Visado digitalmente por: CHALCO CANGALAYA Edison Vicente FAU 20521286769 soft
Cargo: Jefe de la Oficina de Asesoría Jurídica
Motivo: Soy el autor del documento

Visado digitalmente por: PALOMINO PEREZ Elvis Romel FAU 20521286769 soft
Cargo: Jefe de la Oficina de Planeamiento y Presupuesto
Motivo: Soy el autor del documento

Visado digitalmente por: MENDOZA ROMERO Magaly Rosa FAU 20521286769 soft
Cargo: Oficial de Seguridad de Información
Motivo: Soy el autor del documento

Visado digitalmente por: ALEGRIA ZEVALLOS Miriam FAU 20521286769 soft
Cargo: Gerenta General
Motivo: Soy el autor del documento

POLÍTICAS ESPECÍFICAS DE SEGURIDAD DE LA INFORMACIÓN DEL ORGANISMO DE EVALUACIÓN Y FISCALIZACIÓN AMBIENTAL - OEFA

Vinculadas a la implementación 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"*.

ÍNDICE

I. OBJETIVO

Establecer las Políticas Específicas de Seguridad de la Información, con el objeto de proteger y administrar los activos de información, gestionar los riesgos asociados a los mismos; y, mantener un esquema de seguridad basado en la confidencialidad, disponibilidad e integridad de la información en la Entidad; en el marco de la Política y Objetivos de Seguridad de la Información del Organismo de Evaluación y Fiscalización Ambiental - OEFA.

II. BASE LEGAL

2.1 Ley N° 29733, Ley de Protección de Datos Personales.
2.2 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.
2.3 Resolución de la Comisión de Normalización y de Fiscalización de Barreras Comerciales No Arancelaria N° 129-2014/DNB-INDECOPI, que aprueba la nueva versión 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"*.
2.4 Resolución de Presidencia del Consejo Directivo N° 071-2018-OEFA/PCD, que conforma y designa a los miembros del Comité de Gobierno Digital del Organismo de Evaluación y Fiscalización Ambiental - OEFA.
2.5 Resolución de Presidencia del Consejo Directivo N° 077-2018-OEFA/PCD, que aprueba el Manual de Gestión de Procesos y Procedimientos *"Innovación y Gestión por Procesos"*.
2.6 Resolución de Presidencia del Consejo Directivo N° 062-2019-OEFA/PCD, que designa a el/la Oficial de Seguridad de la Información del Organismo de Evaluación y Fiscalización Ambiental - OEFA.
2.7 Resolución de Secretaría General N° 070-2017-OEFA/SG, que aprueba la *"Política y Objetivos de Seguridad de la Información del Organismo de Evaluación y Fiscalización Ambiental - OEFA"*.
2.8 Resolución de Gerencia General N° 084-2018-OEFA-GEG, que aprueba el Manual de Gestión de Procesos y Procedimiento *"Recursos Humanos"*.
2.9 Resolución de Gerencia General N° 019-2019-OEFA/GEG, que aprueba el Reglamento Interno de los/as Servidores/as Civiles del Organismo de Evaluación y Fiscalización Ambiental - OEFA.
2.9 Resolución de Gerencia General N° 025-2019-OEFA/GEG, que aprueba la *"Política de Protección de Datos Personales del Organismo de Evaluación y Fiscalización Ambiental - OEFA"*.
2.10 Resolución de Gerencia General N° 075-2019-OEFA/GEG, que aprueba el Manual de Procedimientos *"Tecnologías de la Información"*.

Las referidas normas incluyen sus modificatorias.

III. ALCANCE

Las presentes Políticas Específicas son aplicables a las áreas y a los/as usuarios/as del Sistema de Gestión de Seguridad de la Información del Organismo de Evaluación y Fiscalización Ambiental - OEFA.

IV. VIGENCIA

Las presentes Políticas Específicas entran en vigencia desde el día siguiente de su publicación en el Portal Institucional del Organismo de Evaluación y Fiscalización Ambiental - OEFA(www.oefa.gob.pe).

V. DEFINICIONES

5.1. Área: Órganos, unidades orgánicas, coordinaciones y unidades funcionales establecidas mediante Resolución de la Alta Dirección.
5.2. Autenticación: Proceso de confirmación o verificación de alguien que es o que dice ser.
5.3. Base de datos: Conjunto de datos pertenecientes a un mismo contexto y almacenados sistemáticamente para su posterior uso.
5.4. Activos de información: Conocimientos o datos que tienen valor para la Institución, viene a ser lo que una entidad valora y por lo tanto debe proteger, estos pueden ser: los datos creados o utilizados por un proceso del OEFA, recursos o documentación (digital, papel u otro medio).
5.5. Cadena de custodia: Procedimiento controlado que implica la extracción, transporte y entrega de la información.
5.6. Código malicioso: Programas informáticos que tienen por objetivo ingresar al sistema de información sin que se detecte su presencia vulnerando la información de la Entidad, sus vías de diseminación son: el correo electrónico, sitios de internet, redes, dispositivos móviles, dispositivos removibles.
5.7. Contratista: Persona natural o jurídica que vende o arrienda bienes, presta servicios en general, consultorías en general, consultorías de obra o ejecuta obras, que celebra un contrato con la Entidad.
5.8. Criptografía: Estudio de los algoritmos, protocolos y sistemas que se utilizan para dotar de seguridad a las comunicaciones, a la información y a las entidades que se comunican.
5.9. Custodio: Persona responsable de administrar controles autorizados por los propietarios de los activos de información, protegiendo los activos asignados para su custodia.
5.10. Equipamiento perimetral: Integra elementos y sistemas, tanto electrónicos como mecánicos, para la protección de perímetros físicos, detección de tentativas de intrusión y/o disuasión de intrusos de la red de la Entidad.
5.11. Gestión de incidentes: Acción que se lleva a cabo para conseguir o resolver un incidente ante un impedimento de la operación o una violación a las Políticas de Seguridad de la Información.
5.12. No repudio: 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.
5.13. Practicante preprofesional: Estudiante de un Centro de Formación Profesional.
5.14. Practicante profesional: Egresado o Bachiller de un Centro de Formación Profesional.
5.15. Privilegios: Ventaja exclusiva o especial que goza por concesión de un superior.
5.16. Procesamiento de información: Técnicas eléctricas, electrónicas o mecánicas usadas para manipular datos para el empleo humano o de máquinas.

5.17. Propietario de activo de información: Servidor/a civil que en atención a sus funciones se le han asignado la responsabilidad de gestionar un activo de información. El término *"propietario"* no significa que la persona tenga en realidad derechos de propiedad sobre el activo.

5.18. Recursos informáticos: Componentes de hardware y software que son necesarios para el buen funcionamiento y la optimización del trabajo con computadoras.

5.19. Recuperación de información: Conjunto de actividades orientadas a facilitar la localización y restauración de determinados datos y sus interrelaciones.

5.20. Respaldo de información: Copia de los datos originales que se realiza con el fin de disponer de un medio para recuperarlos en caso de pérdida.

5.21. Servidor/a civil: Personal del OEFA que se encuentra contratado/a bajo el Decreto Legislativo N° 1057, Decreto Legislativo que regula el régimen especial de contratación administrativa de servicios, la Ley N° 30057, Ley del Servicio Civil o el Decreto Legislativo N° 728, Ley de Fomento del Empleo.

5.22. Secigrista: Estudiante de la carrera de derecho asignado al OEFA para prestar el Servicio Civil de Graduandos (SECIGRA).

5.23. Sistema de Gestión: Gestión de servicios que se ofrecen, y que incluye planear, controlar y mejorar.

5.24. Tercero/a: Persona, natural o jurídica, inscrita en el Registro de Terceros del OEFA.

5.25. Tercero/a Seleccionado/a: Tercero/a elegido/a como resultado de un proceso de selección para ser contratado/a por el OEFA.

