Firmado digitalmente por:
CORDOVA CHACON Denis Omar
FAU 20522224783 soft
Motivo: Doy V° B°
Fecha: 07/12/2020 17:43:[illegible]

DIRECTIVA PARA EL USO DE RECURSOS Y SERVICIOS INFORMÁTICOS DEL ORGANISMO DE SUPERVISIÓN DE LOS RECURSOS FORESTALES Y DE FAUNA SILVESTRE - OSINFOR

Firmado digitalmente por:
ARTICA CUYUBAMBA Gustavo
FAU 20522224783 soft
Motivo: Doy V° B°
Fecha: 07/12/2020 18:26:31-0500

DOCUMENTO CONTROLADO

Propuesto por:	Gestión de Tecnologías de la Información	Fecha de propuesta:	07 de diciembre de 2020
Aprobado por:	Gerencia General	Fecha de aprobación:	07 de diciembre de 2020

ÍNDICE

INTRODUCCIÓN

El Organismo de Supervisión de los Recursos Forestales y de Fauna Silvestre, en adelante el OSINFOR, es un Organismo Público Ejecutor adscrito a la Presidencia del Consejo de Ministros; encargado a nivel nacional, de supervisar y fiscalizar el aprovechamiento sostenible y la conservación de los recursos forestales y de fauna silvestre, y de los servicios de los ecosistemas forestales y otros ecosistemas de vegetación silvestre, otorgados por el Estado a través de títulos habilitantes regulados en el marco de la Ley Forestal y de Fauna Silvestre; de esta manera contribuye a la promoción del comercio legal de los productos madereros, a la mejora del valor económico de los recursos forestales y de fauna silvestre y, por ende a su manejo sostenible.

El OSINFOR ha implementado el Sistema Integrado de Gestión, que está conformado por el Sistema de Gestión de Calidad ISO 9001:2015 y el Sistema de Gestión de Seguridad de la Información NTP/ISO/IEC 27001:2014, en el marco de la mejora del proceso E2. “Gestión de Documentos de Gestión y de Procesos”, así como el cumplimiento Resolución Ministerial N° 004-2016-PCM, que dispone el uso obligatorio de la Norma Técnica Peruana “NTP ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 2a. Edición”, en todas las entidades integrantes del Sistema Nacional de Informática.

El Sistema Integrado de Gestión tiene entre sus objetivos: reducir los riesgos de seguridad de la información, mejorar los procesos de la entidad y cumplir con los requisitos legales y requisitos de los servicios.

La Directiva para el Uso de Recursos y Servicios Informáticos del OSINFOR, se ha formulado en cumplimiento del marco normativo y sobre la base del Sistema de Gestión de Seguridad de la Información, y tiene por objetivo establecer disposiciones para el uso adecuado de los recursos y servicios informáticos del OSINFOR, que permitan reducir los riesgos de seguridad de la información.

DIRECTIVA PARA EL USO DE RECURSOS Y SERVICIOS INFORMÁTICOS DEL ORGANISMO DE SUPERVISIÓN DE LOS RECURSOS FORESTALES Y DE FAUNA SILVESTRE – OSINFOR

I. DISPOSICIONES GENERALES

1.1 Objetivo

Establecer disposiciones para el uso y acceso adecuado a los recursos y servicios informáticos del Organismo de Supervisión de los Recursos Forestales y de Fauna Silvestre - OSINFOR.

1.2 Finalidad

Garantizar la seguridad, integridad y disponibilidad de la información institucional que está almacenada en los equipos y sistemas informáticos, destinados al cumplimiento de las funciones de los/as usuarios/as.

1.3 Base Legal

1.3.1 Decreto Legislativo N° 1412, que aprueba la Ley de Gobierno Digital.
1.3.2 Ley N° 28716, Ley de Control Interno de las entidades del Estado.
1.3.3 Ley N° 29733, Ley de Protección de Datos Personales.
1.3.4 Ley N° 30096, Ley de Delitos Informáticos.
1.3.5 Decreto Supremo N° 009-2009-MINAM, que establece las medidas de Ecoeficiencia para el Sector Público.
1.3.6 Decreto Supremo N° 066-2011-PCM, que aprueba el Plan de Desarrollo de la Sociedad de la Información en el Perú - La Agenda Digital Peruana 2.0.
1.3.7 Decreto Supremo N° 029-2017-PCM, que aprueba el Reglamento de Organización y Funciones del Organismo de Supervisión de los Recursos Forestales y de Fauna Silvestre.
1.3.8 Decreto Supremo N° 033-2018-PCM, que crea la Plataforma Digital Única del Estado Peruano y establece disposiciones adicionales para el desarrollo del Gobierno Digital.
1.3.9 Decreto Supremo N° 118-2018-PCM, que declara de interés nacional el desarrollo del Gobierno Digital, la innovación y la economía digital con enfoque territorial.
1.3.10 Resolución Ministerial N° 004-2016-PCM, que aprueba el uso obligatorio de la Norma Técnica Peruana "NTP ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 2a. Edición", en todas las entidades integrantes del Sistema Nacional de Informática.
1.3.11 Resolución Presidencial N° 125-2016-OSINFOR, que aprueba el Reglamento Interno de los Servidores Civiles del Organismo de Supervisión de los Recursos Forestales y de Fauna Silvestre - OSINFOR.
1.3.12 Resolución Presidencial N° 127-2017-OSINFOR, que aprueba el Manual de Procesos y Procedimientos Estratégicos y de Apoyo del Organismo de Supervisión de los Recursos Forestales y de Fauna Silvestre - OSINFOR.
1.3.13 Resolución de Jefatura N° 042-2018-OSINFOR, que aprueba la Directiva de Control de Documentos del Organismo de Supervisión de los Recursos Forestales y de Fauna Silvestre - OSINFOR.
1.3.14 Resolución de Jefatura N° 036-2018-OSINFOR, que aprueba dieciséis (16) políticas para la seguridad de la información del OSINFOR.
1.3.15 Resolución de Jefatura N° 058-2018-OSINFOR, que aprueba la Directiva M5-DIR-008-V.01 *"Directiva del Sistema de Información Gerencial del Organismo de Supervisión de los Recursos Forestales y de Fauna Silvestre - SIGO"*

Las referidas normas incluyen sus respectivas modificaciones, normas conexas o que las sustituyan, de ser el caso.

1.4 Alcance

La presente Directiva es de carácter general y de aplicación obligatoria para todos los/las usuarios/as que utilizan los recursos y servicios informáticos del OSINFOR.

1.5 Definiciones

1.5.1 **Ataque de diccionario:** Es una técnica de violación de contraseñas en la cual se prueban consecutivamente palabras del diccionario para validar una clave o contraseña.

1.5.2 **Cuenta de usuario/a:** Es la credencial de un/a usuario/a y permite el acceso a los sistemas o servicios. Una cuenta se identifica por un nombre de usuario/a (comúnmente conocido como login) y una contraseña.

1.5.3 **Digitalización:** Es la capacidad de usar datos y tecnologías digitales, con miras a generar, procesar y compartir información que permita establecer nuevas actividades o cambios en las ya existentes.

1.5.4 **Directorio Activo:** Es el servicio de directorio propietario de Microsoft para su uso en redes de dominio de Windows. Cuenta con funciones de autenticación y autorización y proporciona una plataforma para otros servicios informáticos.

1.5.5 **Dispositivos de Almacenamiento**: Los dispositivos de almacenamiento son elementos técnicos destinados a proveer de espacio físico para albergar información, y están clasificados según capacidad y velocidad de transferencia.

1.5.6 **Equipo Informático:** Un equipo informático está formado por distintos dispositivos electrónicos que permiten la ejecución de programas informáticos. A los equipos informáticos también se les denomina computadoras.

1.5.7 **Esquema Ponzi:** Es una operación de inversión fraudulenta en la que el operador paga a sus inversionistas el dinero nuevo que pagan los nuevos aportantes, en lugar del beneficio obtenido a través de fuentes legítimas.

1.5.8 **Grupo de seguridad:** Se refiere a un grupo de usuarios/as con privilegios especiales para configurar y monitorear un recurso informático.

1.5.9 **Permiso de usuario/a:** Son controles de acceso que se aplican a objetos protegibles, como el sistema de archivos, bases de datos, aplicaciones y objetos del Directorio Activo.

