LINEAMIENTOS DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

DOCUMENTO CONTROLADO

Propuesto por:	Gestión Institucional	Fecha de propuesta:	17/11/2022
Aprobado por:	Gerencia General	Fecha de aprobación:	17/11/2022

Firmado digitalmente por: SANCHEZ SALDAÑA Sandra FAU 20522224783 soft
Motivo: Doy V° B°
Fecha: 17/11/2022 19:00:35-0500

Firmado digitalmente por: TEJADA ROJAS Ofelia Maribel FAU 20522224783 soft
Motivo: Doy V° B°
Fecha: 17/11/2022 19:01:35-0500

OSINFOR
Firmado digitalmente por: ROJAS SARAPURA Alejandro Alberto FAU 20522224783 soft
Motivo: En señal de conformidad
Fecha: 17/11/2022 19:16:23-0500

ÍNDICE

LINEAMIENTOS DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

I. Objetivo 3

II. Finalidad 3

III. Alcance 3

IV. Responsabilidades 3

V. Definiciones 4

VI. Políticas de Seguridad de la Información 5

6.1 **Organización interna de la seguridad de la información** 5

6.2 **Seguridad en dispositivos móviles y de almacenamiento** 5

6.3 **Seguridad ligada a los recursos humanos** 6

6.4 **Gestión de activos de información** 8

6.5 **Control de accesos** 11

6.6 **Criptografía** 14

6.7 **Seguridad física y de ambiente** 15

6.8 **Pantalla y escritorios limpios** 19

6.9 **Seguridad de las operaciones** 20

6.10 **Seguridad de las comunicaciones** 23

6.11 **Seguridad para la adquisición, desarrollo y mantenimiento de los sistemas de información** 25

6.12 **Seguridad en la relación con proveedores** 28

6.13 **Gestión de debilidades, eventos y/o incidentes de seguridad de la información……..** 31

6.14 **Privacidad y protección de datos personales** 32

6.15 **Trabajo remoto** 35

LINEAMIENTOS DE LAS POLITICAS DE SEGURIDAD DE LA INFORMACIÓN

I. Objetivo

Establecer los lineamientos de carácter administrativo, técnico y operativo del conjunto de políticas de seguridad de la información diseñadas para el Sistema de Gestión de Seguridad de la Información (SGSI) del Organismo de Supervisión de los Recursos Forestales y de Fauna Silvestre (OSINFOR).

II. Finalidad

Contribuir al cumplimiento de la Política del Sistema Integrado de Gestión y logro de sus objetivos, protegiendo los activos de información y garantizando los niveles adecuados de integridad, confidencialidad y disponibilidad de la información institucional, lo cual permite la continuidad operacional de los procesos y servicios que desarrolla el OSINFOR en beneficio de la ciudadanía.

III. Alcance

El presente lineamiento debe ser conocido y aplicado de forma obligatoria por todos los/las servidores/as civiles del OSINFOR, las personas que realicen modalidades formativas, y las que presten servicios a la Entidad, independientemente del vínculo contractual al que se encuentren sujetos.

IV. Responsabilidades

4.1 La Unidad Funcional de Calidad e Innovación (UFCI) es responsable de la administración del SGSI.

4.2 La Unidad de Recursos Humanos (URH), es responsable de informar a todos los/las servidores/as civiles de sus obligaciones respecto del cumplimiento de las políticas de seguridad de la información, gestionar los acuerdos de confidencialidad, coordinar las capacitaciones y comunicar las incorporaciones, modificación de funciones y ceses del personal.

4.3 La Unidad de Abastecimiento (UA), es responsable de comunicar a los/las proveedores y/o contratistas que presten servicios al OSINFOR, respecto del cumplimiento de las políticas de seguridad de la información, gestionar los acuerdos de confidencialidad y coordinar la capacitación de los/las proveedores críticos. Asimismo, supervisar la seguridad física de las instalaciones y control patrimonial.

4.4 La Unidad de Administración Documentaria y Archivo (UADA), es responsable de velar por el cumplimiento de las normas referidas a la administración documentaria y archivo.

4.5 La Oficina de Tecnología de la Información (OTI), es responsable de planificar, implementar y administrar el hardware, software y base de datos de los sistemas de información del OSINFOR, manteniendo su seguridad.

4.6 La Oficina de Asesoría Jurídica y la Secretaría Técnica de las Autoridades de los Órganos Instructores del Procedimiento Administrativo Disciplinario, son responsables de apoyar en el tratamiento de incidentes de seguridad de la información, cuando se requiera su intervención.

4.7 El/La Oficial de Seguridad y Confianza Digital es responsable de:

a) Realizar las capacitaciones de seguridad de la información en coordinación con la URH y la UA, así como supervisar el cumplimiento de las normativas institucionales de seguridad de la información.
b) Realizar el seguimiento, documentación y análisis de los incidentes de seguridad de la información.
c) Comunicar al Centro Nacional de Seguridad Digital (CNSD), todo incidente de seguridad digital que se presente en la entidad, mediante los canales de reporte establecidos por el CNSD o su equivalente.

4.8 El/La Oficial de Datos Personales es responsable de comunicar a la Autoridad Nacional de Protección de Datos Personales, todo incidente de seguridad que haya afectado los datos personales bajo responsabilidad del OSINFOR, en un plazo máximo de 48 horas a partir de la toma de conocimiento de la brecha de seguridad.

4.9 Los/Las Directores/as y Jefes/as de las unidades de organización son responsables de:

a) Velar que el personal a su cargo cumpla con la Política del Sistema Integrado de Gestión, así como el presente lineamiento.
b) Evaluar y autorizar el acceso de los/las usuarios/as a los sistemas de información, servicios y recursos de red y a internet en base a las funciones requeridas para el puesto y/o servicio.

V. Definiciones

5.1 **Antispam:** solución de hardware o software que permite prevenir el correo no deseado.

5.2 **Certificado digital SSL:** es un mecanismo que permite autenticar un sitio web en internet y mantiene la información encriptada y segura en el sitio web.

5.3 **Cookie:** es un mecanismo utilizado por las páginas web para mejorar la experiencia de navegación de los usuarios consistente en crear en el ordenador del usuario un fichero informático con información de sus preferencias, gustos y perfil, con el fin de que en la próxima visita los contenidos y funcionalidades se ajusten a sus preferencias.

5.4 **Contratista:** es un proveedor con vínculo con el OSINFOR.

5.5 **Contraseña segura:** es aquella que contiene al menos 8 caracteres y cumple con los requisitos de complejidad, tales como: mayúscula(s), minúscula(s), dígito(s) y/o caracteres no alfanuméricos.

5.6 **Criptografía:** es la técnica que protege documentos y datos. Funciona a través de la utilización de cifras o códigos para proteger estos documentos y datos que circulan en redes locales o en internet.

5.7 **Dispositivo de almacenamiento removible**: dispositivo que almacena información y que no tiene sistema operativo. Incluye tarjetas de memoria, dispositivo de almacenamiento masivo USB basados en memoria flash, discos magnéticos, discos sólidos, ópticos tales como CDs, DVDs, cintas tapes y cualquier dispositivo de almacenamiento de conexión USB, dispositivos criptográficos, entre otros similares.

5.8 **Dispositivo móvil**: dispositivo portable que contiene un sistema operativo. Incluye las laptops, notebooks, tabletas, teléfonos celulares inteligentes, equipos GPS portátiles, cámaras digitales, etc.

5.9 **Firewall:** programa o equipo informático que controla el acceso de una computadora a la red y de elementos de la red a la computadora, por motivos de seguridad.

5.10 **Log:** es un archivo de texto en el que constan cronológicamente los acontecimientos que han ido afectando a un sistema informático (programa, aplicación, servidor, etc.), así como el conjunto de cambios que estos han generado.

5.11 **Protocolo SFTP:** protocolos de la red Internet ideal para transferir grandes bloques de datos por la red en modo seguro. Concretamente significa Secure File Transfer Protocol (Protocolo de transferencia segura de archivos)

5.12 **Proveedor:** Persona natural o jurídica que puede proveer o abastecer de bienes o servicios a cualquier cliente de lo necesario o conveniente para un fin determinado.

5.13 **Proveedores/as críticos:** son aquellos proveedores/as de servicio y/o contratistas que acceden o pueden acceder a los sistemas de información, servicios de tecnología de la información y áreas seguras donde se almacena y/o procesa información.

5.14 **Seguridad perimetral:** es la integración de elementos y sistemas, tanto electrónicos como mecánicos, para la protección de perímetros físicos, detección de tentativas de intrusión y/o disuasión de intrusos en instalaciones especialmente sensibles.

5.15 **Tercero:** es la persona natural o jurídica que no tiene una relación contractual directa, como es el caso de consultores/as externos, auditores/as, representantes de instituciones externas, entre otros.

VI. Políticas de Seguridad de la Información

6.1 Organización interna de la seguridad de la información

Objetivo: Establecer un marco de gestión para controlar la implementación y operación de seguridad de la información dentro del OSINFOR.

Lineamientos:

a) El OSINFOR define, aprueba y asigna las responsabilidades de la seguridad de la información basado en 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. Estas responsabilidades y funciones se detallan en el Reglamento de Organización y Funciones (ROF), así como en las resoluciones de creación, designación y/o conformación de las unidades y comisiones. La organización interna de la seguridad de la información está conformada por:
   i. Alta Dirección.
   ii. Comité de Gobierno y Transformación Digital.
   iii. Unidad Funcional de Calidad e Innovación.
   iv. Oficial de Seguridad y Confianza Digital.
   v. Oficial de Datos Personales.
   vi. Oficial de Gobierno de Datos.
   vii. Equipo de respuestas ante incidentes de seguridad digital.
b) Se debe establecer y mantener contactos con autoridades y grupos de interés relevantes para la seguridad de la información, a efectos de intercambiar experiencias y obtener asesoramiento para el mejoramiento de las prácticas y controles de seguridad de la información, para lo cual el/la **Oficial de Seguridad y Confianza Digital** mantendrá el directorio de contactos respectivo.
c) En los intercambios de información relacionada a seguridad de la información, no se divulgará información confidencial perteneciente al OSINFOR a personas no autorizadas. En el caso se requiera el intercambio de información confidencial para fines de asesoramiento o de intercambio de experiencias, sólo se permitirá cuando se haya firmado previamente un Acuerdo de Confidencialidad.
d) El OSINFOR integra la seguridad de la información en la gestión de proyectos para reducir los riesgos de seguridad de la información, los cuales deberán ser identificados en una fase temprana y ser tratados oportunamente, primordialmente en los procesos misionales, proceso de gestión de tecnologías de la información y demás procesos de apoyo, acorde a los riesgos identificados.

6.2 Seguridad en dispositivos móviles y de almacenamiento

Objetivo: Fortalecer la seguridad de la información en el OSINFOR a través del buen uso de los dispositivos móviles y de almacenamiento removible asegurando la confidencialidad, integridad y disponibilidad de la información almacenada en los mismos.

Lineamientos:

a) La **UA** debe realizar y mantener actualizado el inventario de los dispositivos móviles de la Entidad.
b) En el caso que un/a servidor/a tenga la necesidad de trabajar con su propio dispositivo móvil (laptop, notebook, tableta), el dispositivo debe cumplir con los criterios de seguridad de la información aplicados a los equipos similares del OSINFOR. Para utilizar estos dispositivos móviles dentro de las instalaciones del OSINFOR, se debe de realizar la Declaración Jurada de Bienes y Equipos de

Propiedad Particular[1], a excepción de los teléfonos celulares y dispositivos de almacenamiento que sean de propiedad de el/la servidor/a.

c) El proceso de instalación y configuración de las aplicaciones de los dispositivos móviles gestionados por el OSINFOR será realizado por la OTI, en función a las capacidades técnicas de estos dispositivos y al licenciamiento requerido.
d) Todos los dispositivos móviles deben utilizar la última o la versión más segura de las aplicaciones, las cuales cuentan con servicios de soporte del fabricante.
e) Los/Las servidores/as con dispositivos móviles asignados por el OSINFOR, deben comunicar a la Mesa de Ayuda los requerimientos o incidentes referentes a la actualización de software y/o aplicaciones autorizadas.
f) Los dispositivos móviles que almacenan y procesan información institucional y/o confidencial en especial de datos personales deben considerar:
    i. Alternativas de autenticación de usuario.
    ii. Bloqueo de acceso del dispositivo.
    iii. Bloqueo de pantalla por inactividad (menor igual a 03 minutos).
    iv. Firewall, en los casos que corresponda.
    v. Antivirus.
    vi. Borrado seguro de contenido al ser puesto a disposición.
g) Para almacenar información confidencial en los dispositivos móviles y/o de almacenamiento removible, ésta debe estar protegida con una contraseña segura para que impida accesos no autorizados a la información contenida en los dispositivos.
h) Todos/as deben proteger los dispositivos móviles y de almacenamiento removible (personales y/o asignados por la Entidad), no debiendo entregarlos a otra persona no autorizada, en particular aquellos dispositivos inteligentes que almacenan información confidencial y/o de uso interno de la Entidad. Los mensajes recibidos de números o remitentes desconocidos deben ser rechazados y borrados sin ser abiertos. Asimismo, todos/as deben cumplir las siguientes disposiciones:
    i. No dejar desatendido los dispositivos móviles y de almacenamiento removible. Adicionalmente, se debe activar el bloqueo de pantalla obligatoriamente.
    ii. No poner identificaciones del OSINFOR en el dispositivo, salvo los estrictamente necesarios.
    iii. Cuando el/la servidor/a se retire de las instalaciones y no lleve consigo el dispositivo móvil y/o de almacenamiento removible, debe guardarlo en un lugar seguro con llave; asimismo, la puerta de su oficina debe permanecer cerrada con llave, en los casos que corresponda.
    iv. Comunicar a la Mesa de Ayuda la pérdida o robo de todo dispositivo móvil y/o de almacenamiento removible gestionado por la Entidad, especialmente si éstos contienen información confidencial.

