MANUAL DE LINEAMIENTOS DE SEGURIDAD DE LA INFORMACIÓN PARA TECNOLOGÍAS DE LA INFORMACIÓN

VERSIÓN 01

Firmado digitalmente por ESPINOZA SAUCEDO Juan Miguel FAU 20419026809 soft
Motivo: Doy V° B°
Fecha: 09.02.2023 14:27:31 -05:00

Firmado digitalmente por SUAREZ BAO Milagros Danitza FAU 20419026809 soft
Motivo: Doy V° B°
Fecha: 14.02.2023 15:17:46 -05:00

Firmado digitalmente por RAMIREZ DIOS DE CACHO Carola Milagros FAU 20419026809 soft
Motivo: Doy V° B°
Fecha: 14.02.2023 16:57:43 -05:00

Firmado digitalmente por TANTALEAN LEON Javier Justo FAU 20419026809 soft
Motivo: Doy V° B°
Fecha: 14.02.2023 17:09:19 -05:00

ÍNDICE

PRESENTACIÓN

La norma ISO 27001 es el estándar internacional para la gestión de la seguridad de la información en las organizaciones, tanto para la información física como para la digital. Dicha norma forma 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 en las entidades del Estado se implemente el Sistema de Gestión de Seguridad de la Información - SGSI.

Siendo que, con Resolución N° 087-2020-OSCE/PRE se aprobó 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, a través de la cual la entidad, en cuanto 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.

En ese contexto, en el marco de la implementación del SGSI se ha elaborado el Manual de Lineamientos de Seguridad de la Información para Tecnologías de la Información que tiene por objetivo salvaguardar la confidencialidad, integridad y disponibilidad de la información de la entidad que se gestiona a través de la implementación y mantenimiento de los productos digitales así como de la plataforma tecnológica de la entidad.

En ese sentido, el presente manual es una herramienta que servirá para la mejora continua de la gestión y aplicación del SGSI en los procesos que contempla el Manual Integrado de los Sistemas de Gestión de la Calidad, Seguridad de la Información y Antisoborno del OSCE, y tomando como base la Norma Internacional ISO 27001:2013 o su equivalente en la Norma Peruana NTP ISO 27001:2014.

CAPÍTULO 1: OBJETIVO Y CAMPO DE APLICACIÓN

El objetivo del Manual de Lineamientos de Seguridad de la Información para Tecnologías de la Información, es salvaguardar la confidencialidad, integridad y disponibilidad de la información del OSCE a través de Políticas de Seguridad de la Información aplicables a sus tecnologías de la información, para asegurar la mejora continua del Sistema de Gestión de Seguridad de la Información - SGSI.

El campo de aplicación del presente manual contempla los procesos del SGSI, según lo previsto en el numeral 4.3 del Manual Integrado de los Sistemas de Gestión de la Calidad, Seguridad de la Información y Antisoborno del OSCE.

CAPÍTULO 2: REFERENCIAS NORMATIVAS

En el presente manual se utiliza las siguientes referencias:

2.1 ISO 27001:2013 Tecnologías de la información – Técnicas de seguridad – Sistemas de gestión de seguridad de la información - Requisitos.

2.2 Ley N° 27269, Ley de Firmas y Certificados Digitales.

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

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

2.5 Decreto Legislativo N° 1412, Decreto Legislativo que aprueba la Ley de Gobierno Digital.

2.6 Decreto de Urgencia N° 006-2020, Decreto de Urgencia que crea el Sistema Nacional de Transformación Digital.

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

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

2.9 Decreto Supremo N° 029-2021-PCM, Decreto Supremo que aprueba el Reglamento del Decreto Legislativo N° 1412, Decreto Legislativo que aprueba la Ley de Gobierno Digital, y establece disposiciones sobre las condiciones, requisitos y uso de las tecnologías y medios electrónicos en el procedimiento administrativo.

2.10 Decreto Supremo N° 157-2021-PCM, Decreto Supremo que aprueba el Reglamento del Decreto de Urgencia N° 006-2020, Decreto de Urgencia que crea el Sistema Nacional de Transformación Digital.