1.5.10 **Recursos informáticos:** Son todos aquellos componentes de hardware y software, que son necesarios para el buen funcionamiento y la optimización del trabajo con computadoras y periféricos, tanto a nivel individual, colectivo u organizativo, por ejemplo: software ofimático, correo electrónico, carpetas compartidas, etc.

1.5.11 **Servicios informáticos:** Es el conjunto de servicios basados en tecnologías de la información, que se brinda a los/las usuarios/as, para facilitar su trabajo diario. Dichos servicios contemplan el acceso a redes, internet, correo electrónico, telefonía, sistemas de información y aplicaciones, herramientas colaborativas, entre otros.

1.5.12 **USB (Universal Serial Bus):** Es un medio compartido de comunicaciones que sigue un estándar que define los cables, conectores y protocolos usados para conectar, comunicar y proveer alimentación eléctrica entre computadoras, periféricos y dispositivos electrónicos.

1.5.13 **UPS (Uninterrumplible Power Supply):** Es una fuente de suministro eléctrico, que posee una batería para brindar energía constante a un dispositivo, en el caso de interrupción eléctrica.

1.5.14 **Usuario/a:** Existe 03 tipos de usuario/a: (i) Tipo A: Es aquella persona que tiene un régimen laboral con la Entidad (servidor civil), (ii) Tipo B: Es aquella persona que mantiene una relación contractual con la Entidad (practicantes, locadores/as, consultores/as, terceros u otros); y, (iii) Tipo C: Es aquella persona a la que se le brinda acceso a los sistemas de información que administra la Entidad (SIGO$_{SFC}$, SIADO Región, SISFOR u otros según corresponda) y no tiene un régimen laboral o relación contractual con el OSINFOR (actores forestales y de fauna silvestre, socios estratégicos u otros).

Si en la presente Directiva no se especifica el Tipo de usuario/a, se entiende que aplica para todos los usuarios.

1.6 Acrónimos

1.6.1 **OSINFOR:** Organismo de Supervisión de los Recursos Forestales y de Fauna Silvestre
1.6.2 **OTI:** Oficina de Tecnología de la Información
1.6.3 **PCM:** Presidencia del Consejo de Ministros
1.6.4 **SEGDI:** Secretaría de Gobierno Digital
1.6.5 **SGSI:** Sistema de Gestión de Seguridad de la Información
1.6.6 **GIS:** Sistema de Información Geográfica (por sus siglas en inglés)
1.6.7 **SIGO:** Sistema de Información Gerencial del OSINFOR
1.6.8 **URH:** Unidad de Recursos Humanos

II. DISPOSICIONES ESPECÍFICAS

2.1 Lineamientos para la creación de cuentas de usuario/a y contraseñas

2.1.1 Solicitud de creación o alta de cuenta de usuario/a

a) La cuenta de usuario/a de Tipo A es solicitada por la URH y/o el/la Director/a o Jefe/a del Órgano o Unidad Orgánica que corresponda, mediante el Formato Control de accesos a aplicaciones y servicios TI (A5-FOR-117-V.01) o en el Formato control de accesos a aplicaciones y servicios por grupo de usuarios/as (A5-FOR-140-V.01), según sea necesario.

b) La cuenta de usuario/a de Tipo B es solicitada por la UA y/o el/la Director/a o Jefe/a del Órgano o Unidad Orgánica que corresponda, mediante el Formato Control de accesos a aplicaciones y servicios TI (A5-FOR-117-V.01) o en el Formato control de accesos a aplicaciones y servicios por grupo de usuarios/as (A5-FOR-140-V.01), según sea necesario.

c) La cuenta de usuario/a de Tipo C es solicitada por el Órgano o Unidad Orgánica que corresponda, mediante el Formato Control de accesos a aplicaciones y servicios TI (A5-FOR-117-V.01) o en el Formato Control de accesos a aplicaciones y servicios por grupo de usuarios/as (A5-FOR-140-V.01), según sea necesario. Asimismo, estos usuarios suscribirán el Formato Carta de compromiso del buen uso del sistema de información (A5-FOR-142-V.01).

2.1.2 Cuenta de usuario/a

a) Para la cuenta de usuario/a de Tipo A, se utilizará la inicial del nombre, seguido por el apellido paterno. En el caso de que exista homonimia parcial se agregará la inicial del apellido materno.

b) Para la cuenta de usuario/a de Tipo B, se empleará el tipo de relación contractual, seguido de la abreviatura del Órgano o Unidad Orgánica donde desarrollará el servicio y un correlativo numérico de la siguiente forma: LocadorUA1, PracticanteOTI1, ConsultorOTI1.

c) Para la cuenta de usuario/a de Tipo C, en caso pertenezca a una institución pública del Estado, se usará el mismo formato de Tipo A y alternativamente se puede usar caracteres especiales (tales como: punto o guion bajo) o numeración correlativa, según corresponda a cada sistema de información; en caso sea una persona natural o jurídica se podrá usar el nombre o denominación de la organización, número de DNI o RUC según corresponda.

d) En casos excepcionales la cuenta de usuario/a de Tipo A y C podrá ser modificada a solicitud de la URH o del Órgano o Unidad Orgánica, según corresponda, siempre y cuando la cuenta del/de la usuario/a, represente un término ofensivo o discriminatorio. Para tal caso la nueva cuenta debe mantener relación directa con el nombre y apellido del/de la usuario/a.

2.1.3 Construcción de contraseña segura

a) Las contraseñas deben contener al menos 8 caracteres y deben cumplir los siguientes requisitos mínimos de complejidad:

i. Incluir caracteres de al menos tres de las siguientes categorías:
   - Mayúsculas (de la **A** a la **Z**)
   - Minúsculas (de la **a** a la **z**)
   - Dígitos de base 10 (del **0** al **9**)
   - Caracteres no alfanuméricos (por ejemplo: *, !, $, #, %)

ii. No debe contener el nombre de cuenta del/de la usuario/a o partes del nombre completo del/de la usuario/a en más de dos caracteres consecutivos.

b) El/La usuario/a de la cuenta, debe evitar el uso de contraseñas débiles, las cuales suelen tener las siguientes características:

i. Contienen información personal como fechas de nacimiento, direcciones, números telefónicos o nombres de parientes, mascotas, amigos y personajes de fantasía.
ii. Contienen información relacionada con el trabajo como nombres de edificio, comandos de sistemas, sitios, compañías, hardware o software.
iii. Contienen patrones como aaaabbb, qwerty, zyxwvuts, o 123321.
iv. Contienen palabras comunes deletreadas hacia atrás, o precedidas o seguidas por un número (por ejemplo, **oterces**, **secreto1** o **1secreto**).

2.1.4 Se recomienda utilizar frases en lugar de palabras individuales en la construcción de contraseñas. Las contraseñas formuladas en base a frases, brindan mayor seguridad contra ataques de diccionario; para tal efecto, deben seguir las mismas pautas generales de construcción de contraseñas e incluir letras mayúsculas, minúsculas, números y caracteres no alfanuméricos (por ejemplo: **ElTraficoEnJavierPradoEstuvoHorribleALa1DeLaTarde!**).

Para la protección de la contraseña, se debe tener en cuenta lo siguiente:

a) Todas las contraseñas de cuentas de usuario/a (por ejemplo, correo electrónico, sistemas de información o aplicaciones, computadora de escritorio, entre otros) deben ser cambiadas al menos cada TRES meses.

b) Las contraseñas no deben ser insertadas en mensajes de correo electrónico o cualquier otra forma de comunicación electrónica. Tampoco deben ser reveladas telefónicamente a nadie.

c) La OTI podrá generar y utilizar contraseñas iniciales al momento de crear cuentas nuevas o mientras se realice la configuración inicial de un equipo, pero estas contraseñas deberán ser modificadas inmediatamente por el/la usuario/a. Cualquier modificación futura también deberá ser realizada por el/la mismo/a usuario/a. En caso excepcional, por razones de soporte técnico realizado por la OTI y, de ser estrictamente necesario, el/la usuario/a podrá brindarle su contraseña al responsable de soporte técnico de la OTI; sin embargo, una vez concluido el soporte técnico, el/la usuario/a deberá modificar la contraseña.

d) En el caso de los sistemas de información o aplicaciones que cuenten con la funcionalidad de expiración automática de contraseñas tras un periodo de vigencia, el/la usuario/a de Tipo A deberá comunicarse con la OTI para el desbloqueo de la cuenta; en caso de los/as usuarios/as de Tipo B, el/la Director/a o Jefe/a del Órgano o Unidad Orgánica, en donde haya brindado el servicio, es quien deberá solicitar a la OTI el desbloqueo respectivo; y, en caso de los/as usuarios/as de Tipo C, el Órgano o Unidad Orgánica deberá solicitar a la OTI dicho desbloqueo.