5.26. Trabajo a distancia: Comprende la modalidad de teletrabajo regulada en la Ley N° 30036, Ley que regula el teletrabajo y su Reglamento, aprobado por Decreto Supremo N°017-2015-TR, así como el trabajo remoto, regulado en el Decreto de Urgencia N° 026-2020.

5.27. Trazabilidad: Seguimiento de los documentos desde su creación hasta su disposición final.

5.28. Usuario/a: Servidor/a civil, contratista, tercero/a seleccionado/a practicante pre profesional, practicante profesional y secigrista, que tenga vínculo laboral o contractual con la Entidad; o, se encuentre en alguna modalidad formativa, según corresponda; y, use habitualmente el hardware y software brindados por el OEFA.

VI. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Mediante la Resolución de Gerencia General N° 070-2017-OEFA/SG, se aprueba la *"Política y Objetivos de Seguridad de la Información del Organismo de Evaluación y Fiscalización Ambiental - OEFA"*, conforme a la siguiente redacción:

Política	Objetivos
"Somos una Entidad que brinda servicios de evaluación, supervisión, fiscalización y de aplicación de incentivos en materia ambiental, con respeto de los derechos y equilibrio entre la inversión y la protección del ambiente; en la cual, la información es un recurso estratégico que genera conocimiento, asegura la continuidad de nuestras operaciones y fortalece la confianza con la población, la empresa y el Estado.	Objetivo 1: Implementar los controles de seguridad de la información en el marco de la Norma Técnica Peruana - NTP ISO/IEC 27001:2014, en atención a la gestión de riesgos y mejora continua para asegurar la confidencialidad, integridad y disponibilidad de la información del OEFA.

Política	Objetivos
Nuestro compromiso con la seguridad de la información en la Entidad se enmarca en la implementación y continuidad de mecanismos para asegurar su confidencialidad, disponibilidad e integridad, así como la mejora continua del Sistema de Gestión de Seguridad de la Información, en cumplimiento del marco legal vigente y estándares internacionales.	Objetivo 2: Difundir las políticas y controles de seguridad de la información para concientizar a los colaboradores y contratistas del OEFA, su contribución a la efectividad del Sistema de Gestión de la Información.

VII. POLÍTICAS ESPECÍFICAS

En el marco de la mejora continua del Sistema de Gestión de Seguridad de la Información de la Norma Técnica Peruana de los Sistemas de Gestión de Seguridad de la Información, aprobada por Resolución de la Comisión de Normalización y de Fiscalización de Barreras Comerciales No Arancelaria N° 129-2014/DNB-INDECOPI; y, de nuestra Política de Seguridad de la Información y sus Objetivos, aprobada mediante la Resolución de Gerencia General N° 070-2017-OEFA/SG, en el presente documento establecemos las Políticas Específicas de Seguridad de la Información del OEFA.

VII.1. Dirección de la Alta Dirección para la seguridad de la información

Objetivo: Proporcionar dirección y apoyo de la Alta Dirección para la seguridad de la información en concordancia con los requisitos de la Entidad, las leyes y regulaciones relevantes.

En ese sentido, el OEFA, en el marco de su compromiso con la Seguridad de la Información, debe:

(i) Definir y aprobar las políticas y controles de seguridad de la información.

(ii) Difundir las políticas y controles de seguridad de la información para concientizar a los usuarios del OEFA y su contribución a la efectividad del Sistema de Gestión de Seguridad de la Información.

(iii) Monitorear la implementación de controles de seguridad de la información, relacionados con el Sistema de Gestión de Seguridad de la Información del OEFA, según corresponda; así como, proponer la formulación o modificación de las normas, procedimientos u otra información que se requiera

(iv) Revisar anualmente, como mínimo, la Política de Seguridad de la Información del OEFA; así como, las Políticas Específicas contenidas en el presente documento, promoviendo su modificación y actualización, de ser el caso.

VII.2. Organización de la seguridad de la información

VII.2.1 Organización interna

Objetivo: Establecer un marco de referencia de gestión para iniciar y controlar la implementación y operación de la seguridad de la información dentro de la Entidad.

En ese sentido, el OEFA, en el marco de sus compromisos con el Sistema de Gestión de Seguridad de la Información, debe:

a) Aprobar: *(i)* la estructura organizacional aplicable al Sistema de Gestión de Seguridad de la Información, definiendo y asignando las responsabilidades de la Seguridad de la Información; y, *(ii)* la segregación de los roles, funciones y responsabilidades de los/las usuarios/as y las áreas para la gestión de la seguridad de la información dentro de la Entidad, con la finalidad de reducir oportunidades de modificación no autorizada o no intencional o el mal uso de los activos de la Entidad.
b) Establecer y mantener contactos con autoridades y organismos relevantes para la seguridad de la información.
c) Incluir controles sobre seguridad de la información en la gestión de proyectos desarrollados en el OEFA.

VII.2.2 Dispositivos móviles y trabajo a distancia

Objetivo: Asegurar la seguridad del trabajo a distancia y el uso de los dispositivos móviles.

En ese sentido, el OEFA, en el marco de su compromiso con la Seguridad de la Información debe:

a) Establecer los controles y medidas de seguridad de soporte que deben ser adoptados para gestionar los riesgos para la protección de la información en el uso de dispositivos móviles de propiedad de la Entidad, a través de los correspondientes documentos de gestión interna, que contemplen, entre otros mecanismos, los referidos a:

   - El registro de los dispositivos móviles.
   - La restricción de instalación de software.
   - Un sistema de protección contra software malicioso.
   - Un control de acceso a las aplicaciones.

b) Establecer los controles y medidas de seguridad para proteger la información que se acceda, procese, almacene, transfiera o cualquiera que sea su tratamiento; en la modalidad del trabajo a distancia, a través de los respectivos documentos de gestión interna, que contemplen, entre otros mecanismos, los referidos a:

   - Acciones vinculadas al fortalecimiento de capacidades y remisión de información a los/as usuarios/as.
   - Acciones vinculadas a: *(i)* la seguridad de la información con los/las servidores/as civiles, practicantes preprofesionales y profesionales y secigristas que realizan sus funciones y actividades a través de la modalidad de trabajo a distancia; y, *(ii)* los equipos de propiedad del OEFA.
   - Mantenimiento y sostenibilidad del acceso remoto a los sistemas internos del OEFA.

c) Ser responsable de la custodia y gestión de licencias de software cliente en las estaciones de trabajo de los/as servidores/as civiles.

VII.3. Seguridad de los recursos humanos

VII.3.1. Antes del empleo, servicio o modalidad formativa

Objetivo: Asegurar que los/las servidores/as civiles, contratistas, terceros/as seleccionados/as, practicantes preprofesionales y profesionales; y, los/as secigristas, entiendan sus responsabilidades y sean competentes para los roles que se les considera, en el marco de la gestión de seguridad de la información.

En ese sentido, el OEFA, en el marco de su compromiso con la Seguridad de la Información debe:

a) Verificar los antecedentes (hoja de vida, antecedentes penales, policiales, entre otros) de los/as servidores/as civiles, contratistas, terceros/as seleccionados/as, practicantes preprofesionales y profesionales; y, los/as secigristas; y, secigristas ingresantes a la Entidad, en concordancia con el marco legal vigente y de acuerdo con su vínculo laboral, contractual o modalidad formativa.

b) Suscribir acuerdos con los/las servidores/as civiles, contratistas, terceros/as seleccionados/as, practicantes preprofesionales y profesionales; y, los/as secigristas, según corresponda, las responsabilidades respecto a la seguridad de la información. Dichas responsabilidades deben mantener su vigencia por lo menos un (1) año después de finalizado el vínculo o modalidad formativa con la Entidad.

VII.3.2. Durante el empleo, servicio o modalidad formativa

Objetivo: Asegurar que los/as usuarios/as sean conscientes y cumplan con sus responsabilidades de seguridad de la información.