6.3 Seguridad ligada a los recursos humanos

Objetivo: Garantizar que todo el personal esté informado y capacitado de los controles en materia de seguridad de la información, para en el ejercicio de sus tareas diarias, para reducir los riesgos de error humano, comisión de ilícitos, manejo no autorizado de la información, uso inadecuado de instalaciones y/o recursos.

Lineamientos:

6.3.1 Previo al empleo

a) Durante la etapa de selección, la **URH** realiza la verificación de los documentos presentados por los/las postulantes.
b) Concluida la etapa de selección, la **URH** lleva a cabo controles de verificación a los/las postulantes ganadores/as de los procesos de

[1] Directiva de administración de bienes muebles del OSINFOR vigente.

selección. Estos controles incluyen todos los aspectos que indiquen las normativas vigentes que, a tal efecto, alcanzan al OSINFOR.

c) Todos/as los/las servidores/as y los/las proveedores/as críticos firmarán el Formato Acuerdo de Confidencialidad (SGSI-E2-FOR-004)[2], el cual forma parte del Contrato, en lo que respecta al tratamiento de la información del OSINFOR. Asimismo, las personas que realicen modalidades formativas. La copia firmada del Acuerdo debe ser custodiada en forma segura por la unidad de organización competente[3].
d) Los derechos y obligaciones los/las servidores/as o contratistas relativos a la seguridad de la información se encontrarán incluidos en los términos y condiciones del Contrato, por ejemplo, en relación con las leyes de propiedad intelectual o la legislación de protección de datos personales.

6.3.2 Durante el empleo

a) La concientización, educación y formación en seguridad de la información contempla lo siguiente:
   i. Los/Las servidores/as y contratistas (de ser el caso), recibirán inducción, charlas de capacitación y actualización periódica en materia de seguridad de la información.
   ii. La programación de capacitaciones al personal será elaborada por la **URH** en coordinación con la **UFCI** y será registrada en el Sistema de Gestión de la Capacitación[4].
   iii. La **URH** coordina con los/las servidores/as y el/la Oficial de Seguridad y Confianza Digital, para realizar la inducción correspondiente al personal nuevo y al personal que asuma nuevas responsabilidades, registrando la inducción realizada en el Formato de Inducción del Personal al SGSI (SGSI-E2-FOR-004)[5].
   iv. La **UFCI** actualizará cada año el material correspondiente a la capacitación que realiza el/la Oficial de Seguridad y Confianza Digital.
b) El proceso disciplinario se aplicará en caso de incumplimiento o vulneración de las políticas, normas y/o procedimientos relacionados a la seguridad de la información, por parte de los/las servidores/as, para lo cual se comunicará a la Secretaría Técnica de las Autoridades de los Órganos Instructores del Procedimiento Administrativo Disciplinario, la cual realiza la evaluación correspondiente de acuerdo a la normativa establecida en el sistema administrativo de gestión de recursos humanos.
c) Para el caso de contratistas que presten algún servicio al OSINFOR, serán pasibles de sanciones administrativas de acuerdo con el régimen de infracciones y sanciones de la Ley de Contrataciones del Estado[6], quienes presuntamente hayan vulnerado las políticas, normas y procedimientos relacionados a la seguridad de la información del OSINFOR.

6.3.3 Finalización o cambio de la relación laboral o empleo

a) La **URH** informa a los/las servidores/as sobre los cambios en su relación laboral o término.
b) Los derechos de acceso a la información y a las instalaciones de procesamiento deben ser cancelados y/o restringidos al producirse el término del empleo o contrato.

[2] Formato del Manual del Sistema Integrado de Gestión.
[3] URH en el caso de funcionarios/as, servidores/as civiles y de las personas que realicen modalidades formativas. UA en el caso de proveedores/as y/o contratistas que presten algún servicio al OSINFOR. UFCI en el caso de consultorías y/o servicios no contratados directamente por el OSINFOR.
[4] Sistema Informático de Gestión de la Capacitación de la Autoridad Nacional del Servicio Civil - SERVIR (http://siscapacitacion.servir.gob.pe/).
[5] Formato del Manual del Sistema Integrado de Gestión.
[6] Ley N° 30225, Ley de Contrataciones del Estado y su Reglamento aprobado mediante Decreto Supremo N° 344-2018-EF, y sus modificatorias.

c) La **URH** debe solicitar por correo electrónico a la **OTI** la actualización o desactivación de las cuentas de usuarios, a fin de mantener actualizado los accesos a los sistemas de información y servicios informáticos.
d) El/La Director/a o Jefe/a de la unidad de organización responsable de el/la servidor/a o contratista es quien solicitará el tipo de acceso y/o restricciones a los aplicativos y/o servicios del OSINFOR.
e) Los/Las servidores/as deben realizar la devolución de activos asignados siguiendo el Procedimiento de entrega de cargo de la **URH**[7], consignando en el Acta de Entrega de Cargo (A4.3.3-PRO-002-FOR-001) la ubicación de la información institucional generada durante su relación laboral, lo cual deberá ser validado por la persona que recibe la entrega de cargo respectiva o quien ésta designe.
f) Los/Las servidores/as que finalicen su relación laboral suscribirán una declaración jurada de no retirar información institucional y no divulgar información confidencial, conforme a la documentación para el cese proporcionada por la **URH**.

6.4 Gestión de activos de información

Objetivo: Identificar, clasificar y proteger los activos de información OSINFOR.

Lineamientos:

6.4.1 Inventario de activos

a) Los/Las responsables de los procesos identifican, elaboran y mantienen actualizado un inventario de activos de información, acorde al Procedimiento de Inventario de Activos de Información[8]. El inventario es registrado y revisado con una periodicidad anual y/o cada vez que haya un cambio en el proceso o en la Entidad.
b) En el inventario de activos de información también se deben registrar los medios y/o dispositivos almacenamiento removible del OSINFOR en donde se almacenen datos personales, los cuales serán clasificados como confidenciales.
c) Toda la información y los activos junto a sus medios de procesamiento de información son asignados a un/a responsable.
d) Los cambios en el inventario de los activos de información son coordinados con el/la **Oficial de Seguridad y Confianza Digital.**

6.4.2 Uso aceptable de los activos

a) Los activos de información deben ser utilizados de acuerdo a las políticas, directivas y procedimientos definidos, considerando criterios de buen uso.
b) La información que haya sido clasificada como “Confidencial” o de “Uso Interno”, no puede ser divulgada salvo que haya sido expresamente autorizado por el/la Propietario/a de la Información.
c) Cuando se necesite proporcionar información clasificada como “Confidencial” o de “Uso Interno” a terceros, se deberá requerir autorización por escrito al propietario/a de la información y verificar la suscripción previa de los correspondientes acuerdos de confidencialidad.
d) Todo/a servidor/a designado/a o contratado/a que ponga en riesgo los activos de información del OSINFOR, estará sujeto a la aplicación de medidas disciplinarias de acuerdo al Reglamento Interno de Servidores Civiles del OSINFOR. Esta sanción dependerá de la gravedad del incidente ocasionado y conforme a las normas establecidas.

[7] Procedimiento A4.3.3-PRO-002 del Manual de Procedimientos del OSINFOR vigente.
[8] Procedimiento E2.4.5-PRO-005 del Manual de Procedimientos del OSINFOR vigente.

e) Para el caso de contratistas y sus colaboradores/as que presten algún servicio al OSINFOR, que pongan en riesgo los activos; serán pasibles de sanciones administrativas de acuerdo con el régimen de infracciones y sanciones de la Ley de Contrataciones del Estado[9].

6.4.3 Devolución de los activos

a) Al término de la designación, vínculo laboral, o licencia con o sin goce de haber superior a 30 días calendario, todo/a servidor/a civil debe devolver todos los activos a su superior jerárquico, u otro/a servidor/a que éste/ésta designe para tal fin.

b) La devolución de activos de información asignados al personal sigue el Procedimiento de entrega de cargo[10] de la **URH**, al cual debe adjuntar el Acta de entrega y recepción de bienes en uso[11], que es proporcionado por el/la Especialista de Control Patrimonial de la **UA** previa verificación de los activos de información correspondientes a bienes muebles. En el caso de terceros a quienes se les haya proporcionado activos de información para el desarrollo de algún servicio específico, deberán realizar la devolución al responsable de la supervisión del servicio de la unidad de organización correspondiente.

c) Si los activos de información son equipos informáticos, dispositivos móviles o de almacenamiento removible, se deberá coordinar con la **OTI** para la realización del borrado seguro antes de ser puestos a disposición de otra unidad de la organización o destinados para la baja de bienes.

6.4.4 Clasificación de activos de información

a) Los activos de información de la Entidad deben ser clasificados de acuerdo al Procedimiento de Inventario de Activos[12] y a los Lineamientos de clasificación y desclasificación de información del OSINFOR[13]. Esta clasificación se define en 03 tipos:

i. **Confidencial:** Activos de información cuyo contenido no debe ser divulgado ni distribuido a personas que no sean autorizadas y cuya difusión genere un impacto importante en la Entidad, entre ellas: pérdida económica, sanción legal, pérdida de imagen u otras que alcancen dicho fin. Respecto a la información de datos personales de los/las servidores/as civiles y ciudadanos/as, utilizada por el OSINFOR en cualquiera de sus formas (física o digital) deberán ser categorizados adicionalmente como datos personales de manera explícita en el inventario de activos de información, para asegurar su correcto tratamiento.

ii. **Uso interno:** Activos de información cuyo contenido sólo debe ser de uso y divulgación para el personal interno de la Entidad, las cuales sólo podrán ser divulgados a terceras partes previa suscripción del acuerdo de confidencialidad y la autorización debida de el/la propietario/a de la información, siempre y cuando su divulgación no impacte a la Entidad.

iii. **Público:** Información de acceso público y que su divulgación no genera impacto en la Entidad.

b) El/La propietario/a de la información es el/la encargado/a de la clasificación de los activos de información que están bajo su responsabilidad.

[9] Ley N° 30225, Ley de Contrataciones del Estado, su Reglamento y modificatorias.
[10] Procedimiento A4.3.3-PRO-002 del Manual de Procedimientos del OSINFOR vigente.
[11] Directiva de administración de bienes muebles del OSINFOR vigente.
[12] Procedimiento E2.4.5-PRO-005 del Manual de Procedimientos del OSINFOR vigente.
[13] Directiva de clasificación y desclasificación de información del OSINFOR vigente.

c) El/La propietario/a de la información realiza la actualización en forma anual y/o cuando se estime que un activo de información ha aumentado su nivel de sensibilidad, en este caso se cambia su nivel de clasificación en forma inmediata, sin esperar el próximo ciclo de actualización. En caso contrario, al considerarse que la información ha disminuido su sensibilidad, podrá opcionalmente esperarse el próximo ciclo de actualización o modificar su clasificación con efecto inmediato. La responsabilidad de la decisión corresponde a el/la propietario/a de la información.
d) Toda la información que no ha sido específicamente clasificada es considerada como "Uso Interno", por lo que el/la propietario/a de la información debe autorizarla formalmente.

6.4.5 Etiquetado de activos de información

a) El etiquetado de los activos de información se debe realizar para los documentos en papel clasificados como confidencial siendo realizada por cada unidad de la organización.
b) Todas las correspondencias deben ser realizados por medios de transporte conocidos y seguros. La correspondencia no etiquetada como información confidencial será tratada como de uso interno.
c) Los envíos de información confidencial que se realicen por correo electrónico deben ser etiquetados como confidencial por cada remitente del mensaje, para que el/la destinatario/a pueda tomar las medidas pertinentes.
d) La documentación impresa y clasificada como confidencial, se almacena en lugares que puedan evitar riesgos frente a amenazas como incendios, inundaciones, accesos no autorizados, entre otros.
e) Se debe realizar un seguimiento de los documentos originales y copias de información confidencial, indicando como mínimo, la clasificación de información, el número de copias, la ubicación de las copias y las personas responsables de las copias.