2.2 Uso adecuado de recursos y servicios informáticos

Lo regulado a continuación debe ser aplicado por los/as usuarios/as de Tipo A y B:

2.2.1 Criterios de uso

a) Los recursos y servicios informáticos del OSINFOR deben ser utilizados exclusivamente para el cumplimiento de las labores institucionales y las actividades compatibles con la naturaleza de la función del/de la usuario/a.

b) Los/Las usuarios/as deben utilizar los recursos y servicios informáticos del OSINFOR de manera responsable y ética, cuidando la integridad de los equipos e instalaciones, y respetando las disposiciones establecidas por la legislación vigente.

c) La información institucional es de propiedad del OSINFOR, así esté almacenada en dispositivos electrónicos o informáticos pertenecientes al usuario/a o arrendados por el OSINFOR.

d) El OSINFOR se reserva el derecho a auditar el acceso y uso de los recursos y servicios informáticos en cualquier momento para asegurar el cumplimiento de esta Directiva.

2.2.2 Uso de las cuentas de usuario/a

a) Desde el momento que el/la usuario/a tiene pleno conocimiento de su cuenta de usuario y contraseña para acceder a los recursos y servicios informáticos del OSINFOR, es el/la único/a responsable de todas las operaciones que se realicen con las mismas.

b) Las contraseñas de los recursos y servicios informáticos institucionales son de uso y responsabilidad personal; por lo tanto, no deben ser compartidas con nadie. Todas las contraseñas deben ser tratadas como información sensible y confidencial.

c) Para evitar inconvenientes se recomienda al/a la usuario/a, tomar las siguientes precauciones:

i. Evitar utilizar la misma contraseña de sus cuentas personales (cuentas de Internet, correo web, etc.) en las cuentas del OSINFOR.
ii. No revelar contraseñas en cuestionarios o formularios.
iii. No brindar indicios del formato de una contraseña.
iv. No escribir las contraseñas ni almacenarlas en cualquier parte de la oficina, archivos, sistemas informáticos o dispositivo móvil (teléfono, tableta, entre otros) sin encriptación.
v. No utilizar la característica "Recordar contraseña" de las aplicaciones (por ejemplo, navegadores web).

d) Cualquier usuario/a que sospeche que su contraseña pueda haber sido comprometida, debe reportar el incidente de inmediato a la Mesa de Ayuda de la OTI y cambiar todas sus contraseñas.

e) En el caso de que un/una usuario/a olvide una contraseña, deberá solicitar el soporte respectivo a la Mesa de Ayuda de la OTI. Dicha solicitud debe ser realizada directamente por el/la usuario/a titular de la cuenta. En caso excepcional, por indicación y autorización expresa de su Jefe/a inmediato/a.

2.2.3 Uso de los equipos informáticos

a) Los equipos informáticos serán asignados a los/las usuarios/as por la UA, quien realiza la asignación y control de bienes patrimoniales de la Entidad.

b) Los equipos informáticos no deberán ser desplazados de un lugar a otro sin la autorización de la UA, sin el conocimiento del/de la usuario/a a quien se asignó el bien patrimonial y de la OTI; de acuerdo a los lineamientos en la normativa institucional vigente[1].

c) Los/Las usuarios/as son responsables del cuidado y buen uso de los equipos informáticos asignados o compartidos con otros usuarios/as, debiendo asumir el resarcimiento de los daños y perjuicios que pudiesen ocasionar por negligencia o la indebida manipulación; sin perjuicio de las responsabilidades administrativas o disciplinarias a que hubiere lugar.

d) Cada usuario/a es responsable de los cuidados básicos de su computadora u otro equipo informático asignado, tales como: no ingerir bebidas cerca del equipo de cómputo asignado, no enchufar artefactos eléctricos domésticos (calentadores, hornos microondas u otros) en la misma toma eléctrica donde se conecta el equipo de cómputo, no colocar sobrepeso y mantener un adecuado espacio libre alrededor del equipo de cómputo para su debida ventilación.

e) Sobre los equipos móviles como laptops, discos duros externos u otro dispositivo informático, se deberá asegurar la seguridad física o en todo caso se deberán guardar en lugares seguros.

f) Los/Las usuarios/as no deben manipular los equipos informáticos (abrirlos, cambiar componentes, insertar dispositivos no autorizados, entre otros), siendo pasibles, en caso de daño a los equipos, de las sanciones que al respecto establezca el OSINFOR. Sólo el área de soporte técnico de la OTI está autorizado a realizar las tareas de mantenimiento preventivo o correctivo sobre dichos equipos. Asimismo, la OTI es responsable de brindar la autorización y supervisar las actividades, en caso éstas sean realizadas por proveedores, contratistas o terceros.

[1] Resolución de Jefatura N° 048-2018-OSINFOR, que aprueba la Directiva A2-DIR-001-V.02, Directiva de Administración de Bienes Muebles del OSINFOR.

g) Los equipos informáticos no deben estar ubicados en lugares en los que puedan ser afectados por el sol, temperaturas altas, humedad, filtraciones de agua o campos electromagnéticos intensos.

h) Cada usuario/a debe encender y apagar correctamente todos los equipos informáticos y componentes asignados para el cumplimiento de sus funciones.

i) Si se observa alguna anomalía durante los procesos de encendido y apagado, se debe comunicar a la Mesa de Ayuda de la OTI; asimismo, en caso de atascamiento de papel o mensajes de advertencia en los equipos de impresión.

j) Todos los equipos informáticos deben contar en la medida de lo posible, con un protector de sobretensión o UPS (respaldo de baterías) en buen estado.

k) En caso de interrupción del fluido eléctrico se recomienda desconectar todos los cables de energía de los equipos informáticos (laptops, monitor, CPU, impresoras y protectores de sobretensión). En el caso de los equipos que posean UPS, el tiempo que dure la batería le permitirá a el/la usuario/a guardar sus archivos y salir de los programas en que se encuentra trabajando, luego de lo cual debe apagar sus equipos informáticos. Se recomienda esperar aproximadamente cinco (05) minutos luego de que el suministro de energía se restablezca antes de volver a encender los equipos.

l) Se encuentra prohibido para todos los/las usuarios/as lo siguiente:

i. Despegar las etiquetas autoadhesivas que contienen identificación del fabricante, N° de serie, código patrimonial, entre otros.
ii. Retener equipos informáticos que no se estén usando en los Órganos y/o Unidades Orgánicas. Todo equipo informático que no esté en uso deberá ser puesto a disposición de la UA en coordinación con la OTI, para su distribución correspondiente según las necesidades técnicas de la Entidad.
iii. Mover equipos informáticos o desconectar bruscamente los cables de energía eléctrica cuando estén encendidos.
iv. La instalación de programas maliciosos (virus, gusanos, troyanos, etc.) en los equipos y red de datos institucional.
v. Utilizar los equipos del OSINFOR para participar en la obtención y transmisión de material que viole las leyes sobre acoso sexual y hostilidad laboral.
vi. Hacer ofertas fraudulentas de productos, artículos o servicios desde cualquier equipo del OSINFOR.
vii. Eludir la autenticación o seguridad del/de la usuario/a de cualquier estación de trabajo, red o cuenta de usuario/a.

2.2.4 Uso de dispositivos de almacenamiento

a) Evitar el uso de dispositivos personales para almacenar información institucional en la medida de lo posible. En caso de tener que utilizarlos, se deberá hacerlo cumpliendo con las siguientes prácticas: formateo previo, cifrado, borrado seguro, entre otros.

b) No usar dispositivos extraíbles de tipo promocional o aquellos que se desconoce su origen. Estos dispositivos deben ser examinados convenientemente, para validar que no contengan ningún tipo de software malicioso e incluso formateando el dispositivo previamente para evitar infecciones.

c) Utilizar el borrado seguro de la información confidencial antes de desechar los dispositivos de almacenamiento o transferir su uso a otras personas.

d) La OTI podrá, sustentadamente, deshabilitar los puertos USB y habilitarlos para los/as usuarios/as que necesiten dicha funcionalidad.