En ese sentido, el OEFA, en el marco de su compromiso con la Seguridad de la Información debe:

a) Requerir a los/as usuarios/as cumplir con los controles establecidos en el marco de la gestión de la seguridad de la información en concordancia con los documentos de gestión interna aprobados por la Entidad.

b) Fortalecer las capacidades de los/as usuarios a través de acciones de sensibilización respecto a seguridad de la información de acuerdo con la función o actividad que desempeñan; en el caso de los/as contratistas y terceros/as seleccionados/as se les brindará, mediante comunicaciones electrónicas, la información referida a la seguridad de la información. El fortalecimiento de capacidades e información brindada versa, entre otros, sobre las actualizaciones de políticas y documentos de gestión interna de la Entidad.

c) Conducir el procedimiento administrativo disciplinario a fin de determinar la responsabilidad de los/as servidores/as civiles que hayan transgredido las políticas y documentos de gestión interna, de seguridad de la información; y, de ser el caso, imponer la sanción correspondiente de acuerdo con lo establecido en el Reglamento Interno de los/as Servidores/as Civiles del OEFA.

VII.3.3. Terminación y cambio de empleo, servicio o modalidad formativa

Objetivo: Proteger los intereses de la Entidad como parte del proceso de cambio o terminación del vínculo laboral, contractual o de la modalidad formativa.

En ese sentido, el OEFA en el marco de su compromiso con la Seguridad de la Información debe:

a) Definir y comunicar las responsabilidades y deberes de seguridad de la información a los/as usuarios/as al finalizar el vínculo laboral, contractual o modalidad formativa, según corresponda, o se produzca el cambio de empleo.

b) Solicitar a los/las usuarios/as al finalizar el vínculo laboral, contractual o modalidad formativa o el cambio de responsabilidades del empleo, los documentos físicos y/o digital que les fueron entregados o hayan sido generados como parte del cumplimiento de sus funciones, servicios o actividades; así como otros activos relacionados con el tratamiento de la información que le fueron entregados.

c) Cancelar las cuentas de acceso a los sistemas y/o aplicativos informáticos de los/as usuarios/as, al finalizar el vínculo laboral, contractual o modalidad formativa, o el cambio de responsabilidades del empleo.

d) Remover o bloquear los accesos físicos (llaves de oficinas, almacenes, escritorios, anaqueles, lectores biométricos, entre otros) de los/las usuarios/as, al finalizar el vínculo laboral, contractual o modalidad formativa o el cambio de responsabilidades del empleo; cuando corresponda.

VII.4. Gestión de activos

VII.4.1. Responsabilidad por los activos

Objetivo: Identificar los activos de la Entidad y definir responsabilidades de protección apropiadas

En ese sentido, el OEFA, en el marco de su compromiso con la Seguridad de la Información, debe:

a) Identificar, elaborar y mantener un inventario de activos asociados con información e instalaciones de procesamientos de información, el cual se mantiene actualizado.

b) Asignar a un/a propietario/a del activo de la información y demás activos asociados a los recursos, para el tratamiento de la información que forman parte del inventario.

c) Establecer reglas a los/as usuarios/as para el uso adecuado de los activos relacionados con el tratamiento de la información, referidas a:

- Asegurar la información evitando su exposición o divulgación; de acuerdo con su clasificación.
- Restringir el uso de equipos informáticos de pertenencia personal para desempeñar sus funciones, servicios o actividades.
- Usar los activos de información únicamente para el desarrollo de sus funciones o servicios, de acuerdo al marco normativo vigente y las políticas de seguridad de la información; con el objeto de evitar daños operativos, a la imagen o a otros intereses de la Entidad.
- Devolver todos los activos del OEFA que le fueron brindados para el desarrollo de sus funciones servicios o actividades, al término del vínculo laboral, contractual o modalidad formativa.

VII.4.2. Clasificación de la información

Objetivo: Asegurar que la información recibe un nivel apropiado de protección en concordancia con su importancia para el OEFA.

En ese sentido, el OEFA, en el marco de su compromiso con la Seguridad de la Información, debe:

a) Clasificar la información que se haya generado o se encuentre en posesión del OEFA como pública, secreta, reservada o confidencial de acuerdo con lo establecido en el Texto Único Ordenado de la Ley de Transparencia y Acceso a la Información Pública y su Reglamento, aprobado por Decreto Supremo N° 021-2019-JUS.

b) Desarrollar e implementar, en concordancia con el esquema de clasificación de la información adoptado, un conjunto apropiado de documentos de gestión interna que regulen lo referido al etiquetado de la información, a través del cual se asegure que:

   - La información sea etiquetada y protegida, según su clasificación.
   - El manejo de sus activos se desarrolle de acuerdo con la clasificación de información de la Entidad.

c) Desarrollar e implementar, en concordancia con el esquema de clasificación de la información adoptado, un conjunto apropiado de documentos de gestión interna sobre el manejo de activos, en lo que se debe considerar:

   - La ubicación de la información en un ambiente adecuado que cuente con los accesos restringidos.
   - El almacenamiento de la información debe contemplar mecanismos de seguridad y/o cifrado.

VII.4.3. Manejo de los medios

Objetivo: Prevenir la divulgación, modificación, remoción o destrucción no autorizada de información almacenada en medios.

En ese sentido, el OEFA, en el marco de su compromiso con la Seguridad de la Información, debe:

a) Implementar documentos de gestión interna para la gestión y protección de la información a través de medios removibles (USB, discos duros, entre otros) en concordancia con el esquema de clasificación de la información adoptado; considerando aspectos referidos a:

   - El almacenamiento, procurando el uso de herramientas de cifrado.
   - La autorización del uso de medios removibles.

b) Poner a disposición de la Oficina de Tecnologías de la Información los medios de manera segura cuando ya no se requiera, utilizando procedimientos formales.

c) Proteger los medios que contienen información secreta, reservada o confidencial, contra el acceso no autorizado, el mal uso o la corrupción durante el transporte fuera de la Entidad.

VII.5. Control de acceso

VII.5.1. Requisitos de la Entidad para el control de acceso

Objetivo: Limitar el acceso a la información y a las instalaciones de procesamiento de la información.

En ese sentido, el OEFA, en el marco de su compromiso con la Seguridad de la Información, debe:

a) Establecer los controles de acceso basados en los requisitos y/o necesidades de la Entidad y seguridad de la información, a través de los correspondientes documentos de gestión interna.

b) Establecer disposiciones referidas al control de acceso físico al OEFA y sus ambientes, mediante los respectivos los documentos de gestión interna.

c) Brindar el acceso a los/as usuarios/as solamente a la red y servicios que hayan sido específicamente autorizados a usar. Para lo cual, se debe establecer y/o actualizar los respectivos documentos de gestión interna, que regulen:

- El acceso a plataformas (sistemas de información) aplicaciones (cliente servidor) servicios de instalaciones (software de diseño, ofimática, entre otros) base de datos o cualquier otro recurso informático del OEFA.
- Los requerimientos de autorización y la autorización para el acceso a plataformas, aplicaciones, servicios son brindados por el/la jefe, director/a, subdirector/a o coordinador/a del área usuaria.
- Los tipos de perfiles (usuario general/usuario con privilegios especiales) para el acceso a plataformas, aplicaciones, servicios y base de datos.

VII.5.2. Gestión de acceso de el/la usuario/a

Objetivo: Asegurar el acceso de los/as usuarios/as autorizados/as y prevenir el acceso no autorizado a los sistemas y servicios.

