluyendo qué datos se eliminaron, quién fue responsable y cuándo se llevó a cabo, para garantizar la trazabilidad y transparencia.

- Asegurar que se realice la correcta eliminación de información que se encuentra en los medios de almacenamiento, observando la normativa aplicable.

5.16 POLÍTICA: ENMASCARAMIENTO DE DATOS

A. Propósito

Establecer lineamientos para el enmascaramiento efectivo de datos, garantizando la protección de los datos personales, sensibles y/o confidenciales mientras se mantiene la funcionalidad de los datos.

B. Lineamientos generales:

- Los órganos y unidades orgánicas del OSCE deben de identificar los datos personales, sensibles y/o confidenciales, que se encuentran en sus sistemas de información y que consideran deben ser enmascarados.

- Los órganos y unidades orgánicas deberán solicitar, de considerarlo necesario, aplicar el enmascaramiento de datos en sus activos de información.

C. Responsabilidades de la OTI

- Establecer técnicas de enmascaramiento, en tiempo real, para ocultar datos personales, sensibles y/o confidenciales de la base de datos de producción. Las técnicas de enmascaramiento utilizadas deben cumplir por lo menos con lo siguiente:
    - Evitar la alteración de los datos originales en las bases de datos de producción.
    - Ocultar los datos determinados durante las consultas a las bases de datos.
    - Mantener la integridad y usabilidad de los datos.

- Definir que herramientas para el enmascaramiento son más adecuadas, a fin de que les permita crear políticas de seguridad, para controlar el acceso a la base de datos a nivel de fila y columna.

- Administrar un inventario de los datos personales, sensibles y/o confidenciales que se encuentran enmascarados en los sistemas de información del OSCE.

- Mantener un registro de las técnicas de enmascaramiento utilizadas, las herramientas utilizadas y los datos enmascarados.

- Aplicar técnicas de enmascaramiento para las bases de datos de desarrollo, calidad y producción del OSCE, además de cualquier otra replica de la base de datos que se solicite. De acuerdo a los datos personales, sensibles y/o confidenciales ya definidos.

- Cumplir con las leyes y regulaciones de protección de datos, alineados al enmascaramiento de datos.

- Limitar el acceso a la información confidencial solo a quienes lo necesiten para realizar sus funciones de enmascaramiento permanente.

- Revisar periódicamente, en conjunto con los órganos y/o unidades orgánicas responsables de los sistemas de información, la efectividad de las técnicas de enmascaramiento de datos.

5.17 POLÍTICA: PREVENCIÓN DE FUGA DE DATOS

A. Propósito

Establecer directrices y procedimientos para prevenir la fuga de datos del OSCE, garantizando la protección de la información sensible y confidencial, cumpliendo con los estándares de seguridad de la información según la ISO 27001.

B. Lineamientos generales:

- Los órganos y/o unidades orgánicas del OSCE deben de identificar y clasificar los datos personales, sensibles y/o confidenciales, que se encuentran en el alcance de sus procesos.

- Evitar tomar fotos, realizar grabaciones o capturas de pantallas de la información del OSCE, incluyendo a la documentación física, para actividades no relacionadas con sus funciones asignadas.

- Evitar que personas visitantes a la entidad tomen fotos, realicen grabaciones o capturas de pantallas de la información del OSCE, en ambientes no autorizados.

- Desarrollar capacidades en materia de protección de datos y prevención de fuga de información.

C. Responsabilidades de la OTI

- Gestionar la prevención de fuga de datos mediante el servicio de una empresa especializada de TI para prevenir la fuga de la información confidencial y garantizar la seguridad.

- Establecer un sistema de monitoreo continuo de actividades de TI para detectar comportamientos inusuales o intentos de fuga de datos.

- Implementar herramientas “Data Loss Prevention” para el análisis de seguridad e identificar patrones sospechosos y alertar sobre posibles amenazas.

- Gestionar, de ser necesario, la contratación de proveedoras/es de servicio para atender los incidentes de falla del servicio de las herramientas, cuantas veces sea necesario.

- Determinar protocolos y/o procedimientos necesarios para la prevención de fugas de datos, así como para comunicar adecuadamente a las partes interesadas.

5.18 POLÍTICA: ACTIVIDADES DE MONITOREO

A. Propósito

Establecer lineamientos para monitorear las redes, la infraestructura, los sistemas y las aplicaciones para detectar alertas, comportamientos y tomar medidas apropiadas de forma oportuna para minimizar posibles incidentes de seguridad de la información.

B. Responsabilidades de la OTI

- Establecer los métodos y herramientas adecuadas para el monitoreo de las redes, infraestructura, sistemas y aplicaciones soportados en la plataforma tecnológica del OSCE.

- Implementar un sistema de monitorización continuo de 24/7/365, para detectar y responder a eventos sospechosos que puedan indicar una posible violación de seguridad o un mal uso de los recursos.