2.2.5 Uso de software y aplicaciones informáticas

a) El software base que se instalará en las estaciones de trabajo del OSINFOR es el siguiente:

i. Sistema operativo: Microsoft Windows o equivalente
ii. Suite ofimática: Microsoft Office estándar o equivalente
iii. Software antivirus
iv. Navegadores web
v. Lector de archivos PDF
vi. Compresor de archivos compatible con la extensión ZIP

b) El software base de propósito específico de acuerdo al perfil de usuario/a, es el siguiente:

i. Software GIS: para supervisores forestales y de fauna silvestre, así como especialistas de Geomática y usuarios/as autorizados/as.
ii. Software de diseño gráfico: para especialistas en diagramación, comunicaciones, imagen institucional y usuarios/as autorizados/as.
iii. Software de desarrollo de sistemas: para analistas de sistemas, programadores y usuarios/as autorizados/as.
iv. Software administrativo: para la gestión de actividades de apoyo administrativo.

c) La instalación de software adicional sólo será posible cuando se adquieran las respectivas licencias, las mismas que deberán contar con el visto bueno de la OTI. Las solicitudes de productos de software serán canalizadas a través de la Oficina de Administración a través de un requerimiento formal, la que tramitará su adquisición previa evaluación y opinión técnica por parte de la OTI respecto a las características y especificaciones requeridas, de acuerdo a las normas y procedimientos vigentes del OSINFOR. Se efectuarán revisiones periódicas del software instalado en los equipos informáticos.

d) La OTI conservará los medios de instalación, manuales y claves de activación del software licenciado.

e) Se encuentra prohibido lo siguiente:

i. Adquisición de software sin respetar los principios que rigen la contratación de licencias de software y servicios informáticos, tales como: vigencia tecnológica, trato justo igualitario y libre concurrencia de postores.
ii. Adquisición y uso de licencias de software, sin evaluación previa de la OTI.
iii. Instalación de software sin licencia o de código abierto “Open Sourse”, que no estén autorizados y/o evaluados por la OTI.
iv. La copia no autorizada de material sujeto a derechos de autor, incluyendo la digitalización, distribución o instalación de cualquier software para el cual el OSINFOR no tenga una licencia activa o no cuente con los derechos de autor respectivos.

v. La exportación de software, información técnica, software o tecnología de encriptación en violación de las leyes internacionales o regionales de control de exportaciones.
vi. Utilizar cualquier programa/script/comando, o enviar mensajes de cualquier tipo, con la intención de interferir o deshabilitar la sesión de un/una usuario/a, vía cualquier medio local o a través de Intranet/Internet/Extranet.
vii. Ejecutar cualquier forma de monitoreo de red que intercepte datos no dirigidos a la estación de trabajo del/de la usuario/a, a menos que esta actividad sea parte de las labores normales del/de la usuario/a, controlada y autorizada por la OTI.

2.2.6 Uso de los servicios de internet y telefonía

a) Los servicios de internet y telefonía fija deben ser utilizados exclusivamente para las labores del OSINFOR.

b) Cada usuario/a es responsable de las acciones que efectúe mediante el uso de los servicios de internet y telefonía fija, así como de las páginas a las que accede desde su equipo y/o cuenta de usuario/a otorgada.

c) La OTI en coordinación con la UA, realizarán la asignación y reasignación de las líneas directas, anexos, niveles de autorización de llamadas y bolsas de minutos de telefonía fija, de acuerdo a las necesidades de cada unidad orgánica para el cumplimiento de las funciones institucionales.

d) El/La usuario/a que, para el cumplimiento de sus funciones, necesite accesos adicionales a internet, o autorización para llamadas telefónicas, deberá coordinarlo con su Jefe/a inmediato/a, quien solicitará dicho acceso a la OTI con el respectivo sustento a través de un correo electrónico a la mesadeayuda@osinfor.gob.pe.

e) Se encuentra prohibido para todos los/las usuarios/as lo siguiente:

i. Descargar o acceder a sitios de música o videos, utilizar servicios de televisión, radio, música, video, juegos o cualquier otra actividad en línea que congestione o sature el ancho de banda de los enlaces a Internet del OSINFOR.
ii. Acceder a sitios web de dudosa reputación o potencialmente peligrosos que distribuyan o publiquen material pornográfico u obsceno, así como sitios involucrados en actividades fraudulentas o delictivas, narcotráfico, apología a la violencia y al terrorismo, discriminación, acoso o cualquier otra actividad ilegal.
iii. Conectarse a redes inalámbricas internas sin contar con la autorización del/de la Jefe/a inmediato/a y la OTI.

2.2.7 Uso del servicio de correo electrónico

a) La cuenta de correo electrónico institucional debe ser usada exclusivamente para propósitos relacionados con la labor del OSINFOR.

b) El servicio de correo electrónico del OSINFOR no debe ser utilizado para la creación y distribución de cualquier mensaje mal intencionado u ofensivo, incluyendo comentarios desfavorables acerca de raza, género, color, discapacidades, edad, orientación sexual, pornografía, creencias y prácticas religiosas, creencias políticas, país de origen, entre otros. Los/Las usuarios/as que reciban cualquier mensaje con este contenido de parte de

cualquier otro/a usuario/a del OSINFOR deben reportarlo de inmediato a su superior o responsable de la Unidad Orgánica.

c) Excepcionalmente, la OTI puede monitorear los flujos de mensajes en el sistema de correo institucional cuando las circunstancias lo ameriten (eventos o incidentes de seguridad de la información) o por disposición superior.

d) Los/Las usuarios/as podrán adjuntar archivos en cada mensaje de correo electrónico hasta el límite técnico determinado por la OTI. En el caso que la información por ser remitida supere este límite, se debe consultar a la OTI la alternativa más adecuada según el caso. Si la información debe remitirse entre áreas de una misma sede, esto puede ser realizado mediante carpeta compartida en red u otro medio de grabación de información.

e) Se encuentra prohibido para todos los/las usuarios/as lo siguiente:

   i. Configurar el reenvío automático de correos electrónicos del OSINFOR a un sistema de correo electrónico de terceros (Google, Yahoo, Hotmail, entre otros). Los mensajes que sean reenviados de manera individual por el/la usuario/a no deben contener información confidencial del OSINFOR, no aplica para el caso de los/las usuarios/as externos/as del OSINFOR.
   ii. Utilizar servicios de correo electrónico de terceros (Google, Yahoo, Hotmail u otros) para llevar a cabo labores oficiales del OSINFOR y comunicación con otras instituciones, tampoco debe almacenar o retener mensajes en nombre del OSINFOR.
   iii. Utilizar mecanismos y sistemas que intenten ocultar la identidad del emisor del correo.
   iv. Manipular o alterar las cabeceras de correo electrónico.
   v. Enviar mensajes de correo electrónico no solicitado, incluyendo el envío de mensajes con contenido inapropiado u otro material publicitario a personas que no lo han requerido específicamente.
   vi. Cualquier forma de acoso vía correo electrónico, teléfono o mensajería.
   vii. Creación o retransmisión de “cartas cadena”, esquemas “Ponzi” o “piramidales” de cualquier tipo.

2.3 Uso de medidas de seguridad de la información

2.3.1 Todos los/las usuarios/as de los recursos y servicios informáticos del OSINFOR, deben cumplir con las Políticas de Seguridad de la Información[2].

2.3.2 El/La usuario/a debe asegurar sus equipos informáticos (mediante bloqueo de pantalla o cierre de sesión) siempre que necesite ausentarse de su puesto de trabajo.

2.3.3 Los medios de almacenamiento removibles como CDROM, DVD o unidades de almacenamiento USB deben ser considerados como sensibles; por lo tanto, deben guardarse en un lugar seguro.

2.3.4 Las computadoras portátiles deben ser protegidas, utilizando cables de seguridad o guardadas en un lugar seguro bajo llave.

2.3.5 Las impresiones deben ser retiradas de las impresoras tan pronto como sean impresas; esto ayuda a asegurar que los documentos sensibles dejados en las

[2] Resolución de Jefatura N° 036-2018-OSINFOR, que aprueba dieciséis (16) políticas para la seguridad de la información del OSINFOR.

bandejas de las impresoras no sean revisados ni recogidos por personas incorrectas.

