POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

	Cargo	Nombre
Elaborado por:	**Oficial de Seguridad de la Información y Protección de Datos Personales y Abiertos**	Jenny Castañeda Zubiaur
Revisado por:	**Comité de Gobierno Digital**	Rafael Muente Schwarz
		Sergio Cifuentes Castañeda
		Félix Vasi Zevallos
		Andrés Aguayo Bustamante
		Alberto Arequipeño Tamara
		Tatiana Piccini Anton
		Cynthia Aguirre Campos
		Jessika Márquez Oppe
		Jenny Castañeda Zubiaur
Aprobado por:	**Presidente**	Rafael Muente Schwarz

TABLA DE CONTENIDO

CONTROL DE CAMBIOS

N° Versión	Fecha	Descripción del cambio	Responsable del Documento
4	22/08/2019	Se unifican las políticas de seguridad de la información en un único documento. Se actualiza estructura del documento.	Oficial de Seguridad de la Información
5	22/10/2020	Se reformula la Política de Seguridad de la Información incluyendo lo relacionado a cumplimiento de los requisitos legales aplicables. Se modifica las políticas específicas relacionadas a: a) Dispositivos móviles: se incluye como medio autorizado de conexión a internet, la red inalámbrica privada del colaborador. b) Teletrabajo o acceso remoto: • Se incluirá el término trabajo remoto. • Se retirará la validación del Oficial de Seguridad para las solicitudes de teletrabajo, acceso remoto o trabajo remoto. Se mantendrá la validación del acceso remoto de proveedores especializados. • Se modificará el lineamiento de vigencia del acceso remoto o trabajo remoto que limitaba a renovaciones cada 03 meses, incluyéndose en su lugar que cada Responsable de la UO debe revisar de forma trimestral la relación de sus colaboradores con acceso remoto, trabajo remoto o teletrabajo y validar su correspondencia ante la OTI. c) Uso adecuado de los activos: Se incluye que los equipos de cómputo que son entregados a los colaboradores en calidad de préstamo serán configurados con los puertos de almacenamiento extraíbles bloqueados. d) Uso de Internet: Se modifica lineamiento relacionado al uso de servicios en la nube, “Los colaboradores del OSIPTEL sólo podrán hacer uso del servicio de almacenamiento en la nube institucional, previa autorización de la máxima autoridad de su UO y de acuerdo a los mecanismos de control técnicos establecidos por la OTI.	Oficial de Seguridad de la Información
6	05/08/2021	Se actualizó en 5.1 definición de “equipo desatendido” Se actualiza 6.6 y se precisa la identificación del propietario del activo Se incluyó 6.6.1. Clasificación de la información Se incluyó 6.6.2. Medios removibles Se incluyó 6.6.3. Disposición de medios Se incluyó 6.11.1. Gestión del cambio Se incluyó 6.11.2. Gestión de la capacidad Se actualizó 6.11.4 Respaldo de Información Se incluyó 6.11.5. Protección de información de registros Se actualizó 6.12 Transferencia de Información Se incluyó 6.14. Controles criptográficos	Oficial de Seguridad de la Información

1. Objetivo

El objetivo del presente documento es normar los requisitos de seguridad de la información dentro de los diferentes procesos del OSIPTEL para proteger la confidencialidad, disponibilidad e integridad de la información, recursos, servicios e instalaciones.

2. Alcance

Este documento se aplica a todo el Sistema de Gestión de Seguridad de la Información (SGSI).
Los usuarios de este documento son todas las partes interesadas del SGSI.

3. Base Legal

- MS-SGSI-001 “Manual del Sistema de Gestión de Seguridad de la Información”.
- Directiva N° 001-2018-GG/OSIPTEL “Directiva para la gestión del parque informático”.
- P-GRH-01 “Procedimiento Inducción del Colaborador”.
- P-GTI-01 “Atención de solicitudes de soporte informático”
- P-GTI-02 “Respaldo de Información”
- P-GLO-03 “Control de bienes muebles estatales”.
- P-GLO-06 “Procedimiento de Control de Ingreso y salida de Colaboradores”
- P-GTICE-MOCD-001 “Procedimiento para la Gestión de acceso físico al Centro de Datos”.
- PR-SGSI-002 “Procedimiento de Gestión de Riesgos de Seguridad de la Información”

4. Documentos de Referencia

- Norma ISO/IEC 27001:2013 “Sistemas de Gestión de Seguridad de la Información – Requisitos”.
- Norma NTP-ISO/IEC 27002:2017 “Tecnología de la información. Técnicas de seguridad. Código de prácticas para controles de seguridad de la información.

5. Definiciones y Abreviaturas

5.1. Definiciones

Acceso remoto	Acceso desde un equipo informático a un recurso ubicado físicamente en otra computadora que se encuentra en otro lugar.
Activos de Información	Bien o servicio tangible o intangible, que genera, procesa o almacena información, en el cual se le atribuye un grado de valor según su criticidad o asociación con los procesos de negocio los cuales están alineados a sus objetivos planteados.
Activos de Tecnología de la Información	Recursos tecnológicos con los que cuenta una organización como el software, hardware y servicios.
Colaborador	Personal que labora para el OSIPTEL, contratado bajo la modalidad del Régimen Laboral (D.L. 728), Contrato Administrativo de Servicios-CAS (D.L. 1057), intermediación laboral y convenio de prácticas.