En ese sentido, el OEFA, en el marco de su compromiso con la Seguridad de la Información, debe:

a) Establecer mediante documentos de gestión interna las acciones referidas a:

- Autorizar y solicitar el acceso a los sistemas de información y servicios informáticos para los/as usuarios/as.
- Solicitar la Oficina de Tecnologías de la Información la baja de usuarios/as al finalizar su vínculo laboral o contractual o modalidad formativa.

b) Implementar mediante documentos de gestión interna las acciones para la asignación o revocación de los derechos de acceso según los tipos de usuarios (usuario general/ usuario con privilegios especiales) a los sistemas, servicios informáticos y base de datos en función a sus actividades.

c) Restringir y controlar la asignación y uso de derechos de acceso privilegiado a los/as usuarios, a través de la implementación de registros.

d) Establecer los controles que deben ser adoptados para la asignación de información de autentificación secreta, a través de los respectivos documentos de gestión interna, los cuales deben considerar que:

- Los/as usuarios/as son responsables de la actividad asociada a su usuario de red y a las funciones, servicios o actividades asignadas.
- Las contraseñas deben requerir cierto nivel de complejidad mínimo y no pueden estar asociadas a datos personales que permitan su deducción, como, por ejemplo: nombres propios, nombre de usuario de red, números de documento, dirección, teléfono, entre otros.
- Los criterios para establecer una contraseña segura son:
  - Longitud mínima de ocho (8) caracteres.
  - No usar contraseñas anteriores.
  - Estar formada por al menos tres (3) características de las siguientes: Caracteres alfabéticos en mayúsculas y/o en minúsculas; Caracteres numéricos; Caracteres especiales o extendidos.
- La validez de las contraseñas no podrá superar los tres (3) meses.
- Se debe realizar el bloqueo de la cuenta luego de cinco (5) reiterados intentos fallidos de inicio de sesión.

e) Revisar semestralmente los derechos de acceso de usuario (red, aplicaciones y base de datos) a fin de mantener un control eficaz del acceso a los datos y servicios de información.

f) Remover o adaptar los derechos de acceso a la información e instalaciones de procesamiento de información (incluyendo acceso físico y lógico, llaves, tarjetas de identificación, suscripciones y retiro de cualquier documentación) a los/las usuarios/as de acuerdo con el término de su vínculo laboral o contractual o modalidad formativa.

VII.5.3. Responsabilidades de los/as usuarios/as

Objetivo: Hacer que los/as usuarios/as respondan por la salvaguarda de su información de autentificación.

En ese sentido, el OEFA, en el marco de su compromiso con la Seguridad de la Información, debe exigir a los/as usuarios/as que sigan las políticas y documentos de gestión interna aprobados por la Entidad en el uso y salvaguarda de la información de autentificación secreta.

VII.5.4. Control de acceso a los sistemas y aplicaciones

Objetivo: Prevenir el acceso no autorizado a los sistemas y aplicaciones.

En ese sentido, el OEFA, en el marco de su compromiso con la Seguridad de la Información, debe:

a) Establecer los documentos de gestión interna para el acceso a la información y a las funciones del sistema.

b) Asegurar que los sistemas de información incluyan mecanismos automáticos de gestión de acceso (tales como: bloqueo después de un tiempo de inactividad, obligación de cambio de contraseña, entre otros).

c) Restringir el acceso al código fuente de los programas que el OEFA custodia y/o administra.

VII.6. Criptografía

VII.6.1. Controles criptográficos

Objetivo: Asegurar el uso apropiado y efectivo de la criptografía para proteger la confidencialidad, autenticidad y/o integridad de la información.

En ese sentido, el OEFA, en el marco de su compromiso con la Seguridad de la Información, debe:

a) Usar de controles criptográficos para la protección de la información, los cuales son desarrollados para su implementación en los respectivos documentos de gestión interna.

b) Usar, proteger y establecer el tiempo de vida de las claves criptográficas, siguiendo los procedimientos que se establezcan a través de los respectivos documentos de gestión interna.

VII.7. Seguridad física y ambiental

VII.7.1. Áreas seguras

Objetivo: Impedir acceso físico no autorizado, daño e interferencia a la información y a las instalaciones de procesamiento de la información de la Entidad.

En ese sentido, el OEFA, en el marco de su compromiso con la Seguridad de la Información, debe:

a) Verificar: *(i)* la identificación de las personas que ingresan al OEFA; *(ii)* uso visible de los fotochecks institucionales –para los/as servidores/ras civiles, practicantes preprofesionales y profesionales y secigristas– y los pases –para los/las contratistas, terceros/as seleccionados/as, y visitas– correspondientes durante su permanencia en el OEFA

b) Mantener un registro de los datos de los/as visitantes a los funcionarios públicos, que debe contener la siguiente información día, hora y motivo de visita.

c) Anunciar al personal de seguridad el ingreso de los/as visitantes, contratistas y/o terceros/as seleccionados/as a las instalaciones de la Entidad, previo a su desplazamiento a las oficinas.

d) Controlar y restringir el acceso donde se encuentre el Centro de Cómputo de la Oficina de Tecnologías de la Información, permitiendo el ingreso a los/as servidores/as civiles que laboran en ese ambiente y a los/as practicantes preprofesionales y profesionales, contratistas y terceros/as seleccionados/as que tengan autorización.

e) Definir e implementar controles apropiados para la seguridad de las Oficinas en la que se realice el procesamiento de información secreta, confidencial y/o reservada.

f) Contar con sistemas de detección y extinción de incendios en aquellas oficinas donde se realice el tratamiento de información; cuya administración y monitoreo debe encontrar a cargo del área correspondiente.

g) Examinar el material que ingresa a la zona de despacho y recepción de materiales para detectar cualquier material peligroso ante de su envío al ambiente de destino.

h) Verificar que los bienes, materiales, equipos u otros activos que ingrese a la Entidad, sean debidamente registrados.

i) Verificar la autorización de ingreso y salida de cualquier activo de la Entidad, comprobando la información registrada.

j) Asegurar que los contratistas y terceros/as seleccionadas:

- Que accedan a las instalaciones del Centro de Cómputo solo usen el material estrictamente necesario para llevar a cabo las actividades contratadas.
- No ingresen a las instalaciones del Centro de Cómputo sin la presencia de el/la servidor/a civil a cargo.

k) Asegurar que las puertas y ventanas exteriores e interiores estén protegidos contra accesos no autorizados.

l) Asegurar que los ambientes de procesamiento de la información sensible posean una infraestructura perimetral adecuada, que impida su vulneración a través de delitos contra el patrimonio.

m) Proporcionar un ambiente adecuado para la conservación de medios magnéticos y equipos.

n) Proporcionar un ambiente adecuado para la conservación de los documentos de tipo archivístico y bibliográfico.

o) Mantener en condiciones óptimas de limpieza y de funcionalidad el centro de cómputo y archivo de la Entidad.

VII.7.2. Equipos

Objetivo: Prevenir la pérdida, daño, robo o compromiso de activos e interrupción de las operaciones de la Entidad.

En ese sentido, el OEFA, en el marco de su compromiso con la Seguridad de la Información, debe:

a) Verificar que los equipos informáticos no se encuentren expuestos a amenazas y/o peligros ambientales; de acuerdo a los documentos de gestión interna que se implementen y que las áreas deben cumplir para dicho fin.

b) Evitar la apertura de los equipos informáticos por parte de los usuarios; salvo, previa autorización de la Oficina de Tecnologías de la Información, en caso corresponda.

c) Contar con controles para la seguridad de la apertura de equipos informáticos.

d) Proteger los equipos contra fallas de electricidad y otras alteraciones causadas por fallas en los servicios de suministro.

e) Asegurar que los cables que transportan datos se encuentren debidamente protegidos contra la interceptación, interferencia o posibles daños.

f) Efectuar el mantenimiento de los equipos informáticos de la Entidad.

g) Aplicar controles de seguridad de la información en los equipos informáticos a emplearse en los exteriores de las instalaciones de la Entidad.

h) Asegurar que la información clasificada como no pública sea borrada de manera irreversible; así como también en el caso que contengan software propietario, cuando se encuentre en medios de almacenamiento que serán reutilizados, reemplazados o dados de baja.

i) Establecer la protección apropiada para los equipos desatendidos, lo cual es de conocimiento de los/las usuarios.

j) Cumplir con lo siguiente:

Pantalla Limpia

- El/la usuario/a al ausentarse de su puesto donde desarrolla funciones, servicios o actividades debe bloquear la sesión de los equipos de cómputo mediante las teclas CTRL + ATL + SUPR (opción bloquear) o tecla Windows + L, para proteger el acceso a las aplicaciones y servicios de la entidad de personas no autorizadas.
- La Oficina de Tecnologías de la Información implementa el bloqueo automático de la sesión de usuario mediante el directorio activo al transcurrir cinco (5) minutos de inactividad en el equipo de cómputo.
- La Oficina de Tecnologías de la Información de manera coordinada con la Oficina de Relaciones Institucionales y Atención a la Ciudadanía, determinan y configuran el fondo de pantalla institucional de los equipos de cómputo de la Entidad.
- La pantalla del computador (escritorio) no debe contener ningún tipo de archivo, salvo los accesos directos a las aplicaciones necesarias para que los funcionarios o contratistas ejerzan sus funciones o cumplan sus obligaciones contractuales, según el caso.