2.3.6 El/La usuario/a debe almacenar la información institucional en las carpetas compartidas en red que correspondan a su Unidad Orgánica. Está prohibido almacenar en las carpetas compartidas en red, información ajena al OSINFOR (por ejemplo, archivos de música y video, fotografías personales, instaladores de aplicaciones, entre otros). La OTI está facultada a eliminar esta información sin previo aviso.

2.3.7 Todo archivo que provenga del exterior, ya sea adjunto a un correo electrónico, por internet o en algún medio de almacenamiento removible, debe ser revisado previamente con el software antivirus instalado en el equipo informático. En caso de que se detecte o sospeche que ha existido una infección por virus, troyanos u otros programas maliciosos, se debe desconectar el equipo de la red y solicitar de inmediato la asistencia especializada a la Mesa de Ayuda de la OTI. El equipo no debe volver a ser utilizado hasta que el responsable de soporte técnico de la OTI haya confirmado la solución a la incidencia de seguridad.

2.3.8 Toda persona que, por cualquier modalidad contractual, labore o brinde servicios en el OSINFOR, deberá hacer entrega de los archivos de trabajo almacenados en el computador asignado a su uso, de acuerdo a las Políticas de Seguridad de la Información del OSINFOR, precisando el detalle de los mismos como parte de su entrega de cargo o informe final de servicio, cuando concluya la relación laboral o sea destacada a otra Unidad Orgánica. Está prohibido eliminar o adulterar archivos de trabajo.

2.4 Uso de medidas de ecoeficiencia

2.4.1 La impresión de documentos debe realizarse por ambas caras de la hoja de papel, siempre que sea posible.

2.4.2 Se debe dar preferencia a la comunicación y distribución electrónica (por ejemplo, mediante las aplicaciones de trámite documentario o mediante correo electrónico) de información y documentos, en reemplazo de la escrita. Los correos electrónicos no deben ser impresos salvo que sea absolutamente necesario. Se debe dar preferencia al escaneado y distribución digital de documentos en lugar del fotocopiado cuando se requiera compartir información.

2.4.3 Promover el escaneado de los documentos recibidos a fin de que sean compartidos por las dependencias que lo requieran en forma de archivo digital, evitando el fotocopiado sucesivo del mismo documento.

2.4.4 Los equipos informáticos deben ser apagados completamente al finalizar la jornada laboral.

2.4.5 Los equipos informáticos deben ser apagados o configurados en modo de ahorro de energía, durante los períodos de refrigerio. En el caso de que algunos equipos no se puedan apagar por completo, se debe al menos apagar los monitores.

2.4.6 Se encuentra prohibida la impresión a colores, salvo en el caso las Unidades Orgánicas o Funcionales autorizadas por la Alta Dirección para la producción de mapas, documentos o publicaciones que así lo requieran.

2.5 Gestión de acceso a los servicios informáticos

2.5.1 Lineamientos generales

a) La OTI controla el acceso a los servicios informáticos del OSINFOR, tales como: red de dominio institucional (carpetas compartidas, impresoras, entre

otros), internet, correo electrónico institucional, telefonía fija (IP), sistemas de información y aplicaciones. Asimismo, gestiona el acceso a dichos servicios de acuerdo a los requerimientos y necesidades de cada usuario/a para el desempeño de sus funciones laborales.

b) Los accesos a los servicios informáticos son otorgados previa solicitud de los/las Directores/as o Jefes/as de los Órganos y Unidades Orgánicas mediante el Formato Control de accesos a aplicaciones y servicios de TI (A5-FOR-117-V.01) o el Formato control de accesos a aplicaciones y servicios por grupo de usuarios/as (A5-FOR-140-V.01) según corresponda; así mismo, deberá estar suscrito solo por el/la usuario/a de Tipo A y B, de corresponder.

c) La OTI otorga las cuentas de usuario y contraseña de acceso a los/las usuarios/as para el desempeño de sus funciones, de tal manera que puedan utilizar los servicios informáticos del OSINFOR, siendo estas de carácter personal, intransferible y confidencial.

d) Toda solicitud de alta, baja o modificación de cuenta de usuario/a, debe incluir como mínimo los siguientes datos:

   i. Nombre completo y DNI de la persona para quien se solicita la activación, modificación o desactivación del servicio.
   ii. Función que desempeña, área a la cual pertenece y ubicación física (sede o local) de la persona para quien se solicita la cuenta de usuario, en caso corresponda.

e) Los/Las Directores/as y/o Jefes/as de los Órganos o Unidades Orgánicas son los encargados de autorizar y definir los niveles de acceso a los servicios informáticos de los/las usuarios/as, según corresponda, tomando en cuenta los privilegios de acceso que puedan necesitar para el desarrollo de sus funciones.

f) El acceso a los servicios de red y sistemas de información del OSINFOR deben basarse en la función del/de la usuario/a, en el análisis y evaluación de riesgos a los que están expuestos, en la revocatoria de los derechos de acceso según vínculo laboral y/o contractual, así como en el uso de perfiles de usuarios/as estandarizados definidos según roles.

g) El acceso a los servicios informáticos otorgado a el/la usuario/a es para el estricto cumplimiento de las labores encomendadas, acorde a la Política de Control de Accesos (SGSI-A5-POL-005).

h) La OTI, en el marco de sus competencias funcionales, elabora procedimientos técnicos para el registro y baja de usuarios/as, aprovisionamiento de acceso a los/las usuarios/as, gestión de derechos de acceso privilegiado y revisión o ajuste de derechos acceso, para los servicios de red, así como a los sistemas de información y aplicaciones.

i) Cuando el/la usuario/a de Tipo A se ausente temporalmente de la Entidad, sea por hacer uso de su periodo vacacional, descanso médico o por cualquier otro motivo, por un tiempo mayor de cinco (5) días laborales, la URH deberá informarlo a la OTI, a través del correo electrónico mesadeayuda@osinfor.gob.pe, con la anticipación respectiva, para la suspensión temporal de todas las cuentas de acceso a servicios de dicho usuario/a durante el periodo que dure su ausencia. El/La Director/a o Jefe/a inmediato/a puede solicitar excepcionalmente el restablecimiento de las cuentas de un/una usuario/a temporalmente ausente, bajo responsabilidad.

j) La solicitud de modificación de servicios de la cuenta de usuario/a es realizada por el/la Director/a o Jefe/a del Órgano o Unidad Orgánica que corresponda, a través del correo electrónico mesadeayuda@osinfor.gob.pe.

k) La solicitud de baja de servicios de la cuenta de usuario/a de Tipo A, es realizada por la URH a través del sistema de gestión de legajos de la URH, para lo cual debe mantener actualizado el referido sistema con el fin de realizar la baja correspondiente en todos los servicios informáticos. Excepcionalmente, el/la Director/a o Jefe/a inmediato/a puede solicitar la baja con anticipación a las alertas emitidas por la URH.

l) Para el caso de baja de servicios de la cuenta de usuario/a de Tipo B, se aplicará la fecha de cese del servicio, consultoría, locación u otro.

m) Para el caso de baja de servicios de la cuenta de usuario/a de Tipo C, su cuenta caduca cada 180 días, por lo que el Órgano o Unidad Orgánica que corresponda deberá solicitar su actualización mediante el Formato Control de accesos a aplicaciones y servicios TI (A5-FOR-117-V.01) o el Formato control de accesos a aplicaciones y servicios por grupo de usuarios/as (A5-FOR-140-V.01), en caso sea necesario.