2.11 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.

2.12 Resolución Directoral N° 019-013-JUS/DGPDP, que aprueba la Directiva de Seguridad de la Información Administrada por los Bancos de Datos Personales.

2.13 Resolución Directoral N° 056-2017-INACAL/DN, que aprueba la Norma Técnica Peruana NTP-ISO/IEC 27002:2017 - Tecnología de la información. Técnicas de seguridad. Código de prácticas para controles de seguridad de la información. 1ª Edición.

2.14 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".

2.15 Resolución 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.

CAPÍTULO 3: TÉRMINOS Y DEFINICIONES

3.1 TÉRMINOS Y DEFINICIONES

- **AD (directorio activo, por sus siglas en inglés):** Conjunto de servicios que conectan a las/los usuarias/os con los recursos de red que necesitan para realizar su trabajo.

- **Activo de Información:** Información que, por su importancia para las actividades del OSCE, ha sido declarada como un bien que tiene un valor significativo. Además, es un activo que, como otros activos importantes del negocio, es esencial para las actividades de la entidad y, en consecuencia, necesita una protección adecuada.

- **Algoritmo:** Secuencia de pasos finitos bien definidos que resuelven un problema.

- **Ancho de banda:** Especifica la cantidad de información que se puede enviar a través de una conexión de red en un período de tiempo dado (generalmente un segundo). El ancho de banda se indica generalmente en bites por segundo (bps), kilobits por segundo (Kbps), o megabits por segundo (Mbps). Cuánto más elevado el ancho de la banda de una red, mayor es su aptitud para transmitir un mayor caudal de información.

- **Autenticación:** Proceso técnico que permite determinar la identidad de la persona que firma digitalmente, en función del documento electrónico firmado por éste y al cual se le vincula; este proceso no otorga certificación notarial ni fe pública.

- **Autenticidad:** Propiedad de que una entidad es lo que afirma ser.

- **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.

- **Canal seguro:** Conducto virtual o físicamente independiente a través del cual se pueden transferir datos garantizando una transmisión confidencial y confiable, protegiéndolos de ser interceptados o manipulados por terceros.

- **Certificado Digital:** Documento electrónico generado y firmado digitalmente por una entidad de certificación, la cual vincula un par de claves con una persona determinada confirmando su identidad.

- **Cifrado:** Proceso de codificación de información. Este proceso convierte la representación original de la información, conocida como texto sin formato, en una forma alternativa conocida como texto cifrado.

- **Clave Criptográfica**: Cadena de caracteres que se utiliza en de un algoritmo de encriptación para alterar los datos de forma que parezcan aleatorios.

- **Clave privada:** Es una de las claves de un sistema de criptografía asimétrica que se emplea para generar una firma digital sobre un documento electrónico y es mantenida en reserva por el titular de la firma digital.

- **Clave pública:** Es la otra clave en un sistema de criptografía asimétrica que es usada por el destinatario de un documento electrónico para verificar la firma digital puesta en dicho documento. La clave pública puede ser conocida por cualquier persona.

- **Código de verificación o resumen (hash):** Secuencia de bits de longitud fija obtenida como resultado de procesar un documento electrónico con un algoritmo, de tal manera que:
  (1) El documento electrónico produzca siempre el mismo código de verificación (resumen) cada vez que se le aplique dicho algoritmo.
  (2) Sea improbable a través de medios técnicos, que el documento electrónico pueda ser derivado o reconstruido a partir del código de verificación (resumen) producido por el algoritmo.
  (3) Sea improbable por medios técnicos, se pueda encontrar dos documentos electrónicos que produzcan el mismo código de verificación (resumen) al usar el mismo algoritmo.

- **Credencial de acceso:** Cuenta de acceso asignada a la/el usuaria/o, compuesta por un "nombre de usuario" y por una "Contraseña", que le permite validar su identidad al ingresar y utilizar un producto digital, sistema de información y/o servicio informático.

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

- **Control Criptográfico:** Control añadido que proporciona confidencialidad, autenticidad, no repudio y autenticación.