Dispositivo móvil	Dispositivos que permiten a las personas acceder a datos e información desde cualquier lugar y en cualquier momento. Comprenden los dispositivos Laptops, smartphones, tablets y smartwatch.
Equipo desatendido	Equipo informático cuyo usuario se ausenta momentáneamente.
Medio Removible	Es cualquier componente extraíble de hardware que sea usado para el almacenamiento de información; los medios removibles incluyen cintas, discos duros removibles, CDs, DVDs y unidades de almacenamiento USB, entre otras.
PIN	De las siglas en inglés, Personal Identification Number, es un número de identificación personal utilizado en ciertos sistemas, como el teléfono móvil o el cajero automático, para identificarse y obtener acceso al sistema.
Portal cautivo	Página de inicio de sesión personalizado en redes empresariales que los usuarios invitados deben pasar antes de poder conectarse a la red inalámbrica.
Propietario de Activo de Información	Individuo o entidad de forma responsable, que cuenta con la aprobación del órgano de dirección, para el control de la producción, desarrollo, mantenimiento, utilización y seguridad de los activos. El término propietario no significa que la persona disponga de los derechos de propiedad reales del activo.
Proveedor	Persona natural o jurídica que brinda un servicio o producto al OSIPTEL.
Proyecto	Proceso único, que consiste en un conjunto de actividades coordinadas y controladas con fechas de inicio y finalización, llevadas a cabo para lograr un objetivo conforme con requisitos específicos y requerimientos específicos, incluyendo las limitaciones de tiempo, coste y recursos
Remote Desktop Protocol (RDP)	Protocolo propietario desarrollado por Microsoft que permite la comunicación en la ejecución de una aplicación entre un terminal (mostrando la información procesada que recibe del servidor) y un servidor Windows (recibiendo la información dada por el usuario en el terminal mediante el ratón o el teclado).
Teletrabajo	Todas las formas de trabajo fuera de la oficina, incluyendo los ambientes de trabajo no tradicionales, tales como los ambientes denominados “trabajo a distancia”, “trabajo flexible”, “trabajo remoto”, y “trabajo virtual”.
Tercero	Toda persona que no cuentan con vínculo laboral con el OSIPTEL pero requiere hacer uso de sus activos de información ya sea para la prestación de un servicio (proveedores), en calidad de visitante o administrado (empresa operadora o usuario de servicio de telecomunicaciones).

5.2. Abreviaturas

OCRI	Oficina de Comunicaciones y Relaciones Institucionales.
OAF	Oficina de Administración y Finanzas
OTI	Oficina de Tecnologías de la Información
ORH	Oficina de Recursos Humanos
OSIPTEL	Organismo Supervisor de la Inversión Privada en Telecomunicaciones
TI	Tecnologías de la Información
UO	Unidad Orgánica

6. Políticas

6.1. Seguridad de la Información

"El OSIPTEL como organismo público regulador del sector telecomunicaciones considera a la información como un activo valioso para el cumplimiento de sus funciones y alcance de sus objetivos estratégicos. Por tanto, resulta necesario gestionar la seguridad de la información estableciendo mecanismos para proteger su confidencialidad, disponibilidad e integridad ante amenazas internas o externas, deliberadas o accidentales; y se compromete a cumplir con los requisitos aplicables en seguridad de la información y mejorar continuamente su Sistema de Gestión de Seguridad de la Información.

El OSIPTEL establece los mecanismos para respaldar la difusión y actualización, tanto de la presente política como de los demás componentes del Sistema de Gestión de Seguridad de la Información."

6.2. Gestión de Proyectos

- La Gerencia o Jefatura de UO que tenga bajo su responsabilidad la ejecución de un proyecto, independientemente de su naturaleza, debe realizar el análisis de riesgos de seguridad de la información sobre los activos de información involucrados.
- Los responsables de los proyectos deben comunicar al Oficial de Seguridad de la Información sobre el alcance del proyecto de forma que se definan los requisitos necesarios para preservar la seguridad de la información de los activos de información involucrados.

6.3. Dispositivos Móviles

- Todo colaborador o tercero que a través de un dispositivo móvil haga uso de la información, sistemas o servicios informáticos del OSIPTEL debe cumplir con la presente política y cualquier otra normativa que regule su uso o se derive de esta.
- Los dispositivos móviles del tipo tablet o laptop y los dispositivos de almacenamiento externo como discos duros portátiles, que ingresen o salgan de las instalaciones del OSIPTEL, deberán ser registrados por el personal de seguridad del edificio.
- Los dispositivos móviles que almacenen o guarden información del OSIPTEL deben contar con mecanismos de autenticación como PIN, clave, patrón, etc. Así como el cifrado de memorias o discos de almacenamiento internos y/o externos.
- Los dispositivos móviles de propiedad del OSIPTEL podrán ser conectados a internet a través de medios autorizados como plan de datos, Portal Cautivo del OSIPTEL, red cableada, modem USB o la red inalámbrica privada del colaborador, quedando prohibido el acceso a través de redes inalámbricas públicas como parques, cafeterías, aeropuertos, etc.
- El OSIPTEL proveerá de cables de seguridad para evitar la pérdida o robo de los dispositivos móviles del tipo laptop de su propiedad, así como maletines.
- El colaborador que tenga asignado un dispositivo móvil del OSIPTEL debe evitar dejarlo en cajones sin seguro, lugares de reunión, autos o ambientes sin supervisión; manteniéndolo en lugares que ofrezcan seguridad.

- El colaborador que tenga asignado un dispositivo móvil del OSIPTEL debe ser responsable de su cuidado general, debiendo reportar a Control Patrimonial cualquier tipo de siniestro, en concordancia con el procedimiento "Control de bienes muebles estatales" (P-GLO-03).
- El colaborador que requiera la configuración del correo electrónico institucional en su dispositivo móvil personal, en justificación al cumplimiento de sus labores, deberá contar con la autorización del Gerente de su UO y solicitarlo a OTI a través de los medios que establezcan.
- Los dispositivos móviles de propiedad de colaboradores o terceros, que requieran conectarse a la red de datos del OSIPTEL deberán ser autorizados por la gerencia responsable del colaborador o tercero, a través del Portal de Soporte Informático; el permiso de acceso será temporal y limitado.