6.4.6 Gestión de medios extraíbles

a) Todos los medios extraíbles y su contenido que no son necesarios para el OSINFOR y no tienen posibilidad de recuperación deben ser borrados de manera segura (mecanismos de escritura y/o destrucción física). En el caso de los bienes de capital, deben seguir además el procedimiento según las normas vigentes[14].
b) Los medios de almacenamiento de información son resguardados en un entorno seguro según las especificaciones del fabricante.
c) Se utilizan técnicas criptográficas para proteger los datos en caso de que la confidencialidad e integridad de la información contenida en el medio sean importantes y/o incluyan datos personales.
d) En el caso que los medios y/o dispositivos extraíbles en donde se almacenan datos personales no permitan el cifrado de la información, se deberá implementar controles compensatorios, como por ejemplo empaques a prueba de manipulación, para mitigar los riesgos a los que estarían expuestos.

6.4.7 Disposición de medios

a) Todo medio de almacenamiento de información debe ser resguardado o eliminado, según sea el caso de forma segura, respetando la normativa vigente.

[14] Item 6.5.9 de la Directiva Nº 001-2015/SBN, aprobada por Resolución Nº 046-2015/SBN.

b) Se identifican los activos o dispositivos que requieren su baja o eliminación. Para el caso de documentos, se cumplirá con la "Norma para la eliminación de documentos en los Archivos Administrativos del Sector Público Nacional"[15] y para el caso de bienes físicos, se seguirá el "Procedimiento de Gestión de los Bienes Muebles del Estado"[16]. Adicionalmente, en el caso de equipos informáticos, la **OTI** realiza el "Procedimiento de diagnóstico y baja de equipos informáticos"[17].
c) Los medios eliminados se registran de acuerdo a la normativa de eliminación de activos vigente y se mantiene el registro respectivo.

6.4.8 Transferencia de medios físicos

a) Los medios que contienen información son protegidos durante su transporte para evitar el acceso no autorizado, pérdida, mal uso o alteración de la información.
b) El OSINFOR cuenta con notificadores, servicios de transporte de carga y servicio de mensajería confiables.
c) Todo medio físico que contenga información confidencial que no esté cifrada debe contar con una protección física adicional.
d) Se debe identificar el medio de transporte para todo medio físico que contenga información confidencial, manteniendo un registro del remitente, destinatario, fecha y hora de salida.

6.5 Control de accesos

Objetivo: Garantizar que la información contenida en los sistemas, bases de datos y servicios de información en el OSINFOR, estén debidamente protegidos contra accesos no autorizados.

Lineamientos:

6.5.1 Requerimientos del OSINFOR para el control de accesos

a) Todos los accesos a los activos de información del OSINFOR, tanto lógicos como físicos, deben basarse en la necesidad y rol de el/la usuario/a, considerando:
   i. Identificación de la información relacionada a las aplicaciones y los riesgos a la que está expuesta.
   ii. Identificación de la legislación aplicable y las obligaciones contractuales con respecto a la protección del acceso a datos y servicios.
   iii. Uso de perfiles de usuarios estandarizados definidos según roles.
   iv. Administración de los derechos de acceso.
   v. Revisión periódica de los controles de acceso.
   vi. Revocación de los derechos de acceso.
b) Todo el personal o proveedor/a que requiera acceder a la red y servicios de red debe contar con las autorizaciones respectivas de los/las propietarios/as de los activos de información.
c) El acceso a los recursos de red, tanto internos como externos, son controlados, de manera que el personal no comprometa la seguridad de los activos de información, para lo cual se establecen los lineamientos de uso de la red, segmentación de redes, control de conexiones, controles de enrutamiento y seguridad de la información en los servicios de red.

6.5.2 Gestión de acceso a usuarios/as

[15] Regulado por el Archivo General de la Nación (AGN).
[16] Regulado por la Superintendencia Nacional de Bienes (SBN).
[17] Procedimiento A5.3.2-PRO-004 del Manual de Procedimientos del OSINFOR vigente.

a) Registro y baja de usuarios/as
   i. La **OTI** administra el registro y baja de los/las usuarios/as de los sistemas de información, base de datos y servicios de información.
   ii. El/La Especialista en Administración de Redes gestionará el registro y baja de usuarios de dominio y correo electrónico institucional. El/La Administrador/a de Base de Datos gestionará el registro y baja de usuarios de bases de datos y el/la Técnico/a Informático/a gestionará el registro y baja de usuarios de aplicaciones que no estén integradas al servicio de directorio de la red institucional (directorio activo).

b) Gestión de acceso a los/as usuarios/as
   i. La gestión de acceso a los servicios informáticos se realiza acorde a la "Directiva para el uso de recursos y servicios informáticos del OSINFOR" (A5-DIR-019) y al "Procedimiento Gestión de Accesos" (A5.3.1-PRO-002).
   ii. Los derechos de acceso de los/las usuarios/as son cancelados inmediatamente o suspendidos temporalmente una vez efectuada la comunicación a la **OTI**, en los siguientes casos: cuando cambien sus tareas, se les revoque la autorización, se encuentren de licencia por un tiempo mayor de cinco (5) días laborales, se desvinculen del OSINFOR o por pérdida/robo de sus credenciales de acceso.
   iii. La **OTI** efectúa revisiones periódicas con el objeto de:
      - Cancelar identificadores y cuentas de usuario redundantes.
      - Desactivar cuentas inactivas por más de 60 días.
      - En el caso de existir excepciones, deben ser debidamente justificadas y aprobadas.

c) Gestión de derechos de acceso privilegiados
   i. Se restringe y controla la asignación y uso de los derechos de acceso privilegiados.
   ii. Se identifican los derechos de acceso privilegiados, asociados a cada sistema o proceso, así como los/las usuarios/as a los que se les está otorgando.
   iii. Se cuenta con un registro de todos los derechos de acceso privilegiado asignados, consignando la expiración correspondiente.
   iv. Se revisa periódicamente las cuentas de los/las usuarios/as con los accesos privilegiados y si se encuentran alineados a sus funciones.

d) Gestión de la información de autenticación secreta de los usuarios
   i. Se verifica la identidad de el/la usuario/a antes de proporcionarle la información de autenticación secreta (nueva, sustitutiva o temporal).
   ii. La entrega de la información de autenticación temporal debe hacerse en forma segura y única para cada usuario/a, con la indicación y configuración de cambio de contraseña.

e) Revisión de los derechos de acceso de usuario
   i. El/La Propietario/a de la información debe realizar un proceso formal, a intervalos regulares, a fin de revisar los derechos de acceso de los/las usuarios/as.
   ii. Se contemplan los siguientes controles:
      - Revisar los derechos de acceso de los/las usuarios/as a intervalos de 6 meses.
      - Revisar las autorizaciones de acceso privilegiados a intervalo de 3 meses.

f) Eliminación o ajuste de los derechos de acceso
   i. Los derechos de acceso a la información y/o áreas seguras del personal o usuarios/as externos/as, son eliminados como consecuencia de la desvinculación laboral, resolución de contrato o acuerdo.

ii. Para el caso de cambio de funciones a los/las usuarios/as se realiza los ajustes de los derechos de acceso, de la siguiente manera primero se retiran los derechos de acceso que se tenía y luego se dan los nuevos derechos de acceso, previa autorización de el/la responsable del sistema de información (administrador/a de la gestión de datos) o de el/la responsable del recurso compartido.

iii. Se podrá reducir o eliminar todos los derechos de acceso a la información y los activos asociados a las instalaciones de procesamiento de información antes de la finalización del vínculo laboral o contractual, cambio, siempre y cuando existan causas justificadas.

6.5.3 Uso de información de autenticación

a) Todo/a usuario/a es responsable de la confidencialidad de la contraseña de la cuenta de usuario asignada, así como de las consecuencias por las acciones que se puedan hacer con la cuenta de usuario asignada.
b) El personal cambiará su contraseña regularmente o cada vez que el sistema se lo solicite. Está prohibido compartir las contraseñas de las cuentas de usuario asignadas.
c) Para realizar la restauración de contraseñas se sigue las instrucciones establecidas por la **OTI**.

6.5.4 Control de acceso a los sistemas y a las aplicaciones

a) Restricción de acceso a la información
   i. El acceso a la información y a las funciones del sistema cuentan con controles de seguridad de la información (por ejemplo, usuario y contraseña), a fin de evitar accesos no autorizados a recursos o información, así mismo, los derechos de acceso ya sea de lectura, escritura, borrar y ejecutar son controlados, también los datos y aplicaciones que son accedidos por el usuario.
   ii. En caso amerite o sea necesario, se deberá limitar el acceso a los recursos de red de las cuentas de usuario, por horarios de trabajo y tiempo de conexión.
   iii. Se cancelan sesiones inactivas luego de un periodo determinado en las aplicaciones críticas y sistemas operativos.
   iv. En caso de alguna posible intrusión fallida o exitosa de los controles de inicio de sesión, se genera un evento de seguridad de la información.
b) Procedimientos seguros de inicio de sesión
   i. Todos/as los/las usuarios/as del OSINFOR cuentan con una cuenta de usuario y contraseña, lo que asegura el inicio seguro a los sistemas de información y sistema operativo.
   ii. En el caso que se requiera podrá tenerse una línea de conexión exclusiva para transmisión de información para los usuarios externos, estableciendo una comunicación segura entre el OSINFOR y el punto de acceso del usuario externo.
c) Sistema de gestión de contraseñas
   i. Los sistemas de gestión de contraseñas son interactivos y garantizan contraseñas de calidad.
   ii. Todas las contraseñas e identificaciones (IDs) son individuales, permitiendo a los/las usuarios/as seleccionar y cambiar sus contraseñas.
   iii. El cambio de contraseñas es de cada 90 días y se tienen restricciones para la reutilización de contraseñas.
   iv. El almacenamiento y transmisión de las contraseñas se realiza en forma protegida.
d) Uso de programas utilitarios privilegiados

i. El uso de programas utilitarios está restringido y se limita el uso sólo para usuarios/as autorizados/as.
ii. Todo programa utilitario pasa por un proceso de identificación, autenticación y autorización de uso, así como su registro, definición y documentación.
iii. Todo programa innecesario para el/la usuario/a según perfil es eliminado.

e) Control de acceso al código fuente del programa
   i. El acceso al código fuente de las aplicaciones o sistemas de información del OSINFOR se encuentra restringido y controlado estrictamente, manteniendo un registro de todos los accesos a bibliotecas fuentes de programas.
   ii. Las bibliotecas de programas fuentes no deben mantenerse en los sistemas en producción.
   iii. Se cuenta con un registro de bibliotecas fuentes de programas sujetos a procedimientos de control de cambios.

6.6 **Criptografía**

Objetivo: Proteger la confidencialidad, autenticidad y la integridad de la información en el OSINFOR, asegurando que la información clasificada como reservada y/o confidencial reciba un tratamiento especial a través de mecanismos criptográficos, reduciendo los riesgos durante el almacenamiento, transporte y transmisión de la información.

Lineamientos:

6.6.1 Uso de controles criptográficos en sistemas de información y servicios de TI

a) La protección del acceso a sistemas, datos y servicios contempla los siguientes aspectos:
   i. El dominio *osinfor.gob.pe* trabaja con certificados digitales SSL, los cuales son utilizados durante el acceso a los diferentes sistemas de información.
   ii. El control sobre los certificados digitales vigentes lo realiza el/la Especialista en Administración de Redes solicitando la información sobre los certificados actuales y los que se van a implementar.
   iii. Si es un certificado nuevo:
      - Se verifica los requerimientos técnicos del certificado digital, como son el tipo de cifrados (1024, 2048 bits), vigencia, etc.
      - Se realiza el pedido y la compra del nuevo certificado.
      - Se implementa el certificado en el aplicativo y dirección URL respectiva.
      - Se valida el funcionamiento del certificado, realizando las pruebas en las páginas web respectivas.
      - Se elabora un informe sobre el funcionamiento de la instalación del certificado nuevo y de los que ya están instalados.
   iv. Si no es un certificado nuevo:
      - Se verifica la vigencia del certificado de acuerdo con la información solicitada.
      - Si la vigencia es menor de 3 meses se solicita la renovación del certificado.

b) Los controles criptográficos de la plataforma digital única del Estado Peruano (.GOB.PE) a la cual se ha migrado el portal institucional https://www.gob.pe/osinfor, son establecidos y administrados por la Secretaría de Gobierno y Transformación Digital de la Presidencia del Consejo de Ministros.

6.6.2 Uso de controles criptográficos para firmar digitalmente

a) El OSINFOR utiliza el certificado digital emitido por el Registro Nacional de Identificación y Estado Civil del Perú (RENIEC), el cual consiste en certificados digitales de clase III emitidos a nombre de los servidores civiles de OSINFOR, donde cada servidor/a representa al suscriptor, y el OSINFOR al titular de la entidad pública. Este certificado es utilizado para firmar digitalmente los documentos.
b) La OTI gestiona y realiza el control sobre estos certificados digitales, brindando la asistencia técnica para la instalación y configuración de dicho certificado.
c) El personal técnico instala y configura el certificado en el equipo asignado a el/la servidor/a, solicitando a el/la servidor/a asignar una contraseña para uso del certificado.
d) El/La servidor/a valida el uso del certificado para firma digital con la contraseña generada personalmente.