2.5.2 Acceso a la red de dominio institucional

Lo regulado a continuación debe ser aplicado por los/as usuarios/as de Tipo A y B:

a) Activación del servicio

i. La cuenta del/de la usuario/a de dominio se activa al momento de recibir la solicitud, la cual debe indicar explícitamente la pertenencia o inclusión de la nueva cuenta de usuario/a de dominio en un grupo de seguridad específico previamente autorizado, en el caso sea requerido (por ejemplo “GG_OTI”). La inclusión de la cuenta de usuario/a de dominio a un grupo deberá consignarse en la solicitud; salvo indicación contraria, la cuenta de usuario/a será por defecto incluido en los grupos de seguridad del área a la cual pertenece.

ii. La OTI procederá a activar la cuenta de usuario/a de dominio, asignando el identificador de la cuenta de usuario/a y contraseña inicial correspondiente, acorde con los lineamientos precisados en el numeral 2.1 de la presente Directiva y el detalle de la solicitud. La contraseña de la cuenta debe ser cambiada por el/la usuario/a inmediatamente después de la finalización de las labores de configuración del equipo informático asignado.

iii. La configuración del perfil de usuario/a de dominio en el equipo informático asignado, es realizada directamente por el área de soporte técnico de la OTI.

iv. La identificación del nombre del equipo (hostname) asignado a el/la usuario/a, tomará en cuenta la ubicación o área de pertenencia, así como un código numérico único. Por ejemplo, a un equipo perteneciente a la OTI se le puede asignar como nombre **oti-0111,** en el cual la primera parte indica el área de pertenencia y la segunda parte indica los últimos dígitos de su código patrimonial.

b) Precisiones adicionales a la modificación o desactivación del servicio

i. En caso de modificación de la información de la cuenta de usuario/a de dominio, debe ser solicitado por el/la Director/a o Jefe/a inmediato/a a través del correo electrónico mesadeayuda@osinfor.gob.pe y debe indicar los cambios específicos a realizar a dicha cuenta. Si el/la usuario/a cambia de área o puesto, la cuenta de usuario/a será removida de todos los grupos a los que pertenece, antes de asignar la

nueva pertenencia a grupos. De no haber indicación, la cuenta del usuario/a será por defecto incluida en los grupos de seguridad de su nuevo puesto o área de pertenencia, verificando que sea removida de los grupos del área previa.

ii. En caso de suspensión de la cuenta de usuario/a, se debe especificar si será desactivada de forma temporal o permanentemente. En ambos casos, la cuenta del/de la usuario/a será removida de todos los grupos de seguridad a los que perteneciera antes de su desactivación.

iii. De no existir solicitud de suspensión o baja por parte del área de pertenencia del/de la usuario/a o de la URH, la OTI procederá a la desactivación de la cuenta del/de la usuario/a si observa que la misma tiene sesenta (60) días o más sin utilización.

2.5.3 Acceso a correo electrónico institucional

Lo regulado a continuación debe ser aplicado por los/as usuarios/as de Tipo A y B:

a) Activación del servicio

i. El servicio de correo electrónico deberá cumplir los lineamientos para creación de cuentas establecidos en el numeral 2.1 de la presente Directiva. El servicio de correo electrónico está integrado con la red de dominio institucional; en ese sentido, la identificación de la cuenta de correo electrónico y cuenta del/de la usuario/a de dominio, será la misma para ambos servicios. Si se requiere la creación de un correo genérico o institucional que designe no a una persona, sino a una función o área específica (por ejemplo, soporte@osinfor.gob.pe), se debe especificar quién será el/la servidor/a o funcionario/a responsable del manejo de esta cuenta de correo electrónico, tiempo de vigencia y especificar las actividades que se realizarán con ella. Asimismo, en el caso que la cuenta de correo sea utilizada por más de un/una usuario/a de un determinado Órgano o Unidad Orgánica, el/la Directora/a o Jefe/a correspondiente deberá indicar el personal autorizado para manejo de dicha cuenta, así como los permisos respectivos.

ii. Mediante el Formato Control de accesos a aplicaciones y servicios TI (A5-FOR-117-V.01) se debe indicar si se requiere una capacidad de almacenamiento superior a la que corresponde por defecto a el/la usuario/a (tipo funcionario, tipo servidor o tipo proveedor de servicios).

iii. Asimismo, en la solicitud se debe precisar la pertenencia o inclusión de la nueva cuenta de correo en un grupo de distribución específico (por ejemplo: “equipo_sgsi@osinfor.gob.pe” u “oti@osinfor.gob.pe”). De no haber indicación, el/la usuario/a será por defecto incluido en los grupos de distribución del área a la cual pertenece, así como a los grupos de distribución global del OSINFOR.

iv. Adicionalmente debe precisarse si la cuenta de correo debe ser sólo para uso interno (sólo envío y recepción de correos del dominio de OSINFOR). Salvo indicación contraria, por defecto las cuentas de correo podrán enviar y recibir correos de cualquier dominio externo.

v. La OTI procederá a la creación del buzón de correo correspondiente siempre y cuando exista disponibilidad de las licencias que correspondan. De acuerdo a la ubicación del/de la usuario/a, se configurará el acceso por medio de un cliente de correo para equipos estacionarios o por medio de un cliente de correo web.

b) Precisiones adicionales a la modificación o desactivación del servicio

i. La solicitud de modificación de las características del servicio de correo electrónico deberá precisar los cambios específicos que se deben realizar a la cuenta de correo (por ejemplo: cambio de puesto o área, cambio de pertenencia a grupos de distribución, cambio de autorización para envío a listas globales, entre otros). De no haber indicación, la cuenta de usuario/a será por defecto incluida en los grupos de distribución de su nuevo puesto o área de pertenencia; y, será removida de los grupos del área previa.

ii. En caso se requiera aumentar la capacidad de almacenamiento del buzón de correo electrónico del/de la usuario/a, la solicitud debe incluir la justificación respectiva. La OTI procederá al aumento siempre y cuando exista disponibilidad de recursos en el servicio de correo electrónico.

iii. En caso de suspensión de la cuenta de correo, se debe especificar si será desactivada de forma temporal o permanentemente. En ambos casos, la cuenta de correo será removida de todos los grupos de distribución a los que perteneciera antes de su desactivación.

iv. De no existir solicitud de suspensión o baja por parte del área de pertenencia del/de la usuario/a o de la URH, la OTI procederá a la desactivación del correo electrónico si observa que la misma tiene sesenta (60) días o más sin utilización.

2.5.4 Acceso a servicio de internet

Lo regulado a continuación debe ser aplicado por los/as usuarios/as de Tipo A y B:

a) Activación del servicio

El servicio de internet se activa junto con la creación de la cuenta del/de la usuario/a de dominio. El acceso al servicio de internet se brinda de acuerdo a los siguientes niveles de autorización:

i. **Básico**. Nivel que permite a el/la usuario/a acceder a sitios web limitados. No permite el acceso a redes sociales y correo electrónico de terceros. Este nivel de acceso se configura a los/las proveedores/as de servicios que requieren de acceso a internet en el OSINFOR para el desarrollo de sus actividades. Este acceso debe ser solicitado y autorizado por el/la Jefe/a del área a la cual el/la proveedor/a brinda servicios a través de un correo electrónico a la mesadeayuda@osinfor.gob.pe.

ii. **Estándar**. Nivel que permite al/a la usuario/a acceder a cualquier sitio web cuyo contenido no esté prohibido, acorde a las Políticas de Seguridad de la Información del OSINFOR, así como el acápite 2.2.6 de la presente Directiva. Este nivel de acceso se configura por defecto a todos los/las servidores/as de la Entidad.

iii. **Soporte**. Nivel que permite al/a la usuario/a, además de los permisos de los niveles anteriores, el acceso a descarga de archivos especiales como drivers, instaladores, archivos ejecutables y software. Este nivel de acceso está dirigido al área de soporte técnico de la OTI.

iv. **Funcionario**. Nivel especial que permite acceso a contenido multimedia, servicios de almacenamiento en Internet, redes sociales y mensajería instantánea externa. Este nivel de acceso aplica sólo para la Alta Dirección, Directores/as, Sub Directores/as y Jefes/as de los Órganos y Unidades Orgánicas del OSINFOR. Para este nivel se mantiene la prohibición de acceder a sitios que distribuyan o publiquen material pornográfico u obsceno, así como sitios involucrados en actividades fraudulentas o delictivas, de narcotráfico, apología a la violencia y al terrorismo, discriminación, acoso o cualquier otra actividad ilegal.

v. **Personalizado**. Nivel que permite al/a la usuario/a acceder a sitios web o dominios específicos. Este acceso debe ser especificado y autorizado por el/la Director/a o Jefe/a inmediato/a del/de la usuario/a en la solicitud, en la cual se debe indicar también la justificación del acceso requerido, así como el periodo de tiempo durante el cual debe estar activo. Se realiza a través de un correo electrónico a la mesadeayuda@osinfor.gob.pe.

b) Precisiones adicionales a la modificación o desactivación del servicio

La solicitud de modificación del perfil de navegación o desactivación del servicio de internet, deberá ser realizada por el/la Director/a o Jefe/a inmediato/a del/de la usuario/a a través del correo electrónico mesadeayuda@osinfor.gob.pe y deberá precisar los cambios específicos que se debe realizar al nivel de acceso otorgado previamente, según corresponda.