6.4. Teletrabajo o Trabajo Remoto o Acceso Remoto

- El colaborador contratado bajo la modalidad de TELETRABAJO debe cumplir con la presente política y cualquier otra normativa interna relacionada a seguridad de la información, protección y confidencialidad de los datos.
- El colaborador contratado bajo la modalidad de TELETRABAJO debe guardar confidencialidad de la información proporcionada por el OSIPTEL para la prestación de servicios.
- El colaborador contratado bajo la modalidad de TELETRABAJO contará con un acceso remoto que le permita acceder a los recursos y servicio internos del OSIPTEL, el cual será habilitado por OTI previa autorización del Gerente, Director o Jefe de la UO a la que pertenece. La solicitud de acceso remoto se realiza a través del Portal de Soporte Informático, completando los datos requeridos en el formulario correspondiente e incluyendo en la sección "Motivo" el sustento de la solicitud y referenciando al contrato vigente del colaborador.
- El Gerente, Director o Jefe de la UO que requiera acceso remoto para un colaborador contratado bajo modalidad diferente al TELETRABAJO, debe cumplir con los lineamientos indicados en la presente política.
- El Gerente, Director o Jefe de la UO que autoriza la solicitud de acceso remoto es responsable de evaluar la adecuada correspondencia con aquellos roles que realmente requieren el acceso por cumplimiento de sus funciones; de forma que se preserve la seguridad de la información del OSIPTEL a la que accederá el colaborador.
- El Gerente, Director o Jefe de la UO es responsable de revisar de forma trimestral la relación de sus colaboradores con acceso remoto, trabajo remoto o teletrabajo y validar su correspondencia ante la OTI.
- El colaborador que cuente con acceso remoto ya sea por TELETRABAJO o porque ha sido autorizado para su uso, debe proteger la información a la que tiene acceso de amenazas como el acceso no autorizado, alteración indebida o software malicioso cumpliendo con lo siguiente:
  - ✓ Conectarse desde ambientes físicos seguros.
  - ✓ Bloquear el equipo informático desde el cual se conecta, cuando se retira de su ubicación.
  - ✓ Cerrar sesión en el acceso remoto al finalizar sus actividades.
  - ✓ Conectarse desde accesos a internet confiables, no públicos o gratuitos.

- La OTI provee mecanismos tecnológicos seguros para brindar el servicio de acceso remoto garantizando la transmisión cifrada de la información, así también implementa controles con la finalidad de proteger los recursos y servicios informáticos internos.
- El acceso remoto a terceros sólo se permite en caso de asistencia de proveedores especializados y siempre que cuente con la autorización previa del Gerente de la UO, lo cual debe ser realizado a través del Portal de Soporte Informático.
- El Oficial de Seguridad de la Información validará las solicitudes de acceso remoto de proveedores especializados a través del Portal de Soporte Informático.
- Se encuentra prohibido cualquier otro mecanismo técnico de acceso remoto que permita el acceso desde redes externas a la red del OSIPTEL o viceversa.
- La asistencia remota interna es realizada sólo por el personal técnico de OTI, para lo cual se utilizarán conexiones con protocolos seguros; no está autorizado el acceso remoto entre colaboradores de otras UO.

6.5. Recursos Humanos

- La jefatura de ORH es responsable de la verificación de los antecedentes laborales de los nuevos colaboradores (Planilla y CAS) así como información de grados y títulos u otra información que afecte la seguridad de la información del OSIPTEL.
- El nuevo colaborador del OSIPTEL participa del proceso de inducción organizado por la jefatura de ORH de acuerdo al procedimiento P-GRH-01, con la participación del Oficial de Seguridad de la Información o quién él delegue.
- Todos los productos, creaciones, desarrollos, campañas, trabajos, investigaciones, etc. logrados por el colaborador durante la vigencia de su contrato, serán de propiedad del OSIPTEL.
- La jefatura de ORH debe comunicar a OTI y OAF sobre los cambios en los colaboradores como rotación de puestos, licencias mayores o iguales a 3 meses, o término del vínculo laboral con OSIPTEL, hasta con 3 días de anticipación; de forma que se tomen las medidas de control sobre la revocación de accesos a las instalaciones físicas, recursos y servicios informáticos. Los procedimientos relacionados se encuentran normados en los documentos P-GTI-01 y P-GLO-06 respectivamente.
- Las cuentas de usuario de colaboradores con licencia mayor o igual a 3 meses serán deshabilitadas salvo autorización expresa del Gerente de la UO. En los casos de culminación de vínculo laboral, las cuentas serán inicialmente deshabilitadas por 15 días, posterior a ello serán eliminadas de los servidores. OTI mantiene el respaldo de la información histórica de acuerdo a su procedimiento P-GTI-02 “Respaldo de Información”.
- Para los casos donde se requiera la habilitación de una cuenta que se encuentra en proceso de eliminación, se deberá contar con la autorización del titular de la cuenta, así como la del Gerente de la UO a la que pertenecía.
- Todos los colaboradores deben asistir a las charlas, entrenamientos o capacitaciones en Seguridad de la Información, así como cumplir con las Políticas de Seguridad de la Información.
- Todos los colaboradores están sujetos a cláusulas de confidencialidad, las cuales se mantienen vigentes aun cuando haya finalizado el vínculo laboral con OSIPTEL.