6.6.3 Uso de controles criptográficos en dispositivos móviles y de almacenamiento removible

a) Los/Las servidores/as deben utilizar técnicas de cifrado en sus dispositivos móviles o de almacenamiento removible, cuando los mismos contengan información confidencial de la Entidad, para lo cual solicitarán la respectiva asistencia a la OTI a través de la Mesa de Ayuda.
b) Los/Las servidores/as que apliquen el cifrado de sus dispositivos móviles o de almacenamiento removible, deben tomar en consideración que son los únicos responsables de la contraseña de cifrado establecida y si pierden la contraseña de encriptación se perderá el acceso a todos los datos contenidos en estos dispositivos.

6.6.4 Uso de controles criptográficos para información confidencial

a) La OTI utilizará herramientas y/o mecanismos de encriptación segura de archivos, carpetas y unidades para la ejecución de las copias de respaldo y replicación.
b) Los/Las servidores/as que requieren transferir algún documento en digital que contiene información confidencial, deben establecer una clave o contraseña, teniendo en consideración que una vez que se realice esta acción, sólo la persona que tenga la clave o contraseña podrá acceder al contenido del documento y leerlo.
c) Los/Las servidores/as que apliquen clave en documentos confidenciales deben acordar previamente con el personal autorizado a tener acceso al documento confidencial cual será la clave de acceso establecida para determinado documento.

6.7 **Seguridad física y de ambiente**

Objetivo: Evitar pérdidas, daños a los activos de información, así como la interrupción de las actividades del OSINFOR, a través de la protección de las áreas y/o equipos de almacenamiento y procesamiento de información crítica.

Lineamientos:

6.7.1 Áreas de Seguridad

a) Perímetro de seguridad física
   i. El perímetro de seguridad física se encuentra delimitado para el Centro de Datos, ambientes de comunicaciones de red y el Archivo. Las especificaciones técnicas dependerán del nivel de protección requerido para la seguridad de los activos de información.
   ii. Se protegen las áreas donde funcionan las instalaciones de procesamiento de información, suministro de energía eléctrica, aire

acondicionado y cualquier otra que sea clasificada como crítica y que pudiera afectar el funcionamiento de los sistemas de información.

iii. El área segura debe controlar el acceso físico.

b) Controles de acceso físico

i. El OSINFOR cuenta con controles que aseguren el acceso físico sólo a las personas debidamente autorizadas.

ii. El acceso y la permanencia de visitas sólo serán permitidos para propósitos específicos y con autorización respectiva, quedando debidamente registrados.

iii. El/La servidor/a que atiende al visitante será responsable de la permanencia de éste/a hasta su salida.

iv. De preferencia el/la administrado/a será atendido/a en un ambiente de atención al ciudadano o equivalente, para cualquier caso.

v. La **OTI** supervisa que se limite el acceso a la información digital clasificada y a las instalaciones de procesamiento y resguardo de información digital, permitiendo el acceso exclusivamente a las personas autorizadas.

vi. Se utilizarán los siguientes controles para validar y registrar todos los accesos:

- Sede Central
  - Personal de vigilancia[18].
- Oficinas Desconcentradas:
  - Personal de vigilancia.
  - Cámaras de seguridad con grabador (DVR/NVR)[19]
- Centro de Datos:
  - Cámaras de seguridad internas y externas con grabador (DVR/NVR).
  - Unidad de control de acceso biométrico (huella).
  - Cuaderno de registro de ingreso al Centro de Datos.
- Archivo:
  - Puerta con llave.

vii. Los registros manuales del personal de vigilancia para control de acceso a instalaciones se mantendrán protegidos por el periodo de (6) seis meses para permitir auditar todos los accesos físicos.

viii. Las imágenes y/o grabaciones dentro del grabador DVR/NVR de las cámaras de vigilancia se mantendrán por treinta (30) días calendarios, excepcionalmente, si la grabación contiene información sobre la comisión de delitos, faltas o existe una investigación sobre los hechos grabados, ésta podrá ser almacenada durante un periodo mayor al establecido.

ix. El control de las cámaras de videovigilancia instaladas en la Sede Central está bajo la supervisión de la **UA**, a excepción de las cámaras ubicadas en el Centro de Datos del OSINFOR, cuya administración y control le corresponde al Especialista en Administración de Redes.

x. El control de las cámaras de videovigilancia de las Oficinas Desconcentradas está bajo la supervisión de el/la Jefe/a de la Oficina Desconcentrada.

xi. En caso sea requerido el acceso a información registrada por las cámaras de videovigilancia, se deberá solicitar a la unidad de la

[18] El local en donde se ubica actualmente la Sede Central tiene implementado un servicio de cámaras de seguridad.

[19] La implementación de cámaras de seguridad internas y externas en las Oficinas Desconcentradas es realizada progresivamente, teniendo como prioridad las sedes definidas en el alcance del Sistema de Gestión de Seguridad de la Información.

organización responsable[20], a través de los canales[21] establecidos con la justificación respectiva. Dicha solicitud deberá ser comunicada a el/la **Oficial de Seguridad y Confianza Digital**, para la supervisión de la entrega de información.

c) Seguridad en oficinas, despachos e instalaciones
   i. Las áreas dedicadas al procesamiento de información deben ser ubicadas en lugares que no presenten riesgos desde el punto de vista de acceso al público.
   ii. El personal o terceros no deben facilitar el acceso a las instalaciones a personas desconocidas o no autorizadas.
   iii. Toda persona visitante deberá ser identificado/a y cumplir con el protocolo establecido.
   iv. Los/Las servidores/as, proveedores/as y visitantes deben hacer uso en forma visible de la identificación de acceso (fotocheck/tarjeta de visitante) para el ingreso y durante la permanencia en las instalaciones.
   v. La **UA** mantiene un registro de los/las contratistas autorizados para acceder a las instalaciones de la Sede Central.
   vi. El personal de vigilancia controlará y registrará en el cuaderno de seguridad el ingreso de computadoras portátiles, equipos fotográficos, de vídeo, audio o cualquier otro tipo de equipamiento que registre información.
   vii. El/La **Oficial de Seguridad y Confianza Digital** en coordinación con la **UA** realizará un monitoreo inopinado al personal de vigilancia sobre las actividades de vigilancia de manera semestral.
   viii. La **OTI** en coordinación con la **UA** deberán ubicar el equipamiento de procesamiento, digitalización y reproducción de información, adecuadamente dentro del área protegida para evitar accesos no autorizados que podrían comprometer la información.
   ix. Las puertas permanecerán cerradas fuera del horario laboral.

d) Protección contra amenazas externas y del ambiente
   El/La **Oficial de Seguridad y Confianza Digital** supervisará que los equipos se encuentren ubicados adecuadamente y protegidos de tal forma que se reduzcan los riesgos como resultado de las amenazas y los peligros del medio ambiente, así como las oportunidades de acceso no autorizado.

e) Trabajo en las áreas seguras
   a) Las actividades realizadas en las áreas seguras deben ser supervisadas por el/la **Oficial de Seguridad y Confianza Digital** para identificar y minimizar los riesgos de seguridad de la información.
   b) Los/Las Jefes/as y/o Directores/as de las unidades de organización deben dar a conocer al personal bajo su cargo la existencia del área protegida o de las actividades que allí se llevan a cabo, sólo si es necesario para el desarrollo de sus funciones.
   c) Los/Las Jefes/as y/o Directores/as de las unidades de organización deben limitar y controlar el acceso al personal externo a las áreas protegidas o a las instalaciones de procesamiento de información.
   d) Los/Las servidores/as deben impedir el ingreso de equipos de computación móvil, fotográfico, de video, audio o cualquier otro tipo de equipamiento que pueda registrar o almacenar información, salvo que hayan sido formalmente

[20] UA para cámaras de videovigilancia instaladas en las áreas comunes de la Sede Central, Jefatura de OD para las cámaras de videovigilancia de las Oficinas Desconcentradas, y OTI para cámaras de videovigilancia del Centro de Datos

[21] UA: consultasyservicios@osinfor.gob.pe / OTI: mesadeayuda@osinfor.gob.pe

autorizados por el/la Jefe/a y/o Director/a de la unidad de organización y/o el/la Oficial de Seguridad y Confianza Digital.

f) Áreas de acceso público
   i. La **UA** debe inspeccionar el material entrante para descartar peligros potenciales antes de ser trasladados al almacén.
   ii. La **UA** debe registrar y verificar el material entrante al ingresar al área de almacén tomando en consideración lo establecido en la normativa vigente para este caso.

6.7.2 Protección de equipos

a) Ubicación y protección del equipamiento
   i. Los equipos se encuentran ubicados y protegidos frente a las amenazas y peligros ambientales, así como lejos del alcance de personas no autorizadas.
   ii. El Centro de Datos del OSINFOR cuenta con un sistema automático/dedicado de protección contra incendios, sistema de monitoreo automático y/o manual de las condiciones ambientales de temperatura y humedad, para que no se afecte el normal funcionamiento de los equipos de tratamiento de información.
   iii. Las instalaciones de procesamiento y almacenamiento de información confidencial serán ubicadas en un sitio que permita su supervisión constante.

b) Instalaciones de suministro
   i. Se cuenta con sistemas de protección eléctrica y fuentes de energía tipo UPS (Uninterruptible Power Supply) que brindan soporte al Centro de Datos, estaciones de trabajo (workstations) y a los equipos de telefonía fija; en caso de los equipos informáticos que no cuenten con dicha protección eléctrica, los/las servidores/as son responsables del apagado y/o desconexión de los equipos de cómputo para asegurar la continuidad de las operaciones mientras se restablecen las fallas en el suministro de energía eléctrica.
   ii. Los servicios de suministro son inspeccionados y probados una vez al año por la **UA**, para asegurar su correcto funcionamiento.

c) Seguridad en el cableado
   i. El cableado de energía o de telecomunicaciones se encuentra protegido de cualquier intercepción o daño.
   ii. El cableado de suministro de energía eléctrica y telecomunicaciones en las zonas de tratamiento de información cuenta con un sistema de puesta a tierra (pozo a tierra), el que es revisado anualmente para garantizar su adecuado funcionamiento.

d) Mantenimiento de equipos
   Los mantenimientos de los equipos se realizan de acuerdo con el procedimiento de mantenimiento de equipos informáticos de la **OTI**.

e) Retiro de activos de información de propiedad del OSINFOR
   i. Para el retiro de activos que son bienes de propiedad del OSINFOR se debe contar con autorización formal; adicionalmente el/la Especialista en Control Patrimonial de la **UA** registra la salida de bienes a través del Acta de Autorización de Salida de Bienes Patrimoniales[22] .

[22] Formato N° 03 de la Directiva de administración de bienes muebles del OSINFOR vigente.

ii. El tratamiento de los expedientes en préstamo que se encuentran en las Direcciones de Línea es controlado por la **UADA** a través del Sistema de Información de Gestión Documental (SIADO).

f) Seguridad de equipos fuera del local
   i. El uso de equipos del OSINFOR fuera de las instalaciones debe ser autorizado, el personal autorizado será responsable de su custodia.
   ii. Para poder utilizar algún equipo de tratamiento de información fuera del OSINFOR, se deberá contar con la autorización de el/la Jefe/a Inmediato/a Superior (quien solicita la salida del equipo) y de el/la Jefe/a de la **UA**.

g) Equipo desatendido por el usuario
   i. Los/Las usuarios/as deben cerrar sesión de aplicaciones o servicios de red cuando finalicen, no hagan uso de ellas o cuando se ausenten de su ubicación; asimismo, el equipo utilizará mecanismos de bloqueo de pantalla con protección de acceso luego de tres (03) minutos de inactividad.
   ii. Los/Las usuarios/as deben desconectar y guardar en un lugar seguro cualquier medio de almacenamiento removible utilizado en sus equipos, antes de dejar desatendido su puesto de trabajo.

6.8 **Pantalla y escritorios limpios**

Objetivo: Prevenir el acceso no autorizado, pérdida y/o daño de la información física y digital que se encuentra en los lugares de trabajo, equipos de cómputo, medios magnéticos u ópticos, dispositivos de impresión y digitalización de documentos, durante y fuera del horario laboral.

Lineamientos:

6.8.1 Ubicación de escritorios y equipos
   a) Los lugares de trabajo de los/las servidores/as se localizan en ubicaciones que no queden expuestas al acceso de personas externas. De esta forma se protege tanto el equipamiento tecnológico como los documentos que pudiera estar utilizando el/la usuario/a.
   b) Los equipos que queden ubicados cerca de zonas de atención o tránsito de público se ubican de forma que las pantallas no puedan ser visualizadas por personas externas.