2.5.5 Acceso a servicio de telefonía IP

Lo regulado a continuación debe ser aplicado por los/as usuarios/as de Tipo A:

a) Activación del servicio

i. Por defecto, los anexos cuentan con autorización para llamadas internas y llamadas a servicios gratuitos. Para realizar llamadas a destinos externos, se debe solicitar una clave de usuario/a a través del correo electrónico mesadeayuda@osinfor.gob.pe, la cual es personal, secreta e intransferible. Los niveles de autorización, de acuerdo a la necesidad del Órgano o Unidad Orgánica, son los siguientes:

- Destinos fijos locales
- Destinos fijos locales + fijos nacionales
- Destinos fijos locales + fijos nacionales + móviles
- Destinos fijos locales + fijos nacionales + móviles + internacionales

ii. La solicitud de activación del servicio de telefonía IP debe indicar lo siguiente:

- Si se requiere la asignación de un número de anexo y un teléfono físico IP.
- Si se requiere la creación de una clave de usuario/a para llamadas a destinos externos (locales y nacionales), para lo cual se debe indicar el nivel de autorización.

iii. La asignación de un teléfono físico IP depende de la disponibilidad de equipos nuevos o sin uso. De no haber disponibilidad, el/la usuario/a o área solicitante puede requerir a la OTI la emisión de especificaciones técnicas para gestionar con la Oficina de Administración la adquisición de un equipo compatible con el sistema de central telefónica en uso de la Entidad, de acuerdo a lo establecido en los procedimientos de adquisición vigentes del OSINFOR y la normativa relacionada.

iv. Si se ha requerido una clave de usuario/a para llamadas a destinos externos (locales y nacionales), la OTI verificará con la Oficina de Administración la procedencia de la solicitud y los recursos disponibles, y aplicará, de ser necesario, una bolsa límite de minutos mensuales para cada tipo de llamadas autorizado.

b) Precisiones adicionales a la modificación o desactivación del servicio

i. La solicitud de modificación de las características del servicio debe ser realizada por el/la Directora/a o Jefe/a inmediato del usuario/a a la OTI a través del correo electrónico mesadeayuda@osinfor.gob.pe e indicar los cambios específicos que deben realizarse al número de anexo, teléfono físico o clave de usuario/a (por ejemplo: cambio de puesto o área, traslado del anexo, cambio de nombre del anexo, cambio de nivel de autorización para llamadas al exterior, entre otros). De no haber indicación contraria, cuando un teléfono IP físico sea reasignado a un nuevo usuario/a, se colocará su nombre en el anexo, tanto en el equipo como en el directorio de la central telefónica y directorio telefónico institucional.

ii. En caso de que se requiera elevar el nivel de autorización o las bolsas límites de minutos asignados a una clave de usuario/a, la solicitud debe incluir la justificación con el sustento respectivo. La OTI evaluará la solicitud y los recursos disponibles para el cambio; así mismo, coordinará con la Oficina de Administración cuando sea requerido.

iii. Toda solicitud de traslado, reasignación o devolución de un teléfono físico debe ser realizada en conformidad con la normativa vigente del OSINFOR para la administración de bienes muebles.

iv. En caso de suspensión de la cuenta de usuario/a, se debe especificar si el anexo o clave de usuario/a debe ser desactivado temporal o permanentemente. En ambos casos, se desactivarán todas las categorías de llamadas al exterior para los que tuviera autorización antes de la solicitud.

v. De no existir solicitud de suspensión o baja por parte del área de pertenencia del/de la usuario/a o de la URH, la OTI procederá a la desactivación de la cuenta del/de la usuario/a si observa que la misma tiene sesenta (60) días o más sin utilización.

2.5.6 Acceso a sistemas de información y aplicaciones de software

Lo regulado a continuación debe ser aplicado por los/as usuarios/as de Tipo A, B y C:

a) Activación del servicio

i. Los accesos a los sistemas de información y aplicaciones de software deberán cumplir los lineamientos para creación de cuentas establecidos en el numeral 2.1 de la presente Directiva. Adicionalmente, se requerirá la autorización del responsable del

sistema de información, precisado en la Directiva del SIGO. Para tal efecto, la solicitud debe contar con el visto bueno del/de la responsable del sistema de información correspondiente.

ii. El acceso a los sistemas de información al usuario/a de Tipo C, será realizado previa validación de la suscripción de acuerdo de confidencialidad, convenio de cooperación vigente y/o solicitud respectiva.

b) Precisiones adicionales a la modificación o desactivación del servicio

i. En caso de suspensión del acceso a alguno de los sistemas de información para un/una usuario/a, la solicitud será canalizada a través del correo electrónico mesadeayuda@osinfor.gob.pe.

ii. En el caso de suspensión o baja de la cuenta de usuario/a de los sistemas de información que no estén integrados a la cuenta de dominio institucional, se procederá a la baja individual respectiva.

iii. De no existir solicitud de suspensión o baja por parte del área de pertenencia del/de la usuario/a o de la URH, la OTI procederá a la desactivación de la cuenta del/de la usuario/a de Tipo A y B, si observa que la cuenta de dominio tiene sesenta (60) días o más sin utilización.

2.6 Uso de la Mesa de Ayuda del OSINFOR

2.6.1 La OTI cuenta con una plataforma de atención de incidencias y/o requerimientos de servicios, denominada Mesa de Ayuda de la OTI, que está disponible a través del sistema SIGO integrado, el correo electrónico mesadeayuda@osinfor.gob.pe o del número telefónico 01-615 7373 anexo 123.

2.6.2 Para la atención de dichos requerimientos y/o incidencias se deberá considerar el procedimiento A5.4.1 Atención de Incidencias y/o Requerimientos para mantener la Operatividad de los Servicios TI para usuarios/as finales[3].

2.7 Proceso disciplinario y sanción administrativa

2.7.1 El incumplimiento de la presente Directiva por parte del/de la usuario/a, que genere un perjuicio al OSINFOR, dará lugar a las responsabilidades administrativas y/o civiles que correspondan.

2.8 Difusión y seguimiento

2.8.1. La OTI está encargado de efectuar la difusión y seguimiento de la presente Directiva.

2.9 Responsabilidades

2.9.1 La OTI es el órgano encargado de supervisar el cumplimiento de la presente Directiva, así como de la administración de los recursos informáticos (hardware y software), gestión de accesos y orientación a los/las usuarios/as para la debida utilización de los mismos.

[3] Establecido en el Manual de Procesos y Procedimientos Estratégicos y de Apoyo del OSINFOR, aprobado por Resolución Presidencial 127-2017-OSINFOR.

2.9.2 El/La Jefe/a y/o Director/a de cada Órgano o Unidad Orgánica del OSINFOR, es responsable de las funciones detalladas en la presente Directiva.

2.9.3 La URH, la UA y la DEFFS son los responsables de coordinar, con la OTI, la realización de capacitaciones y/o actividades de concientización para conocimiento y aplicación de la presente Directiva.

2.9.4 La OTI, es responsable de informar a la Alta Dirección sobre el incumplimiento de lo dispuesto en la presente Directiva.

2.9.5 La UA es la responsable de realizar el control de los bienes, durante su asignación, ingreso y traslado.

2.9.6 Cada usuario/a es responsable de la actualización de la contraseña inicial otorgada por la OTI, así como de velar por su protección.

III. DISPOSICIÓN COMPLEMENTARIA

3.1 Cualquier acción o aspecto no contemplado en la presente Directiva, será resuelto por la OTI en coordinación con la Alta Dirección, Oficial de Seguridad de la Información y/o Comité de Gobierno Digital.

