MANUAL DE LINEAMIENTOS DE SEGURIDAD DE LA INFORMACIÓN PARA USUARIAS/OS

VERSIÓN 01

Firmado digitalmente por ESPINOZA SAUCEDO Juan Miguel FAU 20419026809 soft
Motivo: Doy V° B°
Fecha: 31.01.2023 12:53:25 -05:00

Firmado digitalmente por ARANDA VERGARA Ernesto Antonio FAU 20419026809 soft
Motivo: Doy V° B°
Fecha: 31.01.2023 14:15:09 -05:00

Firmado digitalmente por SIFUENTES MENACHO Elvia Anais FAU 20419026809 soft
Motivo: Doy V° B°
Fecha: 31.01.2023 14:46:27 -05:00

Firmado digitalmente por DAVILA CAJAHUANCA Carmen Blancy FAU 20419026809 soft
Motivo: Doy V° B°
Fecha: 31.01.2023 15:09:15 -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. 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 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, 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.

En ese contexto, en el marco de la implementación del SGSI se ha elaborado el Manual de lineamientos de seguridad de la información para usuarias/os 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 la gestión y aplicación del Sistema de Gestión de Seguridad de la Información 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 usuarias/os es asegurar la confidencialidad, integridad y disponibilidad de la información a través de políticas de seguridad de la información, para la mejora continua del sistema de gestión de seguridad de la información.

El campo de aplicación del presente manual contempla los procesos del sistema de gestión de seguridad de la información, 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 Tecnología de la información – Técnicas de seguridad – Sistemas de gestión de seguridad de la información - Requisitos.

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

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

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

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

2.6 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.

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

2.8 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.

2.9 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.

2.10 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.

CAPÍTULO 3: TÉRMINOS Y DEFINICIONES

3.1 TÉRMINOS Y DEFINICIONES

- **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.

- **Credencial de acceso:** Cuenta de acceso asignada a la/el usuaria/o, compuesta por un "nombre de usuario o ID" y por una "Contraseña o password", 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.

- **Custodio del activo de información**: Responsable 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.

- **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.

- **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.

- **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.

- **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 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.

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

- **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 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.

- **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 de el/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 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.

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 las/los usuarias/os 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 fin de salvaguardar la seguridad de la información de la entidad.

A. Responsabilidades de la/el usuaria/o:

- Asegurar que se mantenga actualizado el software antivirus, caso contrario comunicar al equipo de Soporte de la UAST.

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

B. Uso aceptable

- El acceso debe permanecer protegido mediante controles de seguridad a nivel de software y hardware.

- Usar la versión más actualizada de software que brinde seguridad a la información confidencial.

- Los parches o actualizaciones serán obtenidos de manera formal, provenientes del fabricante.

- Tener instalado software antivirus, software de prevención de intrusiones (malware), software para administración, u otro similar.

C. Prohibiciones

- Almacenar o transmitir archivos que contengan información relacionada con los Bancos de Datos personales, salvo autorización expresa de la/el Encargada/o del Tratamiento de Datos Personales.

- Usar en lugares que no ofrezcan las garantías de seguridad física necesaria, a fin de evitar pérdida o robo.

- Utilizar redes inalámbricas públicas.

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

- Modificar la configuración de seguridad.

POLÍTICA: TELETRABAJO

El propósito de esta política es definir los lineamientos para aquellas/os usuarias/os que tengan acceso, sin presencia física en el OSCE, a información mediante el uso de recursos tecnológicos institucionales (redes, carpetas compartidas, productos digitales), a fin de salvaguardar la confidencialidad, integridad y disponibilidad de la información del OSCE.