6.8.2 Escritorios limpios
   a) Toda vez que un/a servidor/a se ausenta de su lugar de trabajo, debe bloquear su estación de trabajo y guardar en lugar seguro cualquier documento, medio magnético u óptico removible que contenga información confidencial.
   b) Si el/la servidor/a está ubicado cerca de zonas de atención de público, al ausentarse de su lugar de trabajo debe guardar también los documentos y medios que contengan información de uso interno.
   c) Al finalizar la jornada de trabajo, el/la servidor/a debe guardar en un lugar seguro los documentos y medios que contengan información confidencial o de uso interno.
   d) Cuando se imprima información sensible y/o confidencial, se debe retirar inmediatamente de las impresoras. Asimismo, no debe permanecer ninguna hoja impresa en la impresora, para evitar que cualquier persona no autorizada las recoja.
   e) No debe exponerse credenciales o notas con información confidencial en los escritorios o lugares de trabajo.

6.8.3 Pantallas limpias

a) Las estaciones de trabajo y equipos portátiles cuentan con mecanismos de protección y bloqueo de pantalla que se activarán luego de tres (03) minutos de inactividad.
b) La pantalla de autenticación a la red del OSINFOR debe requerir solamente la identificación de la cuenta y una clave y no entregar otra información.
c) Toda vez que el/la servidor/a se ausente de su lugar de trabajo debe bloquear su estación de trabajo o laptop para así proteger el acceso a las aplicaciones y servicios del OSINFOR.
d) Las pizarras que contengan información sensible y/o confidencial deben borrarse.

6.9 **Seguridad de las operaciones**

Objetivo: Asegurar la operación correcta y segura en las instalaciones de procesamiento de información, monitorear las actividades de procesamiento de información para detectar acciones no autorizadas y minimizar el riesgo de fallos de los sistemas.

Lineamientos

6.9.1 Procedimientos y responsabilidades operacionales

a) Todo cambio en los procesos, sistemas, plataforma tecnológica, componentes o instalaciones de procesamiento de la información que afecten a la seguridad de la información son gestionados por el "Procedimiento de Gestión de Cambios"[23].
b) La **OTI** realiza la gestión de la capacidad tecnológica para lo cual debe:
   i. Identificar los requerimientos de capacidad teniendo en cuenta la criticidad del sistema para los procesos misionales del OSINFOR.
   ii. Proyectar el aprovisionamiento de recursos, desarrollando planes asociados a la gestión de la capacidad de recursos.
   iii. Depurar datos obsoletos en disco.
   iv. Desinstalar aplicaciones, sistemas, bases de datos o entornos obsoletos e inseguros.
   v. Restringir el ancho de banda para servicios de alta demanda de recursos en caso de que no sean críticos para el OSINFOR.
   vi. Controlar el rendimiento de la plataforma tecnológica, a través de la monitorización de los recursos de tecnología de la información.
   vii. Desarrollar planes asociados a la gestión de la capacidad de recursos.
c) La **OTI** asegura la separación de los ambientes para desarrollo, prueba, integración y producción considerando lo siguiente:
   i. Los ambientes de desarrollo, calidad y producción mantienen el nivel de separación necesario para prevenir problemas operacionales, así como los controles de acceso adecuados para cada uno de ellos.
   ii. El acceso a los ambientes de desarrollo y calidad está restringido exclusivamente al personal de desarrollo de sistemas de la **OTI**, a los/las proveedores/as y/o contratistas, así como los consultores/as externos autorizados/as por la **OTI**, para la realización de labores específicas.
   iii. El acceso a los ambientes de producción está restringido exclusivamente a personal de infraestructura y soporte técnico de la **OTI**, a los/las proveedores/as y/o contratistas, así como los consultores/as externos autorizados/as por la **OTI**, para la realización de labores específicas.
   iv. El/La Especialista en Administración de Redes, el/la Administrador de Base de Datos y el/la Coordinador/a de Proyectos de Sistemas de Información son responsables de la administración, mantenimiento, operatividad continua, seguridad y rendimiento aceptable de los servicios

[23] Procedimiento A5.2.4-PRO-001 establecido en el Manual de Procedimientos del OSINFOR vigente.

y de la plataforma tecnológica de los ambientes de desarrollo, calidad y producción.

6.9.2 Protección ante software malicioso

a) El software utilizado por el OSINFOR debe ser autorizado en forma expresa por la **OTI**.
b) Para reducir la presencia de códigos maliciosos (virus, gusanos, troyanos, spyware, entre otros) en los sistemas de información y los medios de procesamiento, el sistema de antivirus se encuentra habilitado en los equipos del OSINFOR y es verificado en los equipos personales de quienes requieran ingresar a la red del OSINFOR.
c) El/La Especialista en Administración de Redes es responsable de instalar, configurar, monitorear y controlar el sistema de antivirus a nivel de servidores y equipos dentro de la red institucional. El/La Técnico/a Informático es responsable de instalar y monitorear el software antivirus en los equipos de usuario final (computadoras personales, equipos portátiles, teléfonos inteligentes, entre otros), asignados por la Entidad en las distintas sedes.
d) El sistema de antivirus es actualizado periódicamente y configurado para realizar revisiones programadas para la detección de virus en los equipos del OSINFOR.

6.9.3 Respaldo

a) El respaldo y recuperación de la información se realiza de acuerdo al "Procedimiento gestión de la continuidad de operaciones de TI"[24].
b) El respaldo de la información comprende la información alojada en los servidores físicos y/o virtuales (bases de datos, código fuente, aplicaciones, archivos institucionales) equipos de seguridad y de comunicaciones (archivos de configuración) ubicados en el Centro de Datos, lugar de contingencia o almacenamiento en la nube, gestionados por la **OTI**.
c) La plataforma tecnológica para el desarrollo de copias de respaldo debe contar con mantenimiento preventivo anual.
d) Los criterios de seguridad para las copias de respaldo son:
    i. Cifrado que garantice la confidencialidad e integridad de la información.
    ii. Conservación en un ambiente protegido que cumpla con las condiciones de climatización.
    iii. Almacenamiento en lugares diferentes (uno localmente y otro en un sitio externo).
    iv. Utilización de medios diferentes, 2 como mínimo (uno en el sistema de almacenamiento del Centro de Datos, otro en un medio de almacenamiento removible).
    v. Ejecución de copias de seguridad antes de realizar cambios importantes en algún equipo, sistema de información, aplicación o base de datos.
    vi. Ejecución de las copias de respaldo en horarios que no saturen el tráfico de la red, iniciando a partir de las 00:00 horas de lunes a domingo.
    vii. Comprobación de las copias de respaldo de manera periódica, realizando pruebas de restauración, con la participación de personal de la unidad de la organización responsable, de acuerdo con la programación establecida por la **OTI**.
    viii. Control de la vida útil de los medios de soportes físicos de las copias de respaldo. Antes de desechar los soportes que han sido utilizados para realizar copias de respaldo, deberán aplicarse mecanismos de borrado seguro (desmagnetización o destrucción física).
    ix. El periodo de conservación de las copias de respaldo es de 5 años como mínimo, posterior a este tiempo, los medios de respaldo podrán ser

[24] Procedimiento A5.3.5-PRO-004 establecido en el Manual de Procedimientos del OSINFOR vigente.

reutilizados, previa verificación del estado físico y lógico del medio de respaldo.

6.9.4 Registros y monitoreo

a) Todo evento de actividades de usuarios, excepciones, fallas, cambios de configuración y de seguridad se deben registrar en los sistemas. Los/Las especialistas de la **OTI** deben realizar el mantenimiento y revisión periódica de los mismos.
b) Se debe registrar también el uso de privilegios, uso de utilidades y aplicaciones del sistema, archivos accedidos y tipo de acceso; direcciones y protocolos de red; alarmas configuradas por el sistema de control de acceso; activación y desactivación de los sistemas de protección, tales como sistemas de antivirus y sistemas de detección de intrusos.
c) Se deben proteger los registros (logs) contra su alteración y acceso no autorizado, así como prevenir la edición o eliminación de los archivos que contienen estos registros. Asimismo, se debe contar con copias de respaldo de los registros de eventos que se generen de los sistemas de información, servidores, equipos de comunicaciones, etc. al menos de los últimos 30 días.
d) Todas las actividades del administrador y operador que requieran el uso de privilegios administrativos deben ser registrados por dichos equipos y/o sistemas correspondientes. Estos registros son protegidos y se revisan regularmente para controlar las acciones y responsabilidades de los/las usuarios/as privilegiados/as.
e) Todos los equipos de la red conectados al dominio del OSINFOR se conectan al servidor NTP para su sincronización de actualización de los relojes. Cualquier alteración de los relojes en los servidores de producción se debe registrar y reportar para su tratamiento.

6.9.5 Control de software en producción

a) La **OTI** a través de sus especialistas, revisa periódicamente el software instalado y las licencias que se han adquirido para asegurar que sólo el software permitido sea utilizado en el OSINFOR.
b) El/La Técnico/a Informático mantiene un registro del software permitido, así como el inventario de software de la Entidad.
c) La **OTI** salvaguarda el cumplimiento de la Ley de Derechos de Autor, comprendiendo e informando las consecuencias de su incumplimiento, incluyendo las sanciones correspondientes.
d) La **OTI** mantiene actualizado el registro de software permitido, para guiar la compra de nuevo software y definir aquel que debe ser mantenido en las computadoras y servidores.
e) El software no permitido o sin licencias serán desinstalados por personal de soporte técnico de la **OTI**. Así también se desinstalarán el software que ya no se usa en las computadoras.
f) La **OTI** debe velar que el software que se adquiera se realice a través de un proceso de compra formal para asegurar que se obtengan las aprobaciones adecuadas, y que los registros de compra, recepción e inventario son creados y almacenados en los sistemas de información de la Entidad.
g) Para el software desarrollado por la Entidad y/o adquiridos por donación o por convenios, la **OTI** solicita o genera, según sea el caso, la documentación necesaria para asegurar el control de los mismos.
h) El/La Coordinador/a de Proyectos de Sistemas es responsable del inventario del software de sistemas de información de la entidad.

6.9.6 Gestión de vulnerabilidad técnicas

a) La **OTI** realiza el análisis de vulnerabilidades técnicas de los sistemas de información en uso y de la plataforma tecnológica, una vez al año con algún proveedor o servicio externo.
b) Los/Las especialistas de la **OTI** evalúan las vulnerabilidades técnicas identificadas y realizan las acciones de remediación respectiva, bajo la supervisión de el/la **Oficial de Seguridad y Confianza Digital**.

6.9.7 Restricciones en la instalación de software por los/las usuarios/as

a) Se restringe la instalación de software a los/las usuarios/as finales, permitiendo sólo al personal autorizado de la **OTI**. El personal encargado de instalar software en los equipos informáticos de usuario final (computadoras, laptops, tabletas, smartphone, etc.) son los/las técnicos/as de soporte, y el/la especialista en administración de redes en el caso de la plataforma tecnológica del centro de datos y gabinetes de comunicaciones.
b) La **OTI** controla que sólo el software permitido sea instalado en los equipos.

6.9.8 Consideraciones sobre la auditoría de sistemas de información

a) La **OTI** en coordinación con el/la **Oficial de Seguridad y Confianza Digital** planifica y acuerda los requisitos y las actividades de auditoría que implican la verificación de los sistemas operativos para minimizar las interrupciones en los procesos misionales del OSINFOR.
b) Se controla el alcance de las verificaciones, éstas son limitadas a accesos de sólo lectura al software y a los datos; en caso de que las verificaciones afecten la disponibilidad del sistema, se realizan fuera de horario de oficina.

6.10 **Seguridad de las comunicaciones**

Objetivo: Implementar y mantener un nivel apropiado de seguridad en el OSINFOR para transferencia e intercambio de información interna y con instituciones externas.

Lineamientos

6.10.1 Gestión de la seguridad de red

a) Se han establecido procedimientos para la gestión de redes y comunicaciones, así como de gestión de las operaciones e instalaciones de infraestructura de Tecnologías de la Información (TI).
b) El/La Especialista en Administración de Redes es el responsable de gestionar y controlar las redes informáticas, garantizar la seguridad de la información en la red del OSINFOR y proteger los servicios conectados a la red desde accesos remotos. En ese sentido, administra los equipos de seguridad perimetral (firewall, entre otros), los accesos a la red pública de los equipos, la comunicación entre equipos de diferentes redes (habilitar el acceso a nivel de firewall) y los perfiles de internet a través de conexiones remotas vía HTTPS, RDP o SSH hacia las consolas de administración. También administra y monitorea los equipos de comunicaciones de la red interna y externa a través del software de monitoreo establecido, por lo tanto, es responsable de la configuración de la red cableada e inalámbrica y garantizar la disponibilidad de las comunicaciones de la red de datos.
c) La seguridad en los servicios de las redes es controlada, administrada y gestionada a través de los requerimientos, análisis y/o monitoreo que se realiza en el firewall.
d) Asimismo, los administradores de la red interna aseguran las configuraciones de los puertos de red para restringir intrusiones y tráfico malicioso.
e) La red del OSINFOR está segmentada. La red interna se conforma como mínimo de dos segmentos (voz y datos), los cuales están protegidos por

soluciones firewall/UTM, antispam y filtro web, que permite los accesos entre ellos y hacia Internet.

f) El/La Especialista en Administración de Redes mantiene el registro y control de los segmentos de red utilizados en la Sede Central y Oficinas Desconcentradas de ser necesario.