- Implementar o contratar una empresa especializada de TI, para contar con equipos, licencias de software y plataforma tecnológica actualizada para el monitoreo de los diferentes recursos.

- Implementar un centro de monitoreo de seguridad de la información, para monitorear, identificar, correlacionar y alertar actividades de posible riesgo sobre los sistemas, registrando los logs en la herramienta SIEM.

- Implementar sistemas de detección de intrusiones (IDS) que analicen el tráfico de las redes, actividades de los sistemas y aplicaciones que estén configurados para detectar tipos de ataques o intrusiones conocidas.

- Gestionar los mecanismos necesarios para el monitoreo continuo de la infraestructura en los Centros de Computo, así como realizar el escalamiento en caso de fallas, incluyendo la prevención, mantenimiento, mitigación y resolución de incidentes.

- Gestionar el monitoreo de servidores a nivel de sistemas operativos, aplicaciones y almacenamiento que incluya lo siguiente:
    - Los servidores de producción, atendiendo a los mensajes de alerta, así como la revisión de la bitácora (log) de errores; desplegados en la plataforma tecnológica
    - El CPU, memoria, disco y servicios a nivel de sistema operativo
    - Las unidades de almacenamiento
    - Los servidores físicos y virtuales
    - El nivel de uso de almacenamiento.
    - Los logs de los equipos y software que conforman el servicio de almacenamiento.
    - La disponibilidad de los equipos y software que componen el servicio de almacenamiento.

- Realizar el monitoreo de equipos de comunicaciones, enlaces, utilizando protocolos SNMP, TCP/IP para resguardar la seguridad en los centros de cómputo y la Nube.

- Efectuar el monitoreo de la base de datos, aplicaciones y mecanismos de producción que son determinados por el OSCE.

- Monitorear de manera centralizada la disponibilidad de equipos, procesamiento de CPU, disco, memoria y tráfico de red.

- Actualizar de las versiones del sistema operativo en los servidores, plataformas de virtualización, parches de seguridad y actualizaciones, recomendados por la/el fabricante.

- Realizar el monitoreo del servicio de gestión en la Nube, para determinar las alertas, backup y restore en la Nube.

- Establecer controles de acceso para limitar quién puede ver, modificar o eliminar los registros de actividad, asegurando que solo personal autorizado pueda acceder a esta información confidencial.

5.19 POLÍTICA: FILTRADO WEB

A. Propósito

Establecer lineamientos para gestionar el acceso de los usuarios a sitios web y contenido en línea a través de la red en el OSCE.

B. Responsabilidades de la OTI

- Proponer una lista de niveles y permisos, para establecer perfiles de accesos al contenido web.

- Establecer mediante los métodos de lista blanca y lista negra, a las páginas permitidas en la red del OSCE.

- Monitorear continuamente el tráfico web para identificar intentos de acceso a sitios bloqueados, registrar actividades sospechosas y generar alertas en caso de vulneraciones.

- Verificar que las/los usuarias/os cuenten con autorización de su jefa/e inmediata/o para solicitar acceso a sitios web bloqueados, por razones justificadas.

- El permiso que se le brinda al acceso de internet dependerá del perfil definido. Por prevención de riesgos de seguridad se debe de bloquear contenido para adultos, contenido no confiable, desde el equipo de seguridad perimetral.

- Implementar soluciones de filtrado web que permitan la categorización y bloqueo de sitios web.

- Categorizar los sitios web de la siguiente manera:

  Bloqueadas:

  - ✓ Aquellos que contienen malware, phishing y otros tipos de amenazas cibernéticas.
  - ✓ Juegos de azar y apuestas.
  - ✓ Redes sociales y plataformas de streaming, excepto cuando se justifique su uso para tareas laborales específicas.
  - ✓ Aquellos que estarán bloqueados por el sistema de filtrado web, como sitios maliciosos, de contenido inapropiado, redes sociales no autorizadas, entre otros
  - ✓ Los programas maliciosos que se instalan en los dispositivos de las/los usuarias/os, y que consuman ancho de banda y envíen datos confidenciales fuera de la red.

  Permitidas:

  - ✓ Aquellos necesarios para el desempeño de las funciones laborales.
  - ✓ Plataformas de formación y desarrollo profesional.
  - ✓ Recursos educativos y de investigación.
  - ✓ Aquellos que cuenten con la justificación y autorización de la OTI.
  - ✓ Políticas web serán permitidas para grupos y usuarios para controlar el uso de internet en el OSCE.
  - ✓ Todas las excepciones deben ser aprobadas por la OTI.

CONTROL DE CAMBIOS

N° de Ítem	Fecha	Categoría N: Nuevo M: Modificado E: Eliminado	Sección del Manual (numeral)	Descripción del cambio