IV. CONTROL DE CAMBIOS

Versión	Fecha	Justificación	Textos Modificados	Responsable
01	Elaboración inicial del documento			Oficina de Tecnologías de la Información

V. FORMATOS

- Formato Control de accesos a aplicaciones y servicios de TI (A5-FOR-117-V.01)

PERÚ | Presidencia del Consejo de Ministros | Organismo de Supervisión de los Recursos Forestales y de Fauna Silvestre - OSINFOR

FORMATO CONTROL DE ACCESOS A APLICACIONES Y SERVICIOS

A5-FOR-117-V.01

N° : _____ **FECHA SOLICITUD :** / /

I. DATOS DEL USUARIO FINAL

N° Doc. Identidad		**Teléfono de Contacto**	
Apellidos y Nombres		**Tipo de Personal**	
Correo Electrónico		**Cargo/Función**	
Lugar de Trabajo		**Oficina / Unidad/ Área de Trabajo**	

II. ACCESOS A SERVICIOS DE REDES Y COMUNICACIONES

SERVICIO	DETALLE	DESDE	HASTA	RESPONSABLE OTI ASIGNADO
☐ Acceso a Red	☐ Usuario de Red ☐ Punto de Red			
☐ Correo electrónico	☐ Cuenta de Correo ☐ Grupo de Correo Especificar:			
☐ Internet	☐ Básico ☐ Estándar ☐ Funcionario ☐ Personalizado Especificar:			
☐ Carpeta Compartida	Nombre de carpeta: ..... Permisos: ☐ Lectura ☐ Escritura ☐ Control Total			
☐ Telefonía	☐ Fija Local ☐ Fija Nacional ☐ Celular ☐ Internacional			
☐ Otro	Especificar:			

III . ACCESOS A SISTEMAS DE INFORMACIÓN

SISTEMA	MODULO	OPCION	DETALLE	DESDE	HASTA	V.B. del RESPONSABLE DEL SISTEMA DE INFORMACIÓN (1)	RESPONSABLE OTI ASIGNADO

IV. ACCESOS A SERVICIOS DE SOPORTE A USUARIOS

SERVICIO	DETALLE	RESPONSABLE OTI ASIGNADO
☐ Instalación de Equipo	☐ PC ☐ Laptop ☐ Teléfono ☐ Otro Especificar:	
☐ Acceso a dispositivos	☐ Impresora ☐ Escaner ☐ Otro Especificar:	
☐ Instalación de software	Especificar:	
☐ Otro	Especificar:	

V. JUSTIFICACIÓN

VI. OBSERVACIONES

ÁREA USUARIA	OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN

VII. RESPONSABILIDAD

Firma del Usuario Final (2)	Firma y sello del Responsable de Autorización Área Usuaria	Firma y sello del Responsable de la OTI de verificar el acceso otorgado
		Fecha de Verificación: / /
APELLIDOS Y NOMBRES	**APELLIDOS Y NOMBRES**	**APELLIDOS Y NOMBRES**

(1) El acceso a los sistemas de información, se realizará previa autorización del responsable del Sistema de Información, precisado en la Directiva del SIGO.
(2) El acceso otorgado al usuario final a los sistemas y servicios de TI es para el estricto cumplimiento de las labores encomendadas, acorde a lo establecido a la Directiva para el uso de recursos informáticos del OSINFOR (A5-DIR-019-V.01).

- Formato Control de accesos a aplicaciones y servicios por grupo de usuarios/as (A5-FOR-140-V.01)

PERÚ | Presidencia del Consejo de Ministros | Organismo de Supervisión de los Recursos Forestales y de Fauna Silvestre - OSINFOR

FORMATO CONTROL DE ACCESOS A APLICACIONES Y SERVICIOS POR GRUPO DE USUARIOS

A5-FOR-140-V.01

N° : **FECHA SOLICITUD :** / /

I. DATOS DEL USUARIO SOLICITANTE

Apellidos y Nombres		**Teléfono de Contacto**	
Correo Electrónico		**Cargo/Función**	
Lugar de Trabajo		**Oficina / Unidad/ Área de Trabajo**	

II. JUSTIFICACIÓN

Seleccionar de la lista

III. ACCESOS A SERVICIOS DE REDES Y COMUNICACIONES

Seleccionar de la Lista

SERVICIO (1)	DETALLE	TIPO PERSONA (2)	LUGAR DE ACCESO (3)	APELLIDOS Y NOMBRES DEL USUARIO	DNI	DESDE	HASTA	RESPONSABLE OTI ASIGNADO
								Fecha Atención: / /

IV . ACCESOS A SISTEMAS DE INFORMACIÓN

SISTEMA (4)	DETALLE	TIPO PERSONA (2)	LUGAR DE ACCESO (3)	APELLIDOS Y NOMBRES DEL USUARIO	DNI	DESDE	HASTA	CORREO	PERFIL DE USUARIO	RESPONSABLE OTI ASIGNADO
										Fecha Atención: / /

AUTORIZACIÓN DEL RESPONSABLE DEL SISTEMA DE INFORMACIÓN

FIRMA DEL RESPONSABLE DEL SISTEMA DE INFORMACIÓN (5)

VI. OBSERVACIONES

ÁREA SOLICITANTE	OFICINA DE TECNOLOGÍA DE LA INFORMACIÓN

VII. RESPONSABILIDAD

Firma y sello del Responsable de Autorización Área Usuaria (2)	Firma y sello del Responsable de la OTI de verificar el acceso otorgado
	Fecha de Verificación: / /

APELLIDOS Y NOMBRES	APELLIDOS Y NOMBRES

Nota:

(1) Servicio de redes y comunicaciones para el cual se solicita acceso: Red, Correo Electrónico, Red y Correo Electrónico, Internet, Telefonía

(2) Tipo de usuario para quien se solicita el acceso: personal CAS (D.L. 1057), Locador de Servicios, Practicante, Tercero, Externo GORE, Otro, entre otros.

(3) Sede a la que pertenece el usuario para el cual se solicita acceso: Sede Principal, OD Atalaya, OD Chiclayo, OD Iquitos, OD La Merced, OD Pucallpa, Od Puerto Maldonado, Od Tarapoto, FEMA, GORE (región), etc.

(4) Sistema de información para el cual se solicita acceso: SIADO, SISFOR, SIGOsfc, etc.

(5) El acceso a los sistemas de información, se realizará previa autorización del responsable del Sistema de Información, precisado en la Directiva del SIGO.

(6) Es responsabilidad del área solicitante, comunicar oportunamente el cese del personal externo (contratistas, proveedores, terceros, etc) para quienes se solicitó el acceso a los servicios de TI.

- Formato Carta de compromiso del buen uso del sistema de información (A5-FOR-142-V.01)

PERÚ Presidencia del Consejo de Ministros — Organismo de Supervisión de los Recursos Forestales y de Fauna Silvestre OSINFOR FORMATO CARTA DE COMPROMISO DEL BUEN USO DEL SISTEMA DE INFORMACIÓN PARA USUARIOS EXTERNOS	A5-FOR-142-V.01

CARTA DE COMPROMISO DEL BUEN USO DEL SISTEMA DE INFORMACIÓN

Lugar y fecha: .....

Señores
Organismo de Supervisión de los Recursos Forestales y de Fauna Silvestre - OSINFOR

Atención: [Órgano o Unidad Orgánica, según corresponda] del OSINFOR

Por medio de la presente, yo [Nombres y apellidos completos].....
identificado con D.N.I. N° ..... y correo electrónico .....,
con domicilio en.....;
trabajador del/de la [Entidad en la que labora] .....,
en la cual ocupo el cargo de.....

Que, habiendo recibido mi usuario y contraseña (siendo estas de carácter personal, intransferible y confidencial) por parte del OSINFOR, en la fecha del ...../...../....., para el acceso al sistema ....., me comprometo a:

- Mantener y guardar estricta reserva y absoluta confidencialidad respecto a la información registrada en el sistema.
- Proteger los activos de información[1], previniendo su pérdida, modificación y/o destrucción no autorizada, falsificación, robo, uso indebido y/o divulgación de los activos de información.
- No utilizar información para beneficio propio o de terceros.
- Mantener el uso exclusivo y personal del usuario y contraseña que se me ha proporcionado.
- Comunicar al OSINFOR con un plazo de antelación de 05 días al término de mi vínculo laboral con el/la [Entidad en la labora] ....., a fin que pueda controlar mi usuario [cuenta de usuario asignado por OSINFOR] .....; comunicación que enviaré al correo electrónico [Responsable o Coordinador del Órgano o Unidad Orgánica, según corresponda] .....@osinfor.gob.pe, para deslindar responsabilidades.

Así mismo, dejo establecido mi deber y compromiso de Confidencialidad y No Divulgación de Información a la que tenga acceso producto de la cuenta de usuario y contraseña otorgados