6.10.2 Transferencia de información

a) Es obligatorio mantener la seguridad en el intercambio de información del OSINFOR con cualquier otra entidad externa, ya sean estas entidades reguladoras u otras. Los intercambios de información se realizan utilizando el protocolo SFTP. Asimismo, cualquier entidad externa que quiera conectarse al SFTP utilizando la conexión de Internet, deberá suscribir un acuerdo de confidencialidad.

b) Los acuerdos de transferencia de información consideran:
   i. Transferencia segura de información entre el OSINFOR y las entidades externas.
   ii. Ambas entidades tienen que contar con accesos y credenciales al servidor SFTP del cual compartirán información.
   iii. La entidad externa que desea conectarse al servidor SFTP del OSINFOR, tiene que proveer al Especialista en Administración de Redes la dirección IP pública que utiliza, para que ésta sea permitida a través del firewall.
   iv. Ambas entidades se rigen bajo los acuerdos de confidencialidad y no divulgación de la información.

c) Aseguramiento de la mensajería electrónica, considerando lo siguiente:
   i. El servicio de correo electrónico que se brinda al personal es de propiedad exclusiva del OSINFOR. El correo electrónico y su contraseña respectiva son confidenciales, personales e intransferibles.
   ii. El OSINFOR se reserva el derecho de activar las opciones de auditoría sobre los mensajes enviados o recibidos para verificar el cumplimiento de las políticas establecidas para el uso del correo electrónico.
   iii. El personal del OSINFOR es responsable de cautelar que ninguna otra persona utilice su correo electrónico, que no se realice actividades ilegales y que no se utilice el acceso para fines ajenos a los de la Entidad, por lo cual se hacen responsables por todas las actividades realizadas con su cuenta.
   iv. El/La **Oficial de Seguridad y Confianza Digital** como parte de la gestión de incidentes de seguridad, es responsable de realizar las investigaciones y tomar las acciones que correspondan en coordinación con el/la responsable de la unidad de organización que pertenece el/la servidor/a involucrado/a y si amerita, solicitar la revocación del privilegio si se detecta mal uso del correo electrónico.

d) Los acuerdos de confidencialidad o no-divulgación se aplican tanto para los/las servidores/as del OSINFOR como para los/las proveedores/as, contratistas, consultores/as externos, entre otros, quienes requieren acceder a los sistemas de información y/o las áreas de procesamiento de datos. Las obligaciones de confidencialidad inician una vez firmado el acuerdo, sobreviviendo después del cese de labores y extendiéndose de acuerdo con lo estipulado en el mismo, lo que debe ser considerado por los/las servidores/as, a fin de evitar daños y perjuicios.

6.11 Seguridad para la adquisición, desarrollo y mantenimiento de los sistemas de información

Objetivo: Garantizar que la seguridad de la información sea parte integral de los sistemas de información utilizados en el OSINFOR en todo el ciclo de vida de desarrollo del software.

Lineamientos

6.11.1 Requisitos de seguridad para los sistemas de información

a) Análisis y especificación de los requisitos de seguridad de la información

i. Para todos los sistemas desarrollados por o para el OSINFOR, el/la Analista de Sistemas determina (si aplican) los requisitos de seguridad de información en la fase de análisis, con el fin de evitar o minimizar fallas de seguridad en los sistemas de información a desarrollar. El/La **Oficial de Seguridad y Confianza Digital** es quien valida si se cumplen con los requisitos de seguridad establecidos para el análisis, diseño, construcción, pruebas e implementación de los sistemas de información. El/La Jefe/a del Proyecto es responsable de gestionar los sistemas de información de acuerdo con el procedimiento de desarrollo de sistemas de información[25].

ii. Para todos los sistemas de información desarrollados por o para el OSINFOR, los requisitos mínimos de seguridad se registran en el documento Formato de Solicitud de Requerimiento[26]. Estos requisitos deben ser considerados en cada fase del ciclo de vida de desarrollo como son: análisis, diseño, construcción, pruebas e implementación. Así mismo, en el caso que ameriten, se debe de considerar adicionar otros requisitos sobre seguridad de la información.

b) Aseguramiento de los servicios de aplicación en las redes públicas

i. El/La Especialista en Administración de Redes gestiona la utilización de certificados SSL/TLS, utilizando protocolos de comunicación seguros para asegurar la autenticidad de los sistemas de información del OSINFOR a los que acceden los/las usuarios/as.

ii. Los/Las servidores/as del OSINFOR utilizan certificados digitales emitidos por una entidad de certificación, registro o verificación habilitada en el Registro Oficial de Prestadores de Servicio de Certificación de Certificación Digital (ROPS) del Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual (INDECOPI), el cual permite firmar documentos con validez legal según la ley de firmas y certificados digitales, así como su reglamento y modificatorias, dentro de la Infraestructura Oficial de Firma Electrónica (IOFE).

c) Protección de las transacciones de los servicios de aplicación

i. En la fase de construcción y pruebas de los sistemas de información, el/la Arquitecto/a de TI velará que las transacciones para los servicios de las aplicaciones se codifiquen de manera explícita en los paquetes u objetos de la base de datos del sistema de información, de tal manera que se debe precisar el inicio y culminación de la transacción para las siguientes operaciones de registro, actualización, eliminación o envío de información.

6.11.2 Seguridad en los procesos de desarrollo y soporte

a) Política de desarrollo seguro

[25] Procedimiento A5.2.3-PRO-001 establecido en el MAPRO vigente.

[26] Formato establecido en la Directiva del Sistema de Información Gerencial del OSINFOR vigente.

i. El desarrollo o mantenimiento seguro de los sistemas de información en el OSINFOR se realizará de acuerdo con el procedimiento de desarrollo de sistemas de información[27].
ii. En todo momento se deben utilizar técnicas de programación seguras tanto para los desarrollos nuevos como en las situaciones de reutilización de código, tanto para el desarrollo interno como externo.

b) Procedimiento de control de cambios del sistema
   i. Todos los cambios a desplegar en el ambiente de producción deben ser realizados por el/la Especialista en Administración de Redes y el/la Administrador de Base de Datos.
   ii. El registro de control de cambios se realizará de acuerdo a lo establecido en el Procedimiento de Gestión de Cambios de la **OTI**[28].

c) Revisión técnica de aplicaciones después de cambios en la plataforma operativa
   i. El/La Especialista en Administración de Redes, el/la Administrador/a de Base de Datos y el/la Jefe/a del Proyecto verifican y garantizan que los cambios realizados no tengan un impacto adverso en las actividades y operaciones críticas del negocio; posterior al despliegue de los cambios del sistema de información en el ambiente de producción.
   ii. En el acta de pase a producción, el/la Especialista en Administración de Redes, el/la Administrador/a de Base de Datos y/o el/la Jefe/a del Proyecto deben registrar los posibles inconvenientes u observaciones presentados durante el pase a producción.

d) Restricciones en cambios a paquetes de software
   i. El/La Arquitecto/a de TI verificará las modificaciones a los paquetes de software, los cuales deben ser limitados sólo a cambios necesarios. Todos los cambios son estrictamente controlados.
   ii. Antes de realizar cualquier modificación en los paquetes de software, se evaluará el impacto, debiendo considerar los futuros mantenimientos del software como consecuencia de los cambios y la compatibilidad con otros softwares en uso.

e) Principios de la ingeniería de sistemas seguros
   i. Para el análisis:
      - Definir requisitos de seguridad de la información acorde a la normativa aplicable y las funcionalidades requeridas.
      - Identificar posibles amenazas y establecer controles preventivos para reducir la superficie de ataques.
   ii. Para el diseño y construcción:
      - Establecer seguridad por defecto, aplicando el principio del mínimo privilegio, mediante el cual los/las usuarios/as tienen disponible la información y recursos requeridos para el desempeño de sus funciones.
      - Diseñar con alta cohesión y bajo acoplamiento.
      - Implementar seguridad en profundidad. El diseño e implementación de seguridad debe establecerse en varios niveles (aplicación, base de datos, redes, entre otros).
      - Validar los datos de entrada.
      - Implementar un correcto manejo de errores y excepciones.
      - Implementar trazabilidad, registros de log y eventos de seguridad.

[27] Procedimiento A5.2.3-PRO-001 establecido en el MAPRO vigente.
[28] Procedimiento A5.2.4-PRO-001 establecido en el MAPRO vigente.

- Limpiar el código antes que se pase a producción, para que no contenga rutinas de pruebas, comentarios o cualquier tipo de mecanismo que pueda dar lugar a accesos no autorizados.

iii. Para las pruebas e implementación:
- Realizar el control de calidad del sistema de información.
- Realizar las pruebas de seguridad del sistema y configuración.
- Gestionar las vulnerabilidades identificadas.

f) Entorno de desarrollo seguro

i. La **OTI** cuenta con ambientes de Desarrollo para las bases de datos y sistemas de información, donde el/la Especialista en Administración de Redes, el/la Arquitecto/a, el/la Analista Programador/a y el/la Administrador/a de Base de Datos tendrán acceso.

ii. La **OTI** cuenta con ambientes de Pruebas para las bases de datos y sistemas de información, donde el/la Especialista en Administración de Redes, el/la Arquitecto/a de TI, el/la Analista de Pruebas y el/la Administrador/a de Base de Datos tendrán acceso.

iii. La **OTI** cuenta con ambientes de Producción para las aplicaciones y bases de datos, donde el/la Especialista en Administración de Redes y el/la Administrador/a de Base de Datos tendrán acceso para el despliegue de las implementaciones en producción.

iv. La **OTI** cuenta con un repositorio de código fuente, donde el/la Arquitecto y el/la Analista Programador/a tendrán acceso.

g) Desarrollo subcontratado

i. El OSINFOR a través de el/la Jefe/a del Proyecto supervisa y realiza el seguimiento de las actividades de desarrollo de sistemas subcontratados, considerando:
- El acuerdo de licencias, la propiedad del código y los derechos de propiedad intelectual relacionado con el contenido de terceros.
- Los requisitos contractuales para el diseño, la construcción y las pruebas seguras.
- Las pruebas de aceptación para la calidad y precisión de los entregables.
- La presentación del resultado de pruebas por parte del subcontratista. El/La **Oficial de Seguridad y Confianza Digital** establece los niveles mínimos aceptables de seguridad y calidad en coordinación con el/la Analista de Sistemas.
- El procedimiento de desarrollo de sistemas de información vigente.

ii. En las contrataciones relacionadas al desarrollo y/o mantenimiento de los sistemas de información, los términos de referencia deberán contemplar el desarrollo seguro, así como el cumplimiento de la presente política y demás políticas y/o procedimientos que resulten aplicables al servicio.

h) Pruebas de seguridad de sistemas y pruebas de aceptación de sistemas

i. El/La **Oficial de Seguridad y Confianza Digital** validará el cumplimiento de los requisitos de seguridad establecidos en el Formato de Solicitud de Requerimiento[29] utilizando el estándar de verificación de seguridad de aplicaciones OWASP[30]. El resultado de las pruebas

[29] Formato establecido en la Directiva del Sistema de Información Gerencial del OSINFOR vigente.
[30] OWASP (Open Web Application Security Project). Metodología de seguridad de auditoría web, abierta y colaborativa, orientada al análisis de seguridad de aplicaciones Web, y usada como referente en auditorías de seguridad.

de seguridad es consignado en los formatos de pruebas de seguridad[31] según el desarrollo o mantenimiento realizado.

ii. Las pruebas de aceptación de los sistemas de información se realizarán de acuerdo al procedimiento de desarrollo de sistemas de información[32].

iii. La **OTI** implementará controles de seguridad en el desarrollo de los sistemas de información, asimismo realizará pruebas de seguridad (pentesting) de manera anual, a fin de verificar la eficacia de los controles, cuyo resultado será informado al **Oficial de Seguridad y Confianza Digital** mediante un informe técnico.

6.11.3 Datos de prueba

a) Los datos de pruebas se deben seleccionar cuidadosamente, proteger y controlar con el objetivo de garantizar la protección de los datos que se utilizan para la fase de pruebas.

b) La información personal proporcionada por los/las ciudadanos/as no deberán utilizarse para fines de prueba, salvo que estén protegidos mediante el uso de mecanismos de anonimización o disociación. De lo contrario, se deberán utilizar datos personales ficticios o sintéticos.

c) La protección de los datos de prueba contempla:

i. Solicitar la autorización de datos de prueba en el caso que se requiera migrar datos del ambiente de producción hacia el ambiente de desarrollo y/o pruebas, con la finalidad de utilizarlos en las diversas etapas de desarrollo o mantenimiento de los sistemas de información. Esta actividad se realiza a demanda, y para ello el/la Jefe/a del Proyecto deberá solicitar la autorización del administrador de la gestión los datos del activo de información y de el/la **Oficial de Seguridad y Confianza Digital** de acuerdo al Formato de Solicitud de Autorización de Uso de Datos de Prueba[33].

ii. En el caso que los datos a ser migrados a los entornos de desarrollo o prueba contengan datos personales, se debe de tener además la autorización de el/la **Oficial de Datos Personales** del OSINFOR y éstos deben pasar por un proceso de anonimización y/o disociación.

iii. En el caso que no se pueda realizar el proceso de anonimización o disociación, el/la Jefe/a de Proyecto debe de tomar todas las medidas técnicas y organizativas equivalentes para minimizar los riesgos. Cuando tales medidas equivalentes no sean factibles, deberá coordinar con el administrador de la gestión de los datos del activo de información para realizar la evaluación de riesgos y definir el plan de tratamiento, detallando los controles de mitigación respectivos, con el cual se solicita la aprobación de el/la **Oficial de Seguridad y Confianza Digital** y el/la **Oficial de Datos Personales** de OSINFOR.