- **Custodio del Activo de Información**: Es quien tiene la responsabilidad de mantener los niveles de protección adecuados en base a las especificaciones dadas por el propietario del riesgo.

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

- **Dispositivo Móvil:** Aparato electrónico (computadora portátil o smartphone) que permiten el tratamiento de la información durante su desplazamiento y uso en ambientes dentro y fuera de la entidad.

- **Domicilio o lugar de aislamiento domiciliario**: Lugar en el que la/el usuaria/o puede realizar la prestación de servicios, en cumplimiento de las disposiciones emitidas en el marco de la emergencia sanitaria y el estado de emergencia nacional declaradas por la COVID-19, es decir, su lugar de residencia habitual u otro lugar en el que se encuentre como consecuencia de las medidas de aislamiento social obligatorio.

- **Encargado de tratamiento de datos personales:** 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 de la/el 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. Incluye a quien realice el tratamiento sin la existencia de un banco de datos personales.

- **Encriptación:** Mecanismo de seguridad que permite modificar un mensaje de modo que su contenido sea ilegible, salvo para su destinatario.

- **Firma Digital:** Firma electrónica que utiliza una técnica de criptografía asimétrica, basada en el uso de un par de claves único; asociadas una clave privada y una clave pública relacionadas matemáticamente entre sí, de tal forma que las personas que conocen la clave pública no puedan derivar de ella la clave privada.

- **Hardware:** Conjunto de elementos físicos o materiales que constituyen una computadora o un sistema informático.

- **Incidencias:** Interrupción no planificada de un servicio de TI o una reducción de la calidad de un servicio de TI". Es decir, un incidente es cualquier interrupción de servicios de Tecnología de la Información que afecta desde un solo usuario hasta toda la empresa.

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

- **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.

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

- **No repudio:** Es la imposibilidad para una persona de desdecirse de sus actos cuando ha plasmado su voluntad en un documento y lo ha firmado en forma manuscrita o digitalmente con un certificado emitido por una entidad de Certificación acreditada en cooperación de una entidad de Registro o Verificación acreditada, salvo que la misma entidad tenga ambas calidades, empleando un software de firmas digitales acreditado, y siempre que cumpla con lo previsto en la legislación civil. En el ámbito del artículo 2 de la Ley de Firmas y Certificados Digitales, el no repudio hace referencia a la vinculación de un individuo (o institución) con el documento electrónico, de tal manera que no puede negar su vinculación con él ni reclamar supuestas modificaciones de tal documento (falsificación).

- **Oficial de Seguridad de la Información:** Servidor/a designado/a mediante resolución de Presidencia Ejecutiva, que tiene la responsabilidad de supervisar la implementación de la política y objetivos de seguridad de la información de la Institución, alineando los controles y recursos de acuerdo a la gestión de los riesgos.

- **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.

- **Plataforma Tecnológica:** Conjunto de hardware y software que constituyen la base para crear y ejecutar aplicaciones de negocio.

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

- **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, necesidad o negocio.

- **Propiedad Intelectual:** Herramienta que busca que los creadores o aquellos que puedan tener algún tipo de ventaja respecto a algunas otras personas por algunas habilidades de imaginación o de creación o de desarrollo de intelecto, puedan obtener una alternativa legal para proteger esta habilidad.

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

- **Seguridad de la Información:** Preservación de la confidencialidad, integridad y disponibilidad de la información.

- **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 del trabajador o servidor 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.

- **Trabajo remoto**: Prestación de servicios subordinada con la presencia física de el/la trabajador/a en su domicilio o lugar de aislamiento domiciliario, utilizando cualquier medio o mecanismo que posibilite realizar las labores fuera del centro de trabajo, siempre que la naturaleza de las labores lo permita. Este no se limita al trabajo que puede ser realizado mediante medios informáticos, de telecomunicaciones u análogos, sino que se extiende a cualquier tipo de trabajo que no requiera la presencia física del/la trabajador/a en el centro de labores.

- **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 independientemente de su régimen laboral o modalidad contractual autorizada por el OSCE para acceder la información y/o hacer uso de los productos digitales, sistemas de información y servicios 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.

3.2 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.

- **OSI:** Oficial de Seguridad de la Información.