6.6. Activos de información

- OSIPTEL mantiene su inventario de activos de información actualizado de acuerdo al procedimiento PR-SGSI-002 “Gestión de Riesgos de Seguridad de la Información” donde se incluye también la identificación y/o designación del propietario del activo de información.
- Los colaboradores que tengan asignado información y/o activos de TI debe hacer uso de estos en estricto cumplimiento a sus funciones y/o actividades asignadas.
- El acceso a los activos de TI se realiza a través de una cuenta de acceso a red.
- Los colaboradores cuentan con unidades de red (W y P) donde deben almacenar sólo información institucional evitando la duplicidad de datos por ser un uso incorrecto del almacenamiento.
- Los colaboradores deben proteger los activos de TI y la información albergada o procesada en estos, contra el acceso (físico y lógico) no autorizado, robo, daño, saturación de recursos, consumo excesivo del ancho de banda, exposición de datos personales,
- OTI es responsable de implementar mecanismos técnicos para brindar seguridad a los activos de TI, por ello norma su uso a través de la Directiva N° 001-2018-GG/OSIPTEL “Directiva para la gestión del parque informático”.
- Los colaboradores que requieran acceso a llamadas telefónicas externas (salientes) deben solicitarlo a través del Portal de Soporte Informático.
- Los activos de TI son parte de patrimonio del OSIPTEL; por tanto, OTI en coordinación con OAF realizan el proceso de asignación formal.
- Los usuarios que requieran retirar activos de TI de las instalaciones del OSIPTEL deberán solicitarlo y contar con la autorización previa del Jefe o Gerente de la UO correspondiente, así como realizar la comunicación a OTI según los formatos establecidos.
- Los equipos de cómputo que son entregados a los colaboradores en calidad de préstamo (Emergencia Sanitaria Covid-19) serán configurados con los puertos de almacenamiento extraíbles bloqueados.

6.6.1. Clasificación de la información

- Los propietarios de los activos de información son responsables de su clasificación, la misma que deberá realizarse de acuerdo con el procedimiento PR-SGSI-002 “Gestión de Riesgos de Seguridad de la Información”.
- Los activos que son propiamente información siguen los lineamientos de clasificación y etiquetado de la Directiva N° 007-2017-GG/OSIPTEL – Directiva de Confidencialidad y sus modificatorias, así mismo se omite el etiquetado de la información que no tenga clasificación de confidencial.
- Los activos de información deberán ser tratados de acuerdo con su clasificación.

6.6.2. Medios removibles

- La movilización y salida de medios removibles que contengan información confidencial, fuera de las oficinas del OSIPTEL se encuentra prohibida, salvo con autorización expresa del Gerente General. Esta prohibición no incluye el traslado de las cintas de respaldo hacia su lugar de custodia gestionado por la OTI.
- Todo colaborador que para el cumplimiento de sus funciones requiera conectar un medio removible a un equipo de cómputo del OSIPTEL deberá asegurarse que es analizado por el software antimalware/antivirus.

- Los equipos de cómputo que sean retirados de las instalaciones del OSIPTEL porque son entregados a los colaboradores en calidad de préstamos, tendrán los puertos bloqueados para el uso de medios removibles y sólo se habilitarán cuando exista la necesidad y se cuente con la autorización del Gerente o Director o Jefe de la UO.

6.6.3. Disposición de medios

- Los equipos de cómputo que contienen medios removibles y requieran ser dados de baja, deberán pasar por un proceso de borrado seguro.
- OTI es responsable de normar e implementar el proceso de borrado seguro y destrucción de los medios (en caso corresponda), antes que se realice la baja o reutilización del mismo.

6.6.4. Uso de Internet

- El servicio de internet se encuentra disponible para los colaboradores del OSIPTEL como herramienta de apoyo para el cumplimiento de sus funciones y realización de tareas.
- Los colaboradores son responsables de dar buen uso al servicio de internet, así como de adoptar las medidas de seguridad necesarias que garanticen que su trabajo se llevará a cabo de una manera eficiente y productiva.
- OTI es responsable de brindar el servicio de internet a través de mecanismos seguros para lo cual implementa controles y filtros de navegación lo cual puede implicar la restricción parcial o total de sitios web potencialmente peligrosos. Así mismo establece las configuraciones necesarias en los navegadores web autorizados en los equipos de cómputo.
- No está permitido cualquier otro medio de conexión a internet de proveedores externos que no haya sido dispuesto por OTI.
- El OSIPTEL cuenta con la potestad de mantener los registros de navegación de su servicio de internet, así como de toda información entrante o saliente a través de su red, con la finalidad de monitoreo y/o revisión y sin previo aviso.
- Las conexiones inalámbricas a internet se realizarán a través de los portales cautivos, los mismos que serán usados por los visitantes, en caso lo soliciten y se encuentre autorizado por el Jefe o Gerente de la UO correspondiente; la solicitud se realiza por correo electrónico a la cuenta de soporteinformatico@osiptel.gob.pe.
- Cualquier solicitud de cambio en la configuración establecida por OTI deberá ser sustentado y evaluado por el Comité de Gobierno Digital.
- Los colaboradores del OSIPTEL sólo podrán hacer uso del servicio de almacenamiento en la nube institucional, previa autorización de la máxima autoridad de la UO a la que pertenece y de acuerdo a los mecanismos técnicos establecidos por OTI.
- Los colaboradores del OSIPTEL no debe divulgar o publicar información confidencial en sitios web o en servicios de almacenamiento en la nube (dropbox, googledrive, etc.) no autorizados. Así también, está prohíbo visitar sitios web con contenido inapropiado (entretenimiento, pornografía, juegos, contenido ofensivo, redes sociales, chats, conexiones p2p) o que puedan ser fuente de archivos y programas maliciosos.
- OTI gestiona las actualizaciones de software en los equipos informáticos de forma automática, por lo cual no se requiere la descarga de parches u otro software por parte de los colaboradores.