6.12 Seguridad en la relación con proveedores

Objetivo: Garantizar la protección de los activos de información que son accesibles por los/las proveedores/as que presten algún servicio al OSINFOR y mantener un nivel apropiado de seguridad de la información en la entrega de servicios acordados.

Lineamientos

6.12.1 Acuerdos de confidencialidad

[31] Formatos establecidos en el Manual del Sistema Integrado de Gestión (SGSI-E2-FOR-006 para sistemas de información, SGSI-E2-FOR-007 para aplicaciones móviles y SGSI-E2-FOR-008 para servicios web).

[32] Procedimiento A5.2.3-PRO-001 establecido en el MAPRO vigente.

[33] Formato establecido en el Procedimiento A5.2.3-PRO-001 del MAPRO vigente.

a) Todo/a proveedor y/o contratista que prestará servicios al OSINFOR y requiera acceso a los activos de información y/o áreas seguras, deberá suscribir el respectivo acuerdo de confidencialidad.
b) Todas las obligaciones de confidencialidad continuarán vigentes aun cuando la contratación haya culminado por cualquier causa, en función al acuerdo de confidencialidad suscrito.

6.12.2 Activos de información

a) Los recursos que el OSINFOR pone a disposición de el/la proveedor/a y/o contratista, independientemente del tipo que sean (informáticos, datos, software, redes, sistemas de comunicación, etc.) están exclusivamente destinados para cumplir con las obligaciones y propósito para los que fueron proporcionados. El OSINFOR se reserva el derecho de implementar mecanismos de control y auditoría que verifiquen el uso apropiado de estos recursos.
b) Ningún proveedor/a y/o contratista podrá utilizar la información de OSINFOR para beneficio propio o de terceros. La información a la que tenga acceso el/la proveedor/a únicamente podrá ser utilizada para los fines específicamente indicados en la contratación. Toda información proporcionada por el OSINFOR seguirá siendo de propiedad de esta última.
c) El/La proveedor/a y/o contratista sólo podrá crear y/o almacenar información del OSINFOR de forma temporal, siempre que sea estrictamente necesario para el desarrollo del servicio. Esta información temporal no deberá quedar almacenada en ninguna computadora ni unidad de memoria externa del contratista, la misma que será destruida cuando haya dejado de ser útil para la finalidad para la que se creó y/o almacenó.
d) La distribución de la información ya sea en formato digital o papel, se realizará mediante los recursos determinados en la contratación y para la finalidad exclusiva de facilitar las funciones asociadas a dicho contrato.
e) Todo/a proveedor/a y/o contratista, cuyo servicio implique acceso a la información o sistemas de información del OSINFOR, debe conocer lo siguiente:
    i. Cada persona con acceso a la información del OSINFOR es responsable de la actividad desarrollada por su identificador de usuario/a asignado y todo lo que derive, en caso haya sido otorgado.
    ii. No deberán utilizar ningún identificador de otro usuario/a, aunque disponga de la autorización explícita del propietario.
f) Al culminar el vínculo contractual el/la proveedor/a y/o contratista, deberá devolver al OSINFOR todos los activos de información recibidos, para la ejecución de la contratación. Asimismo, ante el pedido efectuado en cualquier momento por OSINFOR, cesará inmediatamente el uso de toda información proporcionada, debiendo entregar (cualquiera sea el soporte en que se encuentre) toda la información que obre en su poder y destruir toda copia que se haya realizado.

6.12.3 Personal de proveedor/a y/o contratista

a) El/La proveedor/a y/o contratista debe verificar los antecedentes profesionales, penales y policiales del personal asignado al servicio.
b) El/La proveedor/a y/o contratista proporcionará al inicio del servicio, la relación de personas, perfiles, funciones y responsabilidades asociadas al servicio provisto, e informará puntualmente de cualquier cambio (alta, baja, sustitución o cambio de funciones o responsabilidades) que se produzca en dicha relación.
c) El/La proveedor/a y/o contratista debe garantizar al OSINFOR la posibilidad de cambio de personal asignado al servicio, cuando se verifique algún incumplimiento de los lineamientos de seguridad de la información.

d) Todo/a proveedor/a y/o contratista será responsable de transmitir y hacer cumplir estas disposiciones a su personal y terceros subcontratados para la prestación de servicios al OSINFOR. En caso de incumplimiento, el OSINFOR se reserva el derecho de solicitar al proveedor/a y/o contratista el cambio de personal; sin perjuicio de ello, el OSINFOR podrá resolver el contrato de prestación de servicios según corresponda e iniciar las acciones legales pertinentes.
e) El/La proveedor/a y/o contratista deberá garantizar que todo su personal que brinde servicios al OSINFOR, cuente con formación y capacitación apropiada para el desarrollo del servicio contratado, y de manera transversal deberá tener conocimiento de estos lineamientos de seguridad de la información del OSINFOR, de corresponder.
f) Cualquier tipo de intercambio de información que se produzca entre el OSINFOR y el/la proveedor/a y/o contratista será realizado dentro del marco establecido por el contrato de prestación de servicios, de modo que dicha información no podrá ser divulgada ni utilizada para otros fines.
g) El/La proveedor/a, contratista o su personal con acceso a sistemas y/o a información del OSINFOR, no deberán transgredir el sistema de seguridad de la información y las autorizaciones, ni capturar tráficos de red por parte de los/las usuarios/as, salvo que se esté llevando a cabo tareas de auditoría y verificación, expresamente autorizadas.
h) Todo/a proveedor/a y/o contratista para ingresar a las instalaciones con un activo de información de tipo tecnológico (computadora portátil, tableta, disco duro externo y similares) deberá declararlo al momento del ingreso.
i) Para el caso de los/las contratistas y sus colaboradores/as se deberá realizar una inducción sobre las políticas de seguridad de la información del OSINFOR, según su nivel de acceso a los activos de información críticos y muy críticos de la Entidad.

6.12.4 Obligaciones para proveedores/as y/o contratistas

a) Garantizar el cumplimiento de las restricciones legales respecto del uso del material protegido por normas de propiedad intelectual.
b) Informar de cualquier pérdida, uso no autorizado o revelación de la información proporcionada o de propiedad de OSINFOR del servicio provisto, comunicando inmediatamente por escrito y adoptar las acciones necesarias para ayudar al OSINFOR a remediarlo.
c) Contar con una garantía de continuidad del servicio, el cual garantizará al OSINFOR, la disponibilidad o restauración del servicio en el menor tiempo frente a cualquier evento o incidente que atente con los procesos del OSINFOR. Las características de dicha garantía se encontrarán establecidas en la contratación.
d) Todo/a proveedor/a y/o contratista que preste servicios dentro de las instalaciones del OSINFOR y/o cuente con acceso a la información del OSINFOR, deberá respetar los lineamientos de seguridad establecidos en este documento, con el fin de reducir los riesgos de acceso no autorizado, pérdida y daño de la información, durante el horario normal de trabajo del OSINFOR y fuera del mismo.
e) Todo/a proveedor/a y/o contratista en caso requiera hacer cambios en la gestión del servicio y que afecte a los activos de información, deberá solicitar autorización al OSINFOR para su evaluación.

6.12.5 Prohibiciones para proveedores/as y/o contratistas

a) El uso de recursos proporcionados por el OSINFOR para actividades no relacionadas con el propósito de servicio.
b) La conexión a la red del OSINFOR de equipos que no estén bajo supervisión y/o autorización del OSINFOR.

c) Introducir en los sistemas de información o la red del OSINFOR, contenidos que contravienen con la moral, ética y buenas costumbres observadas en la Ley N° 27815, Ley del Código de Ética de la Función Pública, según corresponda.
d) Introducir, instalar y/o descargar por dolo o culpa inexcusable en la red del OSINFOR, cualquier tipo de software malicioso (malware), dispositivos lógicos, dispositivos físicos, o cualquier tipo de secuencia de órdenes que causen o sean susceptibles de causar cualquier tipo de alteración o daño en los recursos informáticos del OSINFOR.
e) Intentar obtener sin autorización explícita otros derechos o accesos distintos a los que el OSINFOR le haya asignado.
f) Intentar acceder, sin autorización explícita, a áreas restringidas del OSINFOR.
g) Intentar distorsionar o falsear los registros "log" de los sistemas de información del OSINFOR.
h) Poseer, desarrollar o ejecutar programas que pudieran dañar o alterar los recursos informáticos del OSINFOR, o intentar saltar las Políticas de Seguridad de la Información.
i) El uso, reproducción, cesión, transformación o comunicación pública de cualquier tipo de obra o invención protegida por derechos de propiedad intelectual del OSINFOR sin la debida autorización.
j) El/La proveedor/a y/o contratista no deberá realizar pruebas para detectar y/o utilizar alguna debilidad de seguridad de la información sin autorización explícita del OSINFOR.

6.12.6 Auditorías a proveedores y/o contratistas

a) Todo/a proveedor/a deberá permitir que el OSINFOR lleve a cabo una auditoría de seguridad del servicio en caso amerite, colaborando con el equipo auditor y facilitando todas las evidencias y registros que le sean requeridos.
b) El alcance y profundidad de la auditoría será establecido expresamente por el OSINFOR en cada caso.
c) El OSINFOR se reserva el derecho de realizar auditorías extraordinarias adicionales, siempre que se den las causas específicas que lo justifiquen.

6.13 Gestión de debilidades, eventos y/o incidentes de seguridad de la información

Objetivo: Asegurar la gestión de incidentes de seguridad de la información incluyendo la comunicación sobre eventos de seguridad y debilidades, que permitan prevenir y limitar el impacto de los mismos.

Lineamientos

6.13.1 Reporte de debilidades y eventos de seguridad de la información

a) Todo/a servidor/a, proveedor/a, contratista y/o consultor/a externo/a que preste algún servicio al OSINFOR tiene el deber de comunicar las debilidades, eventos o incidentes de seguridad de la información a la Mesa de Ayuda mediante los canales establecidos. Asimismo, cualquier visitante está en la facultad de poder comunicar eventos y debilidades de seguridad de la información.
b) La comunicación de los eventos, incidentes y/o debilidades de seguridad de la información es a través del correo electrónico mesadeayuda@osinfor.gob.pe o del sistema de Mesa de Ayuda. En el caso de visitantes, la comunicación se realizará a través del área usuaria con la cual se está coordinando la atención, salvo que el/la visitante tenga comunicación directa con el/la **Oficial de Seguridad y Confianza Digital** (teléfono, correo electrónico y/o verbal), en cuyo caso éste/a será quien realizará el registro en el sistema Mesa de Ayuda del OSINFOR.

6.13.2 Gestión de incidentes y mejoras de seguridad de la información

a) Todo evento, debilidad y/o incidente de seguridad de la información es registrado, clasificado, evaluado y atendido de acuerdo con el "Procedimiento de Gestión de Incidentes de Seguridad de la Información".
b) El seguimiento al tratamiento de las debilidades de seguridad de la información identificadas y/o reportadas se realiza a través del registro y control de acciones correctivas y de mejora según el Procedimiento establecido[34].

6.13.3 Recolección de evidencia

a) El/La **Oficial de Seguridad y Confianza Digital**, apoyará a las unidades de organización para la identificación, recolección y conservación de información (logs, capturas de pantalla, imágenes, videos, entre otros), que puede servir como evidencia para propósitos de acción disciplinaria o judicial según corresponda.
b) Las evidencias de los incidentes de seguridad de la información serán conservadas en un repositorio de información accesible para el equipo de respuesta ante incidentes de seguridad digital.

6.14 Privacidad y protección de datos personales

Objetivo: Garantizar el cumplimiento de la Ley de Protección de Datos Personales y su Reglamento, así como los requisitos del Sistema de Gestión de Seguridad de la Información en el OSINFOR, informando a los/las usuarios/as sobre la utilización y tratamiento de la información personal que entreguen y/o suministren de manera voluntaria a través de las distintas plataformas del OSINFOR.