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

- **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.

CAPÍTULO 4: POLITICAS DE SEGURIDAD DE LA INFORMACIÓN

Las políticas de seguridad de la información establecidas en el presente manual son de cumplimiento obligatorio para el personal de la Oficina de Tecnologías de la Información – OTI del OSCE, sujetándose a las acciones correspondientes frente a su incumplimiento.

POLÍTICA: DISPOSITIVOS MÓVILES INSTITUCIONALES

La presente política tiene como propósito establecer lineamientos que permitan el uso adecuado de los dispositivos móviles institucionales asignados a las/los usuarias/os del OSCE, a través de controles de seguridad implementados en los dispositivos móviles a fin de salvaguardar la seguridad de la información de la entidad que se gestiona en dichos dispositivos.

A. Responsabilidades de la OTI:

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

- Mantener actualizado el software antivirus de las computadoras portátiles institucionales.

- En coordinación con la/el Oficial de Seguridad de la Información validar el software instalado en los dispositivos móviles institucionales.

- Configurar e implementar en los dispositivos móviles institucionales, controles para el bloqueo automático del mismo utilizando algún método de seguridad (por ejemplo, contraseñas, biométricos, patrones, reconocimiento de voz).

POLÍTICA: TELETRABAJO

El propósito de esta política es definir los lineamientos para que el personal de la OTI implemente los mecanismos informáticos que permitan salvaguardar la confidencialidad, integridad y disponibilidad de la información del OSCE a través del teletrabajo.

A. Disposición

- Las conexiones de acceso remoto serán gestionadas y controladas por mecanismos de seguridad de la red del OSCE, a fin de mitigar riesgos que podrían vulnerar la seguridad de la información de la entidad.

B. 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 UREH y UABA, tanto para personal del OSCE como para proveedores, respectivamente.

POLÍTICA: CONTROL DE ACCESOS

El propósito de esta política es establecer lineamientos que deben cumplir el personal de la OTI, a fin de que se gestionen de manera adecuada y oportuna los accesos a los productos digitales y componentes de la plataforma tecnológica del OSCE, salvaguardando su seguridad ante accesos no autorizados.

A. Disposiciones

- El/La servidor/a del OSCE, proveedoras/es o terceros que requieran tener acceso a los productos digitales y componentes de la plataforma tecnológica, deben estar debidamente autorizadas/os y acceder haciendo uso de una credencial de acceso.

B. Responsabilidades de la OTI

- Atender los requerimientos de activación o desactivación de credenciales de acceso.

- Crear las credenciales de acceso, teniendo en cuenta lo siguiente:
  - El nombre de usuario de la credencial asignada a el/la servidor/a del OSCE debería estar compuesta por caracteres relacionados a su nombre y/o apellidos.
  - El nombre de usuario 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.

- 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.

POLÍTICA: TRANSFERENCIA DE LA INFORMACIÓN

El propósito de esta política es establecer los lineamientos que permitan implementar y mantener los controles y mecanismos tecnológicos a fin de salvaguardar la seguridad de la información durante su transferencia, ya sea al interior del OSCE y/o con un tercero.

A. Disposición

- 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 información enviada por correo electrónico incluye en el pie de página una advertencia en cuanto a su uso y autorización.

- 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.

B. 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 a los órganos y unidades orgánicas en la autenticación de las/los usuarias/os previa a la transferencia de información.

- Proponer y cuando corresponda, implementar mecanismos o medios que salvaguarden la seguridad de la información durante la transferencia de la misma.

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

- Proponer y cuando corresponda implementar mecanismos de cifrado de datos confidenciales.

POLÍTICA: RESPALDO

El propósito de la presente política es 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.

A. Responsabilidades de la OTI

- Realizar periódicamente las copias de respaldo de la información almacenada en los Centro 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 manteniendo un inventario actualizado de dichas copias de respaldo.

- Mantener 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.

POLÍTICA: CONTROLES CRIPTOGRÁFICOS

El propósito de esta política es establecer lineamientos que permitan asegurar el uso efectivo de controles criptográficos para proteger la confidencialidad, autenticidad y/o integridad de la información.