A. Responsabilidades de la/el usuaria/o:

- Acceder desde redes confiables, no públicas y/o gratuitas.
- Verificar la seguridad de las redes domésticas, es decir, que la red cuente con una contraseña de acceso.
- Cumplir con las Políticas de Escritorio Limpio y Pantalla Limpia.
- Contar con conexión a internet de alta velocidad.
- Comunicar a la/el jefa/e del órgano y/o unidad orgánica o el/la Coordinador/a del Proyecto, así como al equipo de soporte de la UAST, el desperfecto que se presente en la conexión VPN.
- Cumplir las indicaciones de las Guías o Instructivos correspondientes a la instalación y uso adecuado de la conexión VPN.

B. Uso aceptable

- El teletrabajo es para aquellas/os usuarias/os autorizadas/os por la/el jefa/e del órgano y/o unidad orgánica del OSCE o el/la Coordinador/a del Proyecto cuando corresponda.
- El acceso a la red del OSCE (productos digitales, carpetas compartidas, repositorios, entre otros) se realiza a través de la VPN a fin de salvaguardar la seguridad de la información de la entidad.

C. Prohibiciones

- Almacenar información confidencial en los equipos de cómputo personales.
- Subrogar funciones por parte de la/el usuaria/o que permitan a un tercero acceder a información confidencial del OSCE.

POLÍTICA: CONTROL DE ACCESOS

El propósito de la presente política es establecer lineamientos a fin de que el acceso a la 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.

A. 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.

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

- 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 periodo contractual, cese de personal o cambio de puesto de trabajo, según corresponda.

- En coordinación con el OSI, formular la implementación de controles de acceso a los activos de información, los mismos que permitan generar reportes que faciliten el control y auditoría de los referidos accesos.

- 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 solicitante.

B. Responsabilidades de la/el usuaria/o:

- Cambiar la contraseña en el primer inicio de sesión.

- Seleccionar una contraseña que cuente con un nivel adecuado de complejidad, siguiendo las siguientes consideraciones:
  - Longitud mínima de ocho (08) caracteres.
  - Combinación de letras mayúsculas, letras minúsculas y números.
  - Incluir caracteres especiales.
  - Evitar el uso de palabras comunes o datos personales.

- Mantener la confidencialidad de sus contraseñas (no compartirlas), evitando registrarlas en medios físicos o electrónicos.

- Gestionar el cambio de contraseñas ante algún indicio de vulnerabilidad.

- Evitar la activación o hacer uso de la funcionalidad de “recordar clave” o “recordar contraseña” de los navegadores de internet y productos digitales.

- Avisar a la/el OSI de cualquier hecho que pueda afectar la seguridad de la información, a través de medios establecidos en el Procedimiento de Gestión de Incidencias de Seguridad de la Información.

C. Uso aceptable

- Los requerimientos y atenciones de acceso a los activos de información del OSCE son registrados en el formato “Solicitud de Acceso” establecidos para este propósito.

- 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.

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

La presente política tiene como propósito establecer lineamientos para las/los usuarias/os autorizados por el OSCE que acceden a información institucional a través de dispositivos móviles 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 de la entidad.

A. Disposiciones:

- El OSCE 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 del OSCE a través de su propio dispositivo.

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

- Los dispositivos móviles no institucionales deben contar con configuraciones mínimas de seguridad como bloqueo de pantalla y/o biometría y/o perfil de trabajo y/o privacidad y/o respaldo, u otras que se consideren necesarias a fin de salvaguardar la seguridad de la información del OSCE.

- La/El Oficial de Seguridad de la Información brindará a las/los usuarias/os las indicaciones, recomendaciones y sugerencias necesarias para una utilización segura de la red institucional.

B. 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.

- Contar con actualizaciones de seguridad.

C. Prohibiciones

- Permitir el acceso a la información del OSCE a personas no autorizadas.

- Almacenar localmente las contraseñas de las credenciales de acceso asignadas por el OSCE.

- Descargar, almacenar y/o transferir información que no ha sido autorizada por el OSCE.

D. Incidentes de seguridad

La/El usuaria/o debe reportar inmediatamente a la/el Oficial de Seguridad de la Información, lo siguiente:

- Toda debilidad, evento o incidente de seguridad de la información presentada en el dispositivo no institucional.