Lineamientos:

6.14.1 Finalidad del tratamiento de datos personales

a) Los datos personales de el/la usuario/a se recopilan para una finalidad determinada, explícita y lícita, salvo que se trate de una finalidad expresamente permitida o exigida por la normativa vigente aplicable. Asimismo, se excluye los casos de actividades históricas, estadísticas o científicas, debiendo tener en cuenta lo regulado en la normativa sobre la materia.
b) El OSINFOR tiene las siguientes finalidades, para el tratamiento de datos personales:
    i. Gestión de la información de los datos personales del personal para fines del cumplimiento de la relación contractual, beneficios sociales, comunicaciones, entre otros.
    ii. Gestión de la información de los/las postulantes a las convocatorias de trabajo ofrecidas por la Entidad, para fines de control administrativo y transparencia.
    iii. Gestión de información de terceros, proveedores/as y/o contratistas de la Entidad, para fines de control administrativo, y cumplimiento de la relación contractual de los servicios prestados.
    iv. Gestión de la información de controles de acceso físico y videovigilancia, para fines de seguridad de los bienes e instalaciones de la Entidad.
    v. Gestión de solicitudes de los/las usuarios/as vía Mesa de Partes, para su atención y respuesta.
    vi. Gestión de información de los asistentes a las capacitaciones y eventos, para fines de control administrativo y comunicaciones.

[34] Procedimiento E2.4.5-PRO-002 del Manual de Procedimientos del OSINFOR vigente.

vii. Remitir a los/las administrados/as información relacionada a los servicios del OSINFOR y/o disposiciones de obligatorio conocimiento y cumplimiento, de conformidad con la norma de creación de la Entidad.

6.14.2 Tratamiento y seguridad de los datos personales

a) Todo tratamiento de datos personales será adecuado, relevante y no excesivo respecto de la finalidad para la cual fueron recopilados.
b) Los datos personales que vayan a ser tratados deben ser veraces, exactos, necesarios, pertinentes y adecuados respecto de la finalidad para la cual fueron recopilados. Se conservarán de forma tal que se garantice su seguridad.
c) El OSINFOR implementará las medidas de seguridad apropiadas, acorde con el tratamiento que se vaya a efectuar y con la categoría de datos personales que se trate.
d) El OSINFOR se compromete a no divulgar o compartir los datos personales de el/la usuario/a, sin que haya prestado el debido consentimiento para ello, con excepción de los siguientes casos:
    i. Solicitudes de información de autoridades públicas en ejercicio de sus funciones y en el ámbito de sus competencias.
    ii. Solicitudes de información en virtud de órdenes judiciales.
    iii. Solicitudes de información en virtud de disposiciones legales.
e) Los encargados/as de tratamiento de datos personales, adoptan las medidas técnicas, organizativas y legales necesarias para garantizar la seguridad de los datos personales, debiendo vigilar que estén almacenados en repositorios físicos o digitales que reúnan las condiciones de seguridad exigidas por las normativas aplicables.
f) Los/Las proveedores/as y terceros que presten servicios al OSINFOR, deberán cumplir con la Ley N° 29733 “Ley de protección de datos personales” y su Reglamento, así como también las disposiciones que el OSINFOR regule respecto a la materia.
g) En caso se gestione o maneje el flujo transfronterizo de datos personales, el OSINFOR aplicará un nivel adecuado de protección de acuerdo con la Ley N° 29733 “Ley de protección de datos personales” y su Reglamento, asegurando que dicha información solo sea compartida a través de intermediarios con el mismo nivel de seguridad establecido.
h) El OSINFOR requiere del consentimiento libre, previo, expreso, inequívoco e informado de el/la usuario/a para el tratamiento de sus datos, salvo en los casos de excepción expresamente establecidos por Ley.
i) El OSINFOR no requiere consentimiento para tratar datos personales obtenidos de fuentes accesibles al público, gratuitas o no; así mismo, podrá tratar datos personales de fuentes no públicas, siempre que dichas fuentes cuenten con el consentimiento para tratar y transferir dichos datos personales, previa verificación.
j) En el caso de los servicios digitales del OSINFOR que utilicen las plataformas digitales de la Presidencia del Consejo de Ministros, los datos serán almacenados en los servidores de Amazon Web Services, realizándose un flujo transfronterizo a los Estados Unidos de América de dichos datos personales. En ese sentido, el OSINFOR garantiza que el tratamiento de los datos se limite a las finalidades descritas en el numeral 6.13.1 y que se mantengan de forma confidencial, implementando las medidas de seguridad que exige la normativa aplicable.
k) Los datos personales que puedan ser suministrados a través del sitio web u otro medio de recopilación del OSINFOR, serán incorporados a los bancos de datos bajo la titularidad del OSINFOR, excluyendo los portales y servicios brindados por otras entidades. Es de responsabilidad de el/la usuario/a revisar las políticas de privacidad en dichas páginas web para verificar el

nivel de protección de sus datos personales siendo ajena a la responsabilidad de OSINFOR.

6.14.3 Ejercicio de derechos del titular de datos personales

a) Los datos personales que conforman los bancos de datos del OSINFOR, se conservan mientras no se solicite su cancelación por parte de el/la usuario/a, acorde a las normativas legales aplicables a la Entidad.
b) El/La usuario/a o su causahabiente puede ejercer los derechos de información, acceso, rectificación, cancelación, oposición, y demás derechos consagrados en la Ley de protección de datos personales y su Reglamento a través de la Mesa de Partes Digital de la Entidad, utilizando el Formato de Solicitud de Ejercicio de Derechos ARCO (E2.4.5-PRO-008-FOR-001), o presentándolo físicamente en la Mesa de Partes de la sede central u oficinas desconcentradas. En caso de que la Solicitud de Ejercicio de Derechos ARCO no cumpla con los requisitos, se requerirá al solicitante para que subsane dentro del plazo que la Ley establece, acorde al Procedimiento Atención de Derechos de Acceso, Rectificación, Cancelación y Oposición (E2.4.5-PRO-008).
c) Sin perjuicio de lo anterior, el OSINFOR podrá conservar información de el/la usuario/a que solicita la cancelación de sus datos personales, a fin de que sirva de prueba ante un eventual reclamo, por responsabilidades derivadas del tratamiento de dicha información. La duración de dicha conservación no podrá ser superior al plazo de prescripción legal de dichas responsabilidades.
d) Por ello los datos personales serán conservados mientras esté vigente una relación contractual para la prestación de servicios entre el OSINFOR y los/las usuarios/as y/o mientras no se solicite la eliminación de los mismos; sin embargo, algunos datos de carácter personal deberán ser conservados por el OSINFOR por normatividad legal y según plazos establecidos en la legislación.

6.14.4 Manejo de cookies

a) Los sitios web del OSINFOR podrán utilizar cookies para recordar las preferencias de los/las usuarios/as, mejorar la funcionalidad de búsqueda de información y supervisar el rendimiento del sitio web. Asimismo, se utilizará Google Analytics (servicio de analítica web desarrollada por Google para medición y análisis de la navegación en las páginas web). La información que se procesa es anónima, mostrando particularmente qué accesos se visita o cuánto tiempo se pasa en cada enlace sin conocer la identidad. Los/Las usuarios/as, en su navegador podrán observar cookies de este servicio.
b) Los/Las usuarios/as podrán restringir, bloquear o borrar las cookies de los sitios web del OSINFOR, configurando las opciones de su navegador de internet.

6.14.5 Vigencia y modificación

a) El OSINFOR se reserva el derecho a modificar esta política en el supuesto de que exista un cambio en la legislación vigente, pudiendo realizar modificaciones y correcciones en el mismo.
b) Si se introdujera algún cambio, el nuevo texto se publicará en las plataformas digitales del OSINFOR, debiendo el/la usuario/a verificar regularmente este documento para consultar los cambios realizados.

6.15 Trabajo remoto

Objetivo: Garantizar que la ejecución de trabajo remoto sea realizada de manera segura, en los contextos especiales asociados a los/las servidores/as que tengan la obligación o necesidad de cumplir con sus funciones y actividades a distancia, cumpliendo los requisitos reglamentarios del Sistema de Gestión de Seguridad de la Información en el OSINFOR.

Lineamientos:

6.15.1 Consideraciones generales

a) El trabajo remoto utiliza tecnologías de la información y comunicaciones para permitir que los/las servidores/as trabajen en forma remota desde un lugar externo a la Entidad.
b) El OSINFOR a través de la **OTI** y la **UFCI** brinda instrucciones a todos los/las servidores/as para que se cumplan los lineamientos de seguridad de la información establecidos en la entidad en los ambientes donde se desarrolla el trabajo remoto.
c) Los/Las propietarios/as de los activos de información deberán identificar, analizar, valorar los riesgos de seguridad de la información, asociados al desarrollo del trabajo remoto, así como realizar el tratamiento correspondiente.
d) Los/Las servidores/as deben aplicar permanentemente los lineamientos de seguridad de la información, independientemente del lugar y del equipo que utilicen para el desarrollo de sus actividades.

6.15.2 Instrucciones que deben cumplir los/las servidores/as

a) Respecto al ambiente de trabajo:
   i. Asegurarse que el lugar en donde se realizará el trabajo remoto sea un ambiente controlado, en donde se reduzca la probabilidad de accesos no autorizados a la información o recursos institucionales por parte de otras personas.
   ii. Tomar previsiones para que el lugar tenga acceso a la red de internet a través de una conexión inalámbrica (Wi-Fi) o cableada para realizar sus labores, para evitar problemas de señal que puedan impactar durante el trabajo.

b) Respecto a la conectividad:
   i. Verificar regularmente la seguridad de la red doméstica, es decir, revisar que el acceso a la red inalámbrica tenga clave de acceso.
   ii. No conectarse a la red institucional haciendo uso de conexiones a internet inseguras (Wi-Fi de sitios públicos, redes desconocidas, redes sin contraseña, entre otros).
   iii. Utilizar una conexión remota segura a la red institucional, mediante red privada virtual (VPN) para acceder a los sistemas y servicios de tecnología de la información del OSINFOR que no están publicados en Internet.

c) Respecto a los equipos utilizados para el trabajo remoto:
   i. Verificar que los equipos (personales o institucionales) tengan instalado y actualizado un sistema de protección antivirus.
   ii. Verificar que los equipos personales cuenten con las últimas actualizaciones del sistema operativo y aplicaciones instaladas.
   iii. Si se utiliza un equipo personal compartido en el hogar, el/la servidor/a deberá crear un perfil nuevo específico protegido con contraseña, para evitar el acceso de forma fortuita a información institucional por otros/as usuarios/as de dicho equipo.

iv. Verificar que los equipos cuenten (personales o institucionales) con bloqueo automático por inactividad y con contraseña.
v. Realizar la devolución de los equipos institucionales que hayan sido facilitados por la Entidad, cuando concluyan las actividades de trabajo remoto. La Unidad de Abastecimiento realizará el respectivo control del traslado y devolución de los equipos.

d) Respecto al uso de herramientas:
   i. Utilizar las herramientas de comunicación o de videoconferencia aprobadas por la **OTI**, tales como: Skype / Google Meet / Microsoft Teams / Zoom licenciado. Si se necesita utilizar otra herramienta de comunicaciones, deberá ser aprobada por la **OTI**.
   ii. Evitar instalar software de la Entidad en equipos personales, el cual está destinado a ser instalado en equipos institucionales.

e) Respecto al uso de servicios nube:
   i. Establecer contraseñas seguras para su acceso.
   ii. Utilizar a discreción estos servicios y solo para los casos donde se maneje información pública o de carácter no confidencial.
   iii. No almacenar información confidencial, datos personales propios y de terceros en la nube personal.
   iv. No dejar información institucional almacenada en la nube personal de forma permanente. Una vez terminado el trabajo en los repositorios de la nube, eliminar toda información institucional almacenada, previo almacenamiento de los documentos finales en las carpetas compartidas del OSINFOR.
   v. El manejo de información institucional en la nube es responsabilidad de cada servidor/a de OSINFOR, quien asume las respectivas consecuencias en caso de pérdida y/o accesos no autorizados.

f) Respecto al resguardo de la información:
   i. Garantizar la protección de la información física y digital contra su pérdida y todo acceso, utilización, modificación o comunicación no autorizada.
   ii. Guardar la información institucional en los aplicativos, sistemas y unidades de almacenamiento proporcionado por la Entidad, para asegurar el respaldo permanente de la información correspondiente.
   iii. Verificar periódicamente la información almacenada en las carpetas de trabajo gestionadas por la Entidad para validar su integridad.

6.15.3 Medidas a cargo de la **OTI** para el soporte del trabajo remoto

a) Verificar que los equipos de trabajo remoto tienen instalado y correctamente configurado el software VPN y controlar las conexiones VPN.
b) Poner a disposición de los/las servidores/as las aplicaciones, herramientas, guías técnicas del OSINFOR para el trabajo remoto dentro de la Intranet.
c) Restringir el uso de soluciones de administración remota gestionadas por terceros que sean inseguras y/o que permitan evadir la arquitectura de seguridad implantada.
d) Realizar la anulación de las autorizaciones y derechos de acceso cuando finalicen las actividades remotas.
e) Concientizar a los/as servidores/as en el uso y seguridad de los servicios de tecnología de la información.