A. Disposiciones

- La información confidencial 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 utilizarán 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, pudiendo tener un período de expiración.

B. Responsabilidades de la OTI

- Implementar medidas de seguridad que garanticen la confidencialidad de las llaves de 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.

- La/El OSI en coordinación con la UAST y UGDS, definen y gestionan los recursos necesarios para la implementación y protección de los controles criptográficos.

- La/El OSI en coordinación con las/los propietarias/os de los activos de información, la UAST y/o la UGDS definen el ciclo de vida de las llaves criptográficas.

- La UAST y/o la UGDS en coordinación con la/el OSI, implementan 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.

- La/El OSI en coordinación con la UAST y/o UGDS implementan los mecanismos necesarios para la creación, cambio y/o eliminación de las llaves criptográficas.

POLÍTICA: DESARROLLO SEGURO

La presente política tiene como 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.

A. Lineamientos de desarrollo seguro:

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

- 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.

- 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.

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

- Cuando corresponda, previa evaluación técnica, utilizar software de código abierto debidamente documentado y con previa autorización de la OTI.

- 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 o plugins.

- Al menos una vez al año, la UAST realiza 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.

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

- La UAST asegura 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.

B. Principios de ingeniería de sistemas seguros

- Implementación de control de autenticación de usuarios en los productos digitales del OSCE.

- Definición de roles y privilegios en los servicios y sistemas de información del OSCE, a cargo de las/los propietarias/os de activos de Información.

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

- Integridad y disponibilidad de datos históricos de los productos digitales.

- Segregación de funciones en la implementación y mantenimiento de productos digitales.

- Elaboración y actualización oportuna de la documentación técnica de los productos digitales y los componentes de la plataforma tecnológica de la entidad.

- Codificación segura que asegure:
  a) Validación de datos de entrada.
  b) Estilo de programación estandarizado.
  c) Manejo de log de cambios.
  d) Prácticas criptográficas cuando corresponda.
  e) Manejo de errores y logs.
  f) Manejo de archivos y versionamiento del código fuente.
  g) Inspección de código por fases, cuando corresponda.
  h) Estandarización y reutilización de funciones de seguridad.

- Control de calidad previo a la puesta en producción.

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

- Comprobación de Gestión de configuraciones.

POLITICA DE COOKIES

1. OBJETO

La presente política tiene por objeto informar a las/los usuarias/os del Organismo Supervisor de las Contrataciones del Estado – OSCE, respecto del uso de cookies que sirven para almacenar su información y brindar un mejor servicio a través de las aplicaciones web institucionales.

2. ALCANCE

La presente política es de aplicación para las/los usuarias/os que usan las aplicaciones web del OSCE.

3. DEFINICIONES

3.1. Aplicación web: Es una herramienta informática implementada para ser ejecutada en navegadores web desde dispositivos electrónicos.
3.2. Cookies: Son archivos que se guardan en el navegador o dispositivo durante el uso de sitios web o aplicaciones, y que almacenan información relacionada a la/el usuaria/o.
3.3. Dispositivo: Es un equipo electrónico que almacena y procesa información a través de una aplicación como computadoras personales, laptops, teléfonos inteligentes y tabletas.
3.4. Dominio: Es el nombre único que se muestra después del signo @ en las direcciones de correo y después de www. en las direcciones web.
3.5. 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.
3.6. 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.
3.7. Usuaria/o: Persona natural que, mediante un dispositivo, accede a través de un navegador web a aplicaciones.

4. TIPOS DE COOKIES

El OSCE puede utilizar diversos tipos de cookies, como los siguientes:

4.1. Por finalidad

- **Cookies Técnicas**: Permiten navegar a la/el usuaria/o en las aplicaciones web, así como la utilización de las diferentes opciones que existen en ellas.
- **Cookies de Geolocalización:** Permiten identificar el lugar geográfico desde el cual accede la/el usuaria/o a las aplicaciones web.
- **Cookies de Personalización**: Permiten acceder a un servicio dependiendo de las características de la/el usuaria/o, como idioma o tipo de navegador.
- **Cookies Analíticas**: Permiten medir la actividad realizada por la/el usuaria/o en las aplicaciones web, lo cual se utiliza para incorporar mejoras de navegación.