Escritorio Limpio

- Los puestos donde el/la usuario/a desarrolla sus funciones, servicios o actividades deben permanecer limpios y ordenados.
- Cuando se imprima o digitalice documentos con información no pública, estos deben retirarse inmediatamente de dichos dispositivos.
- Los dispositivos de impresión y digitalización deben permanecer limpios de documentos y estar protegidos de su uso no autorizado.
- Los documentos que elaboren los/as usuarios/as, en el ejercicio de sus funciones y actividades o en el cumplimiento de sus obligaciones contractuales, según sea el caso, deben guardarse en la carpeta de almacenamiento en red o almacenamiento en la nube dispuesta por la Entidad.
- Los gabinetes, cajones y archivadores de contengan documentos y/o medios extraíbles con información, deben quedar cerrados durante la hora de almuerzo y al finalizar la jornada laboral, actividades o servicios.
- El/la usuario/a debe apagar los equipos informáticos que use al culminar su jornada laboral, actividades o servicios en el día.
- Reportar a la mesa de ayuda (soporte@oefa.gob.pe) los dispositivos extraíbles de almacenamiento externos o USB olvidados en las instalaciones y asegurar no conectarla en los equipos de cómputos de la Entidad.

VII.8. Seguridad de las operaciones

VII.8.1. Procedimiento y responsabilidades operativas

Objetivo: Asegurar que las operaciones de instalaciones de procesamiento de la información sean correctas y seguras.

En ese sentido, el OEFA, en el marco de su compromiso con la Seguridad de la Información, debe:

a) Establecer documentos de gestión interna, así como las responsabilidades para la gestión y operación de los medios de procesamientos y almacenamiento de la información.

b) Asegurar la segregación de funciones para reducir el riesgo de un uso indebido del sistema.

c) Controlar los cambios en la Entidad, así como en sus procesos y los que se realicen en las instalaciones de procesamiento de la información y sistemas que afecten la seguridad de la información.

d) Monitorear el uso de recursos para hacer proyecciones de futuros requisitos de capacidad, que aseguren el desempeño requerido por los servicios informáticos y sistemas de operación.

e) Verificar que, durante el ciclo de desarrollo de software, se establezcan y trabajen en ambientes de desarrollo, prueba y producción por separado.

f) Resguardar la data de producción del OEFA mediante los backups de información respectivos.

g) Realizar un monitoreo de servicios informáticos, servicios web, centro de datos, conexiones de red en las oficinas desconcentradas y en la sede central.

h) Gestionar el soporte técnico para los usuarios, según su escalabilidad de atención por especialistas o servicios tercerizados, de ser el caso.

VII.8.2. Protección contra códigos maliciosos

Objetivo: Asegurar que la información y las instalaciones del procesamiento de la información se encuentren protegidas contra códigos maliciosos.

En ese sentido, el OEFA, en el marco de su compromiso con la Seguridad de la Información, debe:

a) Establecer los documentos de gestión interna a fin de minimizar los riesgos relacionados con la obtención de archivos y software, desde o a través de redes externas, o por cualquier otro medio, señalando las medidas de protección a aplicar.

b) Implementar un sistema de protección informático en los sistemas de información de la Entidad frente a cualquier tipo de virus que se detecten en los equipos informáticos del OEFA.

c) Mantener instalados y actualizados periódicamente los sistemas de protección de antivirus en cada equipo computador de los/as usuarios/as del OEFA, así como las conexiones de la red interna.

d) Implementar las herramientas de detección y escaneo previo cuando se trate de la lectura de dispositivos de almacenamiento externos ajenos al OEFA; así como, en los servidores físicos dentro de la Entidad.

e) Asegurar que el equipo que no cuente con una herramienta de protección contra códigos maliciosos no sea conectado a la red de datos del OEFA.

f) Contar con programas adecuados que permitan la recuperación de data y archivos en los computadores del OEFA, de haber sido afectados por un código malicioso.

g) Asegurar que se cuente con un equipamiento perimetral de seguridad, a fin de proteger ante amenazas, permitiendo el control de tráfico de entrada y salida para la red de datos del OEFA.

h) Concientizar a los/as servidores/as civiles, contratistas y terceros/as seleccionados/as del OEFA sobre la importancia de la detección, prevención y recuperación de datos respecto a los códigos maliciosos que puedan afectar el adecuado funcionamiento de los sistemas de información; así como, protocolos para afrontar un evento u ocurrencia de infección de virus o malware.

Los/as usuarios/as no autorizados por la Oficina de Tecnologías de la Información, se encuentran prohibidos de realizar: *(i)* la desinstalación y/o desactivación de softwares y/o herramientas de seguridad avaladas previamente por la Oficina de Tecnologías de la Información; y, *(ii)* la instalación y ejecución de programas propios u obtenidos a través de Internet, correo electrónico u otro medio, en los equipos del OEFA, sin la debida autorización de la Oficina de Tecnologías de la Información.

VII.8.3. Respaldo

Objetivo: Proteger al OEFA contra la pérdida de datos.

En ese sentido, el OEFA, en el marco de su compromiso con la Seguridad de la Información, debe:

a) Realizar periódicamente las copias de respaldo de la información almacenada en los equipos informáticos del Centro de Cómputo de la Oficina de Tecnologías de la Información; así como, efectuar las pruebas de restauración de la información en concordancia con su plan o programa correspondiente y como consecuencias de las mismas, documentar las incidencias que se hayan puesto de manifiesto durante su desarrollo.

b) Asegurar que las copias de respaldo de la información almacenada en los equipos informáticos del Centro de Cómputo de la Oficina de Tecnologías de la Información sean resguardados en una ubicación externa a la Entidad o contar con los servicios de un contratista de almacenamiento de respaldo de información que reúna las condiciones adecuadas de acondicionamiento, temperatura y humedad, a fin de asegurar la continuidad de las operaciones; y, siendo trasladada con los elementos de seguridad adecuados y manteniendo un inventario actualizado de la información almacenada externamente.

c) Realizar las copias de respaldo de la información de los equipos de los/as usuarios/as a solicitud de el/la jefe/a, director/a, subdirector/a o coordinador/a del área.

d) Establecer el periodo de retención de la información esencial para la Entidad, en atención al Programa de Control de Documentos Archivísticos; así como, el uso del espacio físico disponible para el almacenamiento.

e) Definir el periodo de existencia para las copias de seguridad y los procedimientos o protocolos a seguir para su destrucción definitiva una vez concluido tal período, de acuerdo a los documentos de gestión interna y a las disposiciones emitidas por el Archivo General de la Nación.

f) Destruir o eliminar de manera segura la información del OEFA, cuando deja de ser necesaria, de acuerdo a los documentos de gestión interna y a las disposiciones emitidas por el Archivo General de la Nación. Para dar soporte a este requisito, los/as propietarios/as de la información deberán revisar de forma periódica, el valor y la utilidad de la información almacenada.

g) Contar con un programa de mantenimiento preventivo y correctivo para los equipos y los medios de respaldo, a efectos de asegurar su correcto funcionamiento.

h) Estimar anticipadamente la cantidad necesaria de medios magnéticos requeridos para efectuar las copias de respaldo, a efectos de asegurar su correcto funcionamiento.

i) Estimar anticipadamente la cantidad necesaria de medios magnéticos requerido para efectuar las copias de respaldo; en caso no contar con ello, solicitar su oportuna adquisición.

j) Revisar periódicamente la vigencia tecnológica de los equipos y softwares utilizados para el respaldo y recuperación de la información.