6.6.5. Uso del Correo Electrónico

- El servicio de correo electrónico se encuentra disponible para los colaboradores del OSIPTEL como herramienta de apoyo para el cumplimiento de sus funciones y realización de tareas.
- OTI es responsable de brindar el servicio de correo a través de mecanismos seguros y confiables para lo cual implementa controles y filtros que pueden implicar la restricción parcial o total de cuentas de correo que remiten información potencialmente peligrosa. Así mismo, a través de su Directiva P-GTI-01 – "Atención de Solicitudes de Soporte Informático", Directiva N° 001-2018-GG/OSIPTEL – "Gestión del Parque Informático", entre otras normas, establece las pautas para su adecuada gestión.
- El software cliente de correo electrónico autorizado es Microsoft Outlook, cualquier otro se encuentra prohibido.
- Los colaboradores no deben hacer uso de correos electrónicos gratuitos personales (Gmail, Hotmail, Yahoo, Outlook, etc.) con excepción de la Alta Dirección, Gerentes, Sub Gerentes, Asesores y Jefes.
- Los colaboradores no deben enviar información confidencial del OSIPTEL por correo electrónico hacia cuentas de terceros y/o gratuitos.
- Los colaboradores que remitan información a cuentas grupales o listas de correo debe asegurarse que los destinatarios tienen necesidad de conocer la información a remitir, entendiéndose que esta información es estrictamente laboral.
- Los colaboradores no deben remitir información de su entorno privado a través de cuentas de correo electrónico del OSIPTEL, tampoco deben usar su cuenta de correo institucional para suscribirse a boletines, revistas, programas u otros medios de notificaciones de carácter personal.
- Los colaboradores que reciban un correo electrónico con contenido malicioso, fraudulento o donde se alerte situaciones que comprometan la seguridad de la información deberá remitir el mensaje a la cuenta de correo informacionsegura@osiptel.gob.pe con la finalidad de que se brinde el tratamiento adecuado, así como evitar su difusión o re-envío a otros destinatarios.
- Los colaboradores deben cuidar y hacer buen uso del servicio de correo electrónico del OSIPTEL, toda acción contraria (envío de publicidad, correos masivos, suplantación de identidad, correos cadenas, virus, código malicioso, contenido inapropiado u ofensivo, entre otros) y/o que ponga en peligro la información almacenada o transmitida por el servicio de correo, así como su infraestructura, está prohibida y será considerada como un ataque.
- Los colaboradores del OSIPTEL debe hacer uso de firmas (resumen de datos) estandarizadas que lo identifiquen en el intercambio de correos electrónicos, la estructura de la firma seguirá lo normado por OCRI.
- Los colaboradores del OSIPTEL son responsables controlar el espacio de almacenamiento en su correo de forma que garantice su disponibilidad contando con opciones de eliminación, copia a carpetas del equipo local entre otras.

6.6.6. Pantalla y Escritorios Limpios

- Los colaboradores deben bloquear su equipo de cómputo cuando se ausenten de su lugar de trabajo, así como guardar en un lugar seguro cualquier documento, medio magnético u óptico removible que contenga información confidencial. Si los colaboradores están ubicados cerca de zonas de atención al público, deben guardar también los documentos y medios que contengan información de uso interno.
- Al finalizar la jornada de trabajo, el funcionario debe guardar en un lugar seguro los documentos y medios que contengan información confidencial o de uso interno.
- OTI configura el bloqueo automático de los equipos de cómputo ante la inactividad por 5 minutos, de forma que se proteja el acceso no autorizado.
- Los colaboradores que usen las impresoras deberá retirar los documentos inmediatamente después de su impresión.

6.7. Control de Acceso

- El acceso a la información, a los recursos y servicios de TI debe ser controlado con la finalidad de preservar su confidencialidad, integridad y/o disponibilidad.
- Los propietarios de los activos de información son los responsables de definir las reglas de acceso y restricciones que son requeridas.
- OTI es responsable de normar e implementar los mecanismos técnicos para controlar el acceso lógico a los recursos y servicios de TI, por tanto, no debe existir equipamiento informático y/o software que no cumpla con las condiciones de seguridad exigidos por este.
- Las Gerencias de las UO deben comunicar a OTI la relación de proveedores que requieren acceso a los sistemas de información con la debida autorización y evidenciar el vínculo contractual con estos, así también comunicar la culminación del contrato para las bajas correspondientes en los accesos.

6.7.1. Identificación y Contraseñas

- Todo acceso a recursos y servicios de TI se realiza con una cuenta de usuario que es un identificador único compuesto por un usuario[1] y contraseña.
- La contraseña está clasificada como información confidencial por lo cual no se debe compartir o mantener anotaciones de esta, ya sea en papeles o archivos digitales.
- Los proveedores de servicios que necesiten acceder a una cuenta de usuario del OSIPTEL, deberán de ser identificados con el prefijo “prov”, estas cuentas serán solicitadas en el Portal de Soporte Informático con la autorización del Gerente, Director o Jefe de la UO correspondiente al área usuaria indicando el vínculo y periodo contractual del proveedor.
- Las empresas operadoras que deban hacer uso de las aplicaciones informáticas de OSIPTEL, designarán a sus usuarios autorizados, estas cuentas deberán ser diferenciadas de las cuentas internas de los colaboradores del OSIPTEL y mantener una nomenclatura estandarizada por OTI.