- La pérdida del dispositivo no institucional, ya sea por extravío, robo o hurto.

POLÍTICA: ESCRITORIO LIMPIO Y PANTALLA LIMPIA

El propósito de la presente política es establecer los lineamientos que permitan salvaguardar la confidencialidad, integridad y disponibilidad de la información a través del escritorio limpio y pantalla limpia.

A. ESCRITORIO LIMPIO

1. Responsabilidades de la/el usuaria/o

- 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.

- 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.

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

2. Prohibiciones

- Dejar sobre los escritorios, documentos impresos y soportes de almacenamiento de datos (CD, DVD, disco duro externo, memoria USB, y medios removibles en general) que contengan información confidencial, para evitar el acceso no autorizado a los mismos.

- Dejar documentos impresos que contenga información confidencial en fotocopiadoras e impresoras.

- Utilizar use papel reciclado que contenga información confidencial.

B. PANTALLA LIMPIA

1. Responsabilidades de la/el usuaria/o

- Al ausentarse de su equipo de cómputo asignado o dispositivo móvil, bloquearlo para impedir el acceso de personas no autorizadas.

- Al término del horario de trabajo bloquear el equipo de cómputo asignado.

2. Prohibiciones

- Dejar desbloqueado el equipo de cómputo desatendido.

- Almacenar archivos con información confidencial en el escritorio del sistema operativo.

POLÍTICA: TRANSFERENCIA DE LA INFORMACIÓN

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

A. Responsabilidades de la/el usuaria/o:

- En coordinación con el OSI, determinar el alcance de la transferencia de la información, a fin de implementar controles de seguridad al transferir información que no sea de carácter público.

- En coordinación con la/el jefa/e del órgano o unidad orgánica gestionar la autorización de la transferencia de información con el propietario del activo de información.

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

B. Uso aceptable:

- Toda transferencia de información del OSCE con terceros es respaldada por un convenio o contrato que incluya cláusulas de confidencialidad y/o no divulgación de la información.

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

- Autenticar la identidad de las/los usuarias/os previo a la transferencia de información.

POLÍTICA: SEGURIDAD DE LA INFORMACIÓN PARA LA RELACIÓN CON LOS PROVEEDORES

El propósito de la presente política es establecer los lineamientos que permitan salvaguardar la protección de los activos de información del OSCE a los que acceden los proveedores de la entidad, en el marco de los servicios que brindan.

A. Disposiciones:

- El acceso a la información del OSCE por proveedoras/es de servicio debe limitarse a lo indispensable para cumplir con el servicio asignado.

- Toda información proporcionada por el OSCE seguirá siendo de su propiedad.

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

- 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.

- El OSCE se reserva el derecho de realizar auditorías extraordinarias adicionales, siempre que se den las causas específicas que lo justifiquen.

- Los órganos o unidades orgánicas del OSCE que requieren la contratación de bienes y servicios relacionados con el tratamiento de activo/s de información, cumplen lo siguiente:
  - En coordinación con el OSI deben evaluar y definir los requerimientos de seguridad en los términos de referencia.
  - 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 de la Información, los incidentes de seguridad de la información reportados por los proveedores.

B. 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 del OSCE 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/a del servicio, cuando se vaya a realizar cambio en el personal que forme parte del servicio.

- Respecto a su personal, todos los servicios que impliquen accesos 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, asegurando al OSCE que en el pasado no haya tenido algún tipo de sanción.
  - 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 al responsable del servicio del área usuaria del OSCE.

C. Prohibiciones del el/la proveedor/a

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

- La conexión a la red del OSCE de equipos y/o aplicaciones que no estén especificados como parte del Software propio o bajo supervisión del OSCE.

- Intentar obtener sin autorización explícita otros derechos o accesos distintos a los que el OSCE haya asignado.

- Intentar acceder, sin autorización explícita, a áreas restringidas del OSCE.

- 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.