VII.8.4. Registros y monitoreo

Objetivo: Registrar eventos y generar evidencias.

En ese sentido, el OEFA, en el marco de su compromiso con la Seguridad de la Información, debe:

a) Producir, mantener y revisar periódicamente los registros y otros relacionados con eventos de actividad de el/la usuario/a, excepciones, fallas y eventos de seguridad de la información; así como, protegerlos contra posibles alteraciones y accesos no autorizados.

b) Implementar controles que aseguren que los eventos de sistemas de información, no sean manipulados, tales como la activación de registros de auditoría. Obtener las copias de seguridad de estos eventos mensualmente.

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

d) Registrar y revisar trimestralmente las actividades de los administradores de los sistemas de información y del operador del sistema.

e) Sincronizar los relojes de todos los sistemas de procesamiento de información en base a una fuente de sincronización única.

VII.8.5. Control de software operacional

Objetivo: Asegurar la integridad de los sistemas operacionales.

En ese sentido, el OEFA, en el marco de su compromiso con la Seguridad de la Información, debe implementar documentos de gestión interna para controlar la instalación de softwares en sistemas operacionales, esto mediante la restricción de otorgamiento de privilegios para evitar incidentes de seguridad de la información y violaciones de derechos de propiedad intelectual.

VII.8.6. Gestión de vulnerabilidad técnica

Objetivo: Prevenir la explotación de vulnerabilidades técnicas.

En ese sentido, el OEFA, en el marco de su compromiso con la Seguridad de la Información, debe:

a) Realizar, previa programación, el análisis de vulnerabilidades técnicas más relevantes de los sistemas de información y su infraestructura, a fin de programar las acciones necesarias para prevenir o mitigar los riesgos identificados en el análisis. Estas acciones serán realizadas con una periodicidad mínima anual.

b) Implementar controles que regulen la instalación de softwares dentro de la Entidad.

c) Aplicar los controles de medidas correctivas necesarios, en función del riesgo de la vulnerabilidad encontrada.

VII.8.7. Consideraciones para la auditoría de los sistemas de información

Objetivo: Minimizar el impacto de las actividades de auditoría en los sistemas operacionales.

En ese sentido, el OEFA, en el marco de su compromiso con la Seguridad de la Información, debe planificar las actividades semestrales de auditoría que impliquen verificaciones en los sistemas de producción, para minimizar el riesgo de interrupción de los procesos de la Entidad. La referida planificación debe realizar en coordinación con la Oficina de Tecnologías de la Información, de corresponder; así como de el/la Oficial de Seguridad de la Información y de el/la propietario/a de la información, en el cual opera el sistema de información a ser auditado.

VII.9. Seguridad de las comunicaciones

VII.9.1. Gestión de seguridad de la red

Objetivo: Asegurar la protección de la información en redes y la protección de la infraestructura de soporte.

En ese sentido, el OEFA, en el marco de su compromiso con la Seguridad de la Información, debe:

a) Gestionar, proteger y conservar la seguridad de los datos en las redes de la Entidad.

b) Identificar e incluir en los acuerdos de servicios de red, los mecanismos de seguridad, niveles de servicio y requisitos de gestión de los servicios de red; ya sea que estos servicios se provean internamente o sean tercerizados. Se debe asegurar que los controles de seguridad, los acuerdos de niveles de servicio y los requisitos de gestión de los servicios de red, suscritos con los contratistas, sean implementados y cumplidos.

c) Los grupos de servicios de información, usuarios/as y sistemas de información deben ser segregados en dominios de red separados por unidades organizativas.

d) Establecer controles y medidas especiales para salvaguardar la confidencialidad e integrar los datos que se transfieren a través de redes públicas e inalámbricas, así como para proteger los sistemas conectados, tales como firewall, filtro de contenidos, antispam, entre otros.

e) Monitorear, revisar y auditar regularmente los servicios provistos por los/as contratistas.

f) Planificar y autorizar los cambios en los servicios que proveen los/as contratistas, considerado los riesgos que podrían generar, en el marco de la normativa aplicable.

g) Autentificar mediante usuario y contraseña el ingreso a la red del OEFA.

h) Restringir el acceso para el uso de los servicios de red y acceso a las aplicaciones.

VII.9.2. Transferencia de información

Objetivo: Mantener la seguridad de la información intercambiada dentro del OEFA y con cualquier contra entidad.

Así, el OEFA, en el marco de su compromiso con la Seguridad de la Información, debe proponer e implementar controles de seguridad de la información para proteger el intercambio de información por medio del uso de cualquier tipo de recurso de comunicación, en comunicación con su clasificación.

Asimismo, el/la jefe, director/a, subdirector/a o coordinador/a del área usuaria deben:

a) Asegurar la implementación de controles de seguridad de la información para la transferencia de la información según su clasificación.

b) Establecer un acuerdo y/o cláusula de confidencialidad y no divulgación previa a la transferencia de información que no sea de carácter público ya sea dentro del OEFA o contra una entidad externa.

c) Intercambiar información (incluyendo la trazabilidad, no repudio, cadena de custodia, control de acceso) entre las diferentes áreas del OEFA y fuera de este, en función de las funciones, servicios y actividades de cada servidor/a civil, contratista, tercero/a seleccionado/a, practicante pre profesional y profesional y secigrista de la Entidad.

d) Asegurar el correcto direccionamiento y transporte de la mensajería electrónica.

e) Entregar la información digital por medios magnéticos o de estado sólido, de forma personal al destinatario, en un sobre cerrado y sellado, su entrega debe quedar registrada.

f) Incorporar al acuerdo de transferencia de información lo siguiente:

- Administración de responsabilidades para controlar y notificar la transmisión, el despacho y la recepción.
- Procedimientos para garantizar la capacidad de seguimiento y no repudiación.
- Responsabilidades en caso de incidentes de seguridad de la información tales como la pérdida de los datos.
- Cualquier control especial necesario para proteger elementos sensibles como criptografía.
- Mantener una cadena de custodias para la información durante el tránsito.
- Niveles aceptables de control de acceso.

g) Considerar para el acceso de terceros/as seleccionados/as y contratistas la información reservada o confidencial, los siguientes requisitos:

- Una definición de la información que se protegerá.
- Duración esperada del acuerdo, en caso sea necesario mantener la confidencialidad de manera indefinida.
- Acciones necesarias al terminar un acuerdo.
- Responsabilidades y acciones de los firmantes para evitar la divulgación de información no autorizada.
- Acciones necesarias al terminar un acuerdo.
- Propiedad de la información, la propiedad intelectual y cómo esta se relaciona con la protección de información confidencial.
- El uso permitido de la información y los derechos del firmante para utilizar la información.
- El proceso para la notificación y reporte de la divulgación no autorizada o fuga de información confidencial.
- Términos para la devolución o destrucción de la información al término del acuerdo.
- Medidas esperadas que se tomarán en caso de un incumplimiento del acuerdo.

h) Contar con la autorización de el/la responsable de los activos de información para el retiro y/o desplazamiento de estos de los ambientes de procesamiento, almacenamiento y comunicación de información, utilizando los medios de transporte autorizados por el OEFA.

i) No comprometer a la Entidad en casos de difamación, acoso, suplantación, reenvío de mensajes en cadena, compras no autorizadas entre otros.