[1] Se entiende por Usuario el nombre de cuenta para el acceso a cualquier sistema informático. Por ejemplo: jrodriguez.

- Los colaboradores o terceros tienen prohibido usar una cuenta de usuario de otra persona o suplantar su identidad. Así también, no debe hacer uso de cuentas genéricas.
- Las contraseñas deben ser robustas para mitigar riesgos de acceso no autorizado, por lo cual debe ser de una longitud mínima de 8 caracteres cumpliendo una combinación de números, símbolos, letras mayúsculas, minúsculas.
- Las cuentas de usuario deben de ser bloqueadas ante 5 intentos fallidos de ingreso de contraseña.
- Las contraseñas almacenadas deben hacer uso de cifrados robustos como AES256 o superior.
- Las cuentas de usuario deben permitir que los usuarios realicen su cambio con una frecuencia máxima de 90 días, no se podrán reutilizar contraseñas anteriores. El usuario de una nueva cuenta de acceso debe cambiar su contraseña la primera vez que inicie sesión.
- El restablecimiento de contraseña por olvido debe ser solicitada a OTI que es responsable de realizar la validación de la identificación del solicitante bajo los mecanismos que establezca y asignando una contraseña temporal que cumpla con las características de fortaleza ya definidas.
- Todos los equipos y/o dispositivos conectados a la red del OSIPTEL (routers, firewalls, switches, etc.) deben contar con contraseñas u otro mecanismo superior de control de acceso. OTI es responsable de la seguridad de la red del OSIPTEL por tanto norma los procedimientos adecuados para su cumplimiento.
- Ningún equipo o dispositivo conectado a la red del OSIPTEL debe mantener contraseñas por defecto u omisión, incluyendo aquellas provistas por fabricantes o proveedores de equipamiento o software.

6.7.2. Usuarios Privilegiados

- Las cuentas de usuarios del tipo administrador, súper administrador y/o administradores del dominio son de uso exclusivo de OTI y deben ser usados solo para labores de mantenimiento, configuración y/o soporte de la plataforma tecnológica institucional.
- Las cuentas de usuario que son usadas por servicios (sistemas, IIS, Oracle, etc.) son de uso exclusivo de OTI y deben de tener una longitud mínima de 30 caracteres, combinación de números, símbolos, letras mayúsculas, minúsculas.

6.8. Seguridad Física y del Entorno

- Toda persona que ingrese a las instalaciones del OSIPTEL debe identificarse y ser registrado tanto en el ingreso como en la salida. Los colaboradores deben usar en todo momento su fotocheck y los terceros deben usar el identificador que se les haya sido asignado.
- OAF es el responsable de normar e implementar los mecanismos técnicos para asegurar el control del acceso físico a las instalaciones, a través de su Coordinador de Seguridad establece los procedimientos necesarios para cumplir con tal fin.
- Las oficinas o instalaciones donde se almacene o procese información confidencial (Centro de Datos, Archivo, entre otras) deben contar con acceso restringido y monitoreado con cámaras de videovigilancia. El ingreso y salida de los colaboradores autorizados debe ser registrado por las UO responsables de dichos ambientes y, de ser el caso, emplear mecanismos biométricos.

- Las oficinas o instalaciones que contengan equipos de comunicaciones (switches, PBX, routers, firewalls) y consolas de administración, deben contar con acceso restringido y monitoreado con cámaras de videovigilancia.

6.8.1. Acceso al Centro de Datos

- El centro de datos es considerado una instalación crítica por almacenar y procesar información sensible e importante para el OSIPTEL.
- El acceso al Centro de Datos está permitido sólo al personal técnico autorizado de OTI. El ingreso y salida es previa identificación dactilar (huella) o mediante uso de llave en el dispositivo de acceso.
- Los terceros que requieran ingresar, deben contar con autorización y estar acompañados por un personal técnico autorizado de OTI quién supervisará los trabajos o actividades a realizar.
- Todo equipamiento debe ser inspeccionado antes de la entrega a fin de determinar si su contenido representa un peligro para la seguridad del centro de datos, de igual manera, esta tarea será supervisada por un personal técnico autorizado de OTI
- Cualquier mantenimiento efectuado en las áreas continuas al Centro de Datos que impliquen uso de químicos o agentes emisores de humo, polvo, gases o cualquier otra sustancia que afecte las alarmas del Centro de Datos, debe ser comunicado y coordinado con OTI a fin de prevenir alguna alteración del Centro de Datos.
- En mención a lo anterior, se debe realizar el correcto sellado de todas las puertas del Centro de Datos (deberá asegurarse el sellado de todo el marco de las puertas, para evitar ingreso de gases) así como ductería (cableado eléctrico, etc.) y falso techo contiguos a sus instalaciones de ser necesario, utilizando para ello cinta de enmascarar - Hogar y Obra (cinta azul) de remoción limpia, este sellado lo deberá realizar el área responsable del mantenimiento o trabajo. Asimismo, 24 horas después de la finalización de los trabajos, dicha cinta deberá ser retirada sin dejar residuos en los marcos de las puertas.

6.8.2. Reutilización o baja de Equipos Informáticos

- Todo equipo informático que contenga medios de almacenamiento debe pasar por un proceso de borrado seguro ante la necesidad de su reutilización o baja.
- OTI es responsable de normar e implementar el proceso de borrado seguro y destrucción de los componentes informáticos (en caso corresponda), antes que se realice la baja o reutilización del mismo.

6.9. Relación con Proveedores

- El acceso a los activos de información por parte del personal del proveedor debe ser autorizado por el propietario del activo.
- Todo personal del proveedor que en prestación de su contrato esté involucrado o en contacto con información, recursos o servicios tecnológicos del OSIPTEL, debe protegerlos del acceso o uso no autorizado, alteración de operaciones, destrucción, mal uso o robo, cumpliendo con los lineamientos de la presente política y con toda aquella normativa que sea aplicable a estos.