- **Cookies Publicitarias**: Permiten a gestionar la oferta publicitaria, adecuando el contenido al servicio solicitado por la/el usuaria/o.

4.2. Por duración

- **Cookies de Sesión**: Recaban y almacenan datos temporalmente mientras la/el usuaria/o mantiene su sesión activa.
- **Cookies Permanentes**: Recaban y mantienen almacenados los datos en el dispositivo de la/el usuaria/o como un historial.

4.3. Por gestión

- **Cookies del OSCE**: Se envían desde un servidor web del OSCE al dispositivo de la/el usuaria/o.
- **Cookies de Terceros**: Se envían desde un servidor o dominio de un tercero al dispositivo de la/el usuaria/o, no obstante, la información recolectada es gestionada por un tercero.

5. AUTORIZACIÓN PARA EL USO DE COOKIES

La/El usuaria/o autoriza expresamente al OSCE a utilizar la información almacenada en las cookies al navegar en las aplicaciones web institucionales, para ofrecerle un mejor servicio, y para usos específicos tales como cálculos estadísticos o conteo de visitas.

La desactivación de las cookies no impide la navegación por las aplicaciones web del OSCE, aunque el uso de algunos de sus servicios podrá ser limitado y, por tanto, su experiencia de navegación podría ser menos satisfactoria.

La aceptación o denegatoria de esta autorización para usos adicionales no condiciona a la/el usuaria/o a la prestación del servicio solicitado o la navegación en las aplicaciones web del OSCE.

La/El usuaria/o tiene la potestad de permitir, bloquear o eliminar estas cookies cuando así lo crea conveniente a través de las opciones de configuración del dispositivo o terminal, así como del navegador que utilice, no obstante, la función de "Ayuda" le mostrará cómo hacerlo.

El OSCE no se hace responsable ni controla el uso de cookies por parte terceros.

6. CONSENTIMIENTO PARA EL TRATAMIENTO DE DATOS PERSONALES

La/El usuaria/o otorga al OSCE su consentimiento para el tratamiento de sus datos personales que pudieran recopilarse a través de las cookies que utiliza la entidad, los cuales serán incorporados al banco de datos personales de titularidad del OSCE, y bajo ningún concepto podrán ser materia de tratamiento por terceros, distinto al antes mencionado, sin el consentimiento previo y expreso de la/el usuaria/o, salvo que sea exigida por la legislación vigente, por orden judicial o por autoridad competente.

Si los datos personales recopilados ya no resultaran necesarios para el estricto cumplimiento de la finalidad para la cual fueron proporcionados, serán archivados y conservados con la confidencialidad y seguridad de la información definida por la Ley N°

29733, Ley de Protección de Datos Personales y su Reglamento, aprobado por Decreto Supremo N° 003-2013-JUS.

La/El usuaria/o es informada/o de la posibilidad de ejercer los derechos de Acceso, Rectificación, Cancelación y Oposición (ARCO) y Derecho de Información. Para tal efecto, el/la usuario/a debe presentar su "Solicitud para el ejercicio de derecho ARCO y derecho de información", de conformidad con la ficha de procedimiento "Gestión de derechos ARCO y derecho de información" con código PS05.02.02. Para descargar la información debe ingresar a: https://www.gob.pe/institucion/osce/normas-legales/2576371-117-2021-osce-sge

La/EL usuaria/o es informada/o de la Política de Privacidad y Protección de Datos Personales del OSCE. Para descargar la información debe ingresar a: https://www.gob.pe/institucion/osce/informes-publicaciones/2571569-politica-de-privacidad-y-proteccion-de-datos-personales-del-osce

7. REVISIÓN Y MODIFICACIÓN DE LA POLÍTICA DE COOKIES

El OSCE se reserva expresamente el derecho a modificar, actualizar o completar en cualquier momento la presente política. Cualquier modificación, actualización o ampliación producida en la presente política será inmediatamente publicada en las aplicaciones web del OSCE.