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

Para ello, el OEFA debe:

a) Asegurar que la información cuya clasificación no es pública, solo sea compartida entre los/as usuarios/as autorizados/as por el/la propietario/a de la información y contando con los controles, concordancia con su clasificación.

b) Evitar que los documentos con información que no sea de carácter público, sean expuestos a personas no autorizadas mientras permanezca bajo su custodia (incluye el proceso de impresión).

c) Acatar las disposiciones del buen uso del correo institucional, internet y servicio de telefonía emitidas por el OEFA.

VII.10. Adquisición, desarrollo y mantenimiento de sistemas

VII.10.1. Requisitos de seguridad de los sistemas de información

Objetivo: Asegurar que la seguridad de la información sea una parte integral de los sistemas de información a través del ciclo de vida completo.

En ese sentido, el OEFA, en el marco de su compromiso con la Seguridad de la Información, debe:

a) Incluir en los requisitos de los nuevos sistemas de información o en las propuestas de mejoras de los sistemas de información existente, aquellos relacionados con la seguridad de la información, desde las etapas iniciales del proyecto.

b) Proteger la información involucrada en los servicios de aplicaciones a través de redes públicas, de actividades fraudulentas, disputas de contrato o divulgaciones no autorizadas y modificaciones.

c) Proteger la información involucrada en las transacciones de los servicios de las aplicaciones, para prevenir la transmisión incompleta, ruteo incorrecto, alteración no autorizada de mensajes, divulgación no autorizada, duplicación o respuesta no autorizada de mensajes.

d) Asegurar que los cambios a realizar, solicitados formalmente por los/as propietarios/as de la información, no causen riesgos de seguridad (de ocurrir un incidente de seguridad en la implementación de un cambio, debe deshabilitarse para su posterior subsanación).

e) Realizar pruebas de calidad de software, validando los datos de entrada y de salida esperados.

VII.10.2. Seguridad en los procesos de desarrollo y soporte

Objetivo: Garantizar que la seguridad de la información esté diseñada e implementada dentro del ciclo de vida de desarrollo de los sistemas de información.

En ese sentido, el OEFA, en el marco de su compromiso con la Seguridad de la Información, debe:

a) Establecer disposiciones para el desarrollo de software y sistemas seguros para la Entidad.

b) Establecer y aplicar procedimientos de control de cambio a los sistemas de información dentro del ciclo de vida del desarrollo.

c) Garantizar que el ambiente de desarrollo debe de mantenerse seguro y siempre separado del ambiente de pruebas y de producción, debiendo existir controles de acceso adecuados para cada uno de ellos.

d) Evitar la alteración de los sistemas de información, que no sean aprobados por los/as propietarios/as de los activos de información.

e) Garantizar los cambios en las plataformas operativas, a través de la implementación de controles, pruebas y verificación, antes de su despliegue en el ambiente de producción, incluyendo respaldos, recursos, criterios de aceptación del cambio y un plan de rollback (retornar a una versión anterior).

f) Proteger el acceso a la información de producción que contenga datos sensibles de los/as usuarios/as que desarrollen funciones y/o actividades de programación en el OEFA.

g) Los sistemas desarrollados o modificados por terceras partes, deben cumplir con lo establecido en la presente Política, incluyendo los criterios de seguridad.

h) Establecer con los/as usuarios/as cláusulas previas y/o acuerdos que resguarden la propiedad intelectual y aseguren los niveles de confidencialidad de la información manejada en los proyectos.

i) Supervisar y monitorear la actividad de desarrollo de sistemas contratado externamente.

j) Establecer gestión de vulnerabilidades técnicas orientada a analizar los problemas de seguridad (vulnerabilidades) que surgen en los productos de software, asociada a proponer las medidas de mitigación al riesgo definido. Al menos una vez al año se debe realizar un escaneo de las aplicaciones, servicios y sistemas operativos en busca de vulnerabilidades, manteniendo un registro de los resultados y las acciones correctivas tomadas.

k) Efectuar validaciones y evaluaciones de seguridad y funcionalidad durante las etapas del ciclo de vida del proyecto.

l) Incluir en los programas críticos, la generación de registros de auditoría, considerando como mínimo la identidad de el/la usuario/a que lee o escribe, la fecha y hora, y el IP de origen. Estos registros deben ser protegidos contra la manipulación no autorizada.

m) Establecer, documentar y aplicar principios de seguridad en ingeniería de sistemas para la implementación de los sistemas de información.

n) Inscribir y/o registrar en INDECOPI, a nombre del OEFA, el software desarrollado (incluido el desarrollado por los contratistas), en el registro intelectual respectivo; bajo la responsabilidad de la Oficina de Tecnologías de la Información. Ello a fin de acogerse a los resguardos que estipula la normativa relacionada a la propiedad intelectual.

VII.10.3. Datos de prueba

Objetivo: Asegurar la protección de datos utilizados para la prueba.

En ese sentido, el OEFA, en el marco de su compromiso con la Seguridad de la Información, debe:

a) Asegurar que los datos personales utilizados en los ambientes de desarrollo y de pruebas sean anonimizados previamente.

b) Asegurar que las pruebas de los sistemas de información se realicen en un ambiente controlado y con los datos seleccionados para tal fin.

VII.11. Relaciones con los/as terceros/as seleccionados/as y contratistas

VII.11.1. Seguridad de la información en las relaciones con los/as terceros/as seleccionados/as y contratistas

Objetivo: Asegurar protección a los activos de información de la Entidad que son accesibles por los/as contratistas y terceros/as seleccionados/as.

En ese sentido, el OEFA, en el marco de su compromiso con la Seguridad de la Información, debe:

a) Asegurar que la información emitida y/o recibida con los/as terceros/as seleccionados/as y contratistas respete los documentos de gestión interna; mitigando los riesgos asociados con el acceso por parte de los/as terceros/as seleccionados/as y contratistas a los activos de la Entidad.

b) Prever que los/as propietarios/as y custodios de información aseguren que los términos y condiciones para el intercambio de información con los contratistas, que accedan, procesen, almacenen, comuniquen o provean componentes de infraestructura de tecnologías de la información para la información del OEFA, se encuentren documentados en un acuerdo.

c) Identificar en los acuerdos con los/as contratistas, los requisitos para abordar los riesgos de seguridad de la información asociado con los servicios de procesamiento de información y la cadena de suministro de productos.

d) Suscribir acuerdos y/o cláusulas de confidencialidad, cuando se requiera información por parte del OEFA a los/as terceros/as seleccionados/as y contratistas.

e) Supervisar que el monitoreo y la revisión de los servicios externos realizados por los contratistas cumplan con los términos de seguridad de la información y que los incidentes y problemas en la seguridad de información sean manejados de forma coordinada con la Oficina de Tecnologías de la Información.

VII.11.2. Gestión de entrega de servicios de el/la tercero/a seleccionado/a y contratista

Objetivo: Mantener un nivel de seguridad de la información y entrega de servicios acordado en línea con los acuerdos con los/as terceros/as seleccionados/as y contratistas.

En ese sentido, el OEFA, en el marco de su compromiso con la Seguridad de la Información, debe:

a) Monitorear, revisar y auditar regularmente la entrega de servicios por parte de los/as terceros/as seleccionados/as y contratistas.

b) Gestionar los cambios a la provisión de servicios por parte de los/as terceros/as seleccionados/as y contratistas, incluyendo el mantenimiento y mejoramiento de los documentos de gestión interna existentes de seguridad de la información, tomando en cuenta la criticidad de la información del negocio, sistemas y procesos involucrados y una reevaluación de riesgos.

VII.12. Gestión de incidentes de seguridad de la información

VII.12.1. Gestión de incidentes de seguridad de la información y mejoras

Objetivo: Asegurar un enfoque consistente y efectivo a la gestión de incidentes de seguridad de la información incluyendo la comunicación sobre eventos de seguridad y debilidades.