- Toda la información albergada en la red corporativa, de forma estática o circulando a través de ella mediante elementos de comunicación o transmisión, es propiedad del OSIPTEL y tiene el carácter de confidencial.
- Todo personal del proveedor de servicio con responsabilidades en áreas de operación o administración de sistemas y redes debe:
  - ✓ Asegurar que la integridad, autenticación, control de acceso, auditoría y registro se contemplan e incorporan al diseñar, implantar y operar los Sistemas de Información y Redes de Comunicaciones.
  - ✓ Asegurar la confidencialidad de la información almacenada, tanto en formato electrónico como físico.
- Todo personal del proveedor que tenga contacto o haya obtenido conocimiento de información del OSIPTEL debe guardar absoluta confidencialidad, esta obligación permanece vigente aún posterior a la extinción del contrato y por tiempo indefinido.
- Toda información (física o digital) que haya sido puesta a disposición del personal del proveedor es estrictamente temporal, con obligación de secreto y sin que ello le confiera derecho alguno de posesión, titularidad o copia sobre dicha información.
- La Gerencias solicitantes de servicios o productos suministrados por proveedores deben de coordinar con OAF de forma que se garantice la inclusión de cláusulas de seguridad en los contratos.
- La OAF brindará a los proveedores, la documentación necesaria relacionada al Sistema de Gestión de Seguridad de la Información.
- El Área o persona designada como coordinador en los contratos con proveedores, será la encargada de monitorear y revisar el cumplimiento de los contratos con terceros, en coordinación con la OAF.

6.10. Adquisición, Desarrollo y Mantenimiento de Sistemas

- OSIPTEL no realiza actividades de desarrollo de sistemas con recursos internos, cualquier nuevo desarrollo es realizado o adquirido a terceros y en casos menores realiza mantenimiento de sus sistemas legados.
- Las Gerencias que requieran la adquisición de sistemas de información deberán de coordinarlo con OTI.
- OTI cuenta con requisitos de seguridad de la información para la adquisición y mantenimiento de sistemas de información, los cuales forman parte de los términos de referencia o requisitos mínimos en sus proyectos.
- OTI es responsable de normar, solicitar e implementar los mecanismos técnicos que protejan los sistemas e información alojados en estos.

6.11. Gestión de las Operaciones

6.11.1. Gestión del cambio

- La OTI es la responsable de gestionar los cambios en la infraestructura tecnológica y/o sistemas de información, y normar los procedimientos necesarios para este fin así como mantener información documentada sobre este proceso.
- Los cambios deberán ser planificados e incluir la identificación de los posibles compromisos en seguridad de la información, los cuales de ser el caso, serán comunicados al Oficial de

Seguridad de la Informacion para su evaluación de acuerdo a las políticas y requisitos de seguridad de la información.

- Los cambios de emergencia que requieren ser aplicados para resolver un incidente, deberán realizarse de forma rápida y controlada.
- Los cambios realizados deben ser verificados para asegurar que se mantiene operativo el sistema de información, incluyendo aquellos aspectos de seguridad de la información del sistema y que el propósito del cambio se cumplió satisfactoriamente.
- Los cambios deben de incluir un plan de roll-back (volver al estado anterior), que incluyan las actividades a seguir para abortar los cambios que se ejecutaron sin éxito y/o eventos imprevistos.

6.11.2. Gestión de la capacidad

- La OTI analiza la demanda de capacidad y realiza proyecciones de crecimiento de los recursos administrados (capacity planning) de manera periódica, con el fin de asegurar el desempeño y capacidad de la plataforma tecnológica del OSIPTEL. Este análisis considera aspectos de consumo de recursos de procesadores, memorias, discos, servicios de impresión, anchos de banda, internet y tráfico de las redes de datos, entre otros.

6.11.3. Protección contra Software Malicioso

- OTI es responsable del control del software por ello norma e implementa los mecanismos técnicos que protejan los recursos y servicios de TI así como la información alojada.
- Los equipos de cómputo cuentan con software de protección contra malware, virus y troyanos.
- Los usuarios tienen restricciones de instalación de software con la finalidad de evitar la propagación de software malicioso,
- El servicio de correo cuenta con un servicio antispam para detectar correos maliciosos y bloquearlos.
- Los usuarios son responsables de reportar cualquier evento que identifiquen como potencialmente peligroso (archivos modificados sin autorización, ventanas emergentes, etc.).

6.11.4. Respaldo de Información

- OTI es responsable de gestionar el respaldo de la información en formato digital, así como del software y sistemas, el cual se estable en su procedimiento P-GTI-02 “Respaldo de Información”.
- El respaldo de información debe almacenarse en lugares remotos para evitar cualquier daño en caso de desastre en las instalaciones del OSIPTEL.
- OTI establece los requisitos necesarios para la protección ambiental y física de las copias de respaldo.
- El OSIPTEL realiza copias de respaldo de la información de sus servicios en producción, los cuales incluyen código fuente, bases de datos y unidades de red (W, P y Q) y se encuentran administrados por la OTI.
- Las copias de respaldo diarias son conservadas por 90 días, las copias de respaldo semanales son conservadas por 12 semanas y las copias de respaldo mensuales son conservadas de forma indefinida.

- OTI realizará pruebas periódicas (mínimo anual) de recuperación del respaldo, para asegurar que son confiables cuando sean necesario.

6.11.5. Protección de información de registros

- La OTI es responsable de asegurar que los componentes principales de la infraestructura tecnológica y sistemas de información cuenten con registros de auditoría sobre fallas y eventos de seguridad.