En ese sentido, el OEFA, en el marco de su compromiso con la Seguridad de la Información, debe:

a) Establecer los documentos de gestión y responsabilidades necesarias, a fin de asegurar una respuesta rápida, efectiva y ordenada a los incidentes de seguridad de la información.

b) Identificar, clasificar y reportar oportunamente a la Mesa de Ayuda de la Oficina de Tecnologías de la Información cualquier evento, incidente y/o debilidad de seguridad de información de la Información, a fin de brindar una atención oportuna.

c) Crear y monitorear el reporte de debilidades, eventos y/o incidentes que afecten la seguridad de la información; para ello, el/la Oficial de Seguridad de la Información realiza el seguimiento y cierre de los incidentes.

d) Priorizar el conocimiento adquirido, a partir de analizar y resolver los incidentes de seguridad de la información, reduciendo la probabilidad o el impacto de incidentes futuros.

e) Definir y elaborar los documentos de gestión para la identificación, recolección, adquisición y preservación de información que sirva como evidencia ante la ocurrencia de debilidades y/o incidencias.

VII.13. Aspectos de seguridad de la información en la gestión de continuidad del negocio

VII.13.1. Continuidad de seguridad de la información

Objetivo: La continuidad de seguridad de la información debe estar embebida en los sistemas de gestión de continuidad del negocio del OEFA.

En ese sentido, el OEFA, en el marco de su compromiso con la Seguridad de la Información, debe:

a) Determinar los requisitos de seguridad de la información y continuidad de la gestión de seguridad de la información en situaciones adversas, sea durante una crisis o desastre.

b) Establecer, documentar implementar y mantener los documentos de gestión interna; así como, controles internos para asegurar el nivel requerido de continuidad de seguridad de la información durante una situación adversa.

c) Realizar las pruebas periódicas y de mantenimiento establecidos en los documentos de gestión interna, permitiendo la continuidad de la información ante situaciones adversas.

d) Verificar los controles internos de continuidad de seguridad de la información que el OEFA ha establecido e implementado a intervalos regulares para asegurarse que son válidos y efectivos durante situaciones adversas.

VII.13.2. Redundancias

Objetivo: Asegurar la disponibilidad de las instalaciones y procesamiento de la información.

En ese sentido, el OEFA, en el marco de su compromiso con la Seguridad de la Información, debe implementar instalaciones de procesamiento de la información con redundancia suficiente para cumplir con los requisitos de disponibilidad.

VII.14. Cumplimiento

VII.14.1. Cumplimiento con requisitos legales y contractuales

Objetivo: Evitar infracciones de las obligaciones legales, estatutarias, regulatorias, o contractuales relacionadas a la seguridad de la información y a cualquier requisito de seguridad.

En ese sentido, el OEFA, en el marco de su compromiso con la Seguridad de la Información, debe:

a) Identificar, documentar y actualizar los requisitos legislativos, estatutarios, regulatorios y contractuales relevantes; así como el enfoque del OEFA, en cada sistema de información y para la Entidad.

b) Implementar los procedimientos necesarios para asegurar el cumplimiento de los requisitos legislativos, regulatorios y contractuales relacionados a los derechos de propiedad intelectual y uso de productos de software propietario y sistemas de información patentados.

c) Proteger los registros de pérdida, destrucción, falsificación, acceso no autorizado y divulgación no autorizada de acuerdo con los requisitos legislativos, regulatorios, contractuales y de la Entidad.

d) Registrar los activos que requieren protección de los derechos de propiedad intelectual.

e) Asegurar la privacidad y protección de datos personales, de conformidad con la Ley N° 29733, Ley de Protección de Datos Personales y la Política de Protección de Datos personales del OEFA.

f) Utilizar los controles criptográficos en cumplimiento de los acuerdos, legislación y regulación correspondiente.

VII.14.2. Revisiones de seguridad de la información

Objetivo: Asegurar que la seguridad de la información está implementada y es operada de acuerdo con las políticas y documentos de gestión de la Entidad.

En ese sentido, el OEFA, en el marco de su compromiso con la Seguridad de la Información, debe:

a) Revisar independientemente y en intervalos planeados, el enfoque de la Entidad respecto al manejo de la seguridad de la información y su implementación (objetivos de control, controles, políticas, y documentos de gestión interna para la seguridad de información).

b) Revisar periódicamente el cumplimiento del procesamiento de la información y de los procedimientos dentro del área de responsabilidad a su cargo con los documentos de gestión y otros requisitos de seguridad apropiados.

c) Revisar periódicamente los sistemas de información respecto al cumplimiento de las políticas y documentos de gestión de seguridad de la información del OEFA.

X. RESPONSABILIDADES

Los órganos, unidades orgánicas, coordinaciones, unidades funcionales y colegiados de la Entidad, en el marco de sus funciones establecidas en los documentos de gestión interna y actos resolutivos correspondientes, son responsables de promover el cumplimiento de las Políticas Específicas de Seguridad de la Información del OEFA.

XI. ANEXO

Anexo N° 1: Matriz de Objetivos Estratégicos Institucionales alineados a las Políticas Específicas del SGSI

Anexo N° 1

Matriz de Objetivos Estratégicos Institucionales alineados a las Políticas Específicas del SGSI

OEI	AEI	Política y Objetivos de Seguridad de la Información	Dirección de la Alta Dirección para la seguridad de la Información	Organización de la seguridad de la información	Seguridad de los recursos humanos	Gestión de activos	Control de acceso	Criptografía	Seguridad física y ambiental	Seguridad de las operaciones	Seguridad de la comunicaciones	Adquisición, desarrollo y mantenimiento de sistemas	Relaciones con los proveedores	Gestión de incidentes de seguridad de la información	Aspectos de seguridad de la información en la gestión de continuidad del negocio	Cumplimiento
OEI.03. Modernizar la gestión institucional	AEI.03.02. Herramientas tecnológicas implementadas para el sistema de fiscalización ambiental en el marco del gobierno digital (comprenderá acciones de automatización de los procesos estratégicos y de apoyo de la entidad)	"Somos una Entidad que brinda servicios de evaluación, supervisión, fiscalización y de aplicación de incentivos en materia ambiental, con respeto de los derechos y equilibrio entre la inversión y la protección del ambiente; en la cual, la información es un recurso estratégico que genera conocimiento, asegura la continuidad de nuestras operaciones y fortalece la confianza con la población, la empresa y el Estado. Nuestro compromiso con la seguridad de la información en la Entidad se enmarca en la implementación y continuidad de mecanismos para asegurar su confidencialidad, disponibilidad e integridad, así como la mejora continua del Sistema de Gestión de Seguridad de la Información, en cumplimiento del marco legal vigente y estándares internacionales". Objetivo 1: Implementar los controles de seguridad de la información en el marco de la Norma Técnica Peruana - NTP ISO/IEC 27001 :2014, en atención a la gestión de riesgos y mejora continua para asegurar la confidencialidad, integridad y disponibilidad de la información del OEFA. Objetivo 2: Difundir las políticas y controles de seguridad de la información para concientizar a los colaboradores y contratistas del OEFA, su contribución a la efectividad del Sistema de Gestión de la Información.			X	X	X	X	X	X	X	X	X	X	X
	AEI.03.03. Gestión administrativa efectiva en el manejo de los recursos del OEFA				X	X	X	X	X	X	X	X	X	X	X	X
	AEI.03.04 Gestión estratégica y operativa efectiva en el OEFA				X	X	X	X	X	X	X	X	X	X	X	X
	AEI.03.05 Imagen institucional fortalecida del OEFA					X	X	X	X	X	X	X	X	X	X	X
	AEI.03.06 Gestión del talento humano con enfoque de género fortalecida en el OEFA				X	X	X	X		X	X			X	X	X
	AEI.03.07 Procesos de gestión documental fortalecidos para el OEFA				X	X	X	X	X	X	X	X	X	X	X	X