6.11.6. Gestión de Vulnerabilidades Técnicas

- Todo proyecto informático que sea implementada en el OSIPTEL debe ser coordinado con OTI y el Oficial de Seguridad de la Información de forma que se incluya los requisitos de seguridad necesarios que eviten posibles vulnerabilidades.
- OTI incluye dentro de los requisitos de adquisición o mantenimiento de software pruebas o análisis de vulnerabilidades.
- El Oficial de Seguridad de la Información realiza periódicamente pruebas de vulnerabilidades sobre los servicios e infraestructura tecnológica, comunicará los resultados a las UO encargadas de la remediación para que planifiquen las acciones necesarias.
- OTI como responsable de la seguridad de los recursos y servicios informáticos, realiza tareas de actualización periódica sobre el software de los servidores, equipos de cómputo, comunicaciones o seguridad perimetral.
- Los colaboradores o terceros que detecten vulnerabilidades o debilidades que puedan poner en peligro la información, recursos o servicios de TI, debe comunicarlo al Oficial de Seguridad de la Información siguiendo el procedimiento P-SGSI-01.
- Los colaboradores o terceros que detecten vulnerabilidades no deben aprovecharse de estas para acceder o difundir información no autorizada, así como producir alguna interrupción o daño en los recursos y servicios de TI.

6.11.7. Restricciones a la Instalación y Uso de Software

- Los colaboradores o terceros no deben realizar instalación de software en los equipos informáticos, esta actividad es exclusiva del personal técnico de OTI.
- OTI es responsable de la seguridad de los recursos y servicios de TI, por tanto, norma e implementa los mecanismos técnicos necesarios para protegerlo de amenazas que afecten su adecuado funcionamiento.
- Está prohibido difundir software o contenidos que violen derechos de autor o programas no licenciados o cuyo propietario de licencia no sea del OSIPTEL. OTI establece estos y otros lineamientos para la gestión adecuada del software a través de su Directiva N° 007-2015-GG-OSIPTEL “Gestión de Software Legal”.
- La actualización de software especializado que no se realice automáticamente a través de las herramientas de OTI deberán ser solicitadas a Soporte Técnico como un requerimiento siguiendo el procedimiento P-GTI-01 “Atención de solicitudes de soporte informático”

6.12. Transferencia de Información

- Las solicitudes de información por parte de Organismos Externos deben ser autorizadas por los propietarios de los activos de información y cuando corresponda debe ponerse en conocimiento de la Gerencia General.
- La transferencia de información por medios informáticos desde o hacia organismos externos se deberá realizar usando mecanismos seguros (TLS, IPSEC, etc.).
- La publicación de documentos en el portal web institucional (.docx, .xlsx, .pdf, etc.) se realizarán previa eliminación de los metadatos que puedan contener.
- Toda publicación web que haga referencia a información autorizada del OSIPTEL debe utilizar el dominio osiptel.gob.pe, no se acepta publicaciones que usen direcciones IP directamente.
- El OSIPTEL hace uso del dominio sociedadtelecom.pe con la finalidad de fomentar el conocimiento y el debate respecto de información especializada en telecomunicaciones.
- El OSIPTEL hace uso del dominio comparatel.pe y checatuplan.pe con la finalidad de publicar su herramienta de comparación de tarifas de los servicios de telecomunicaciones.
- El OSIPTEL hace uso del dominio osiptelperu.com.pe para el envío de encuestas masivas por correo electrónico a los usuarios de los servicios de telecomunicaciones.

6.13. PROTECCIÓN DE DATOS PERSONALES

- El OSIPTEL, en cumplimiento de la Ley N° 29733 - Ley de Protección de Datos Personales, su reglamento, directiva y demás normas modificatorias, complementarias y conexas, realiza tratamiento de datos personales única y exclusivamente para el fin establecido, garantizando su confidencialidad, integridad y disponibilidad.
- En tal sentido, el OSIPTEL se compromete a:
  - Designar a un responsable por cada banco de datos personales; así como un responsable del tratamiento de los mismos.
  - Garantizar el ejercicio de los derechos de acceso, rectificación, cancelación y oposición de los datos personales, a través del correo electrónico datospersonales@osiptel.gob.pe o por escrito dirigido al responsable designado para tal efecto, en cualquier oficina del OSIPTEL a nivel nacional.
  - Promover la toma de conciencia del personal responsable sobre la protección de los datos personales.
  - Cumplir con los requisitos legales, normativos y regulatorios aplicables.
  - Fomentar la mejora continua sobre las medidas adoptadas en protección de los datos personales a fin de minimizar los riesgos e incidentes de seguridad relacionados a los datos personales.

6.14. CONTROLES CRIPTOGRÁFICOS

- Los controles criptográficos son utilizados para la protección de la información clasificada como confidencial durante su transmisión por redes públicas a través de los protocolos HTTPS, SFTP, IPSEC, SSH. La OTI establece el uso de algoritmos de cifrado sólidos.

- La OTI establece los controles necesarios para protección durante la generación, almacenamiento y archivo de las claves criptográficas, incluyendo los respaldos y accesos correspondientes.

7. ACCIONES ANTE DESVIACIONES A LAS POLÍTICAS

El incumplimiento de las disposiciones establecidas en las políticas de seguridad de la información, procedimientos, manuales o cualquier otro documento derivado de estas, tendrá como resultado la aplicación de medidas correctivas y de mejora necesarias. En caso se encontrará responsabilidad en un colaborador y/o tercero, se dará inicio al procedimiento administrativo disciplinario correspondiente y/o a las acciones legales que la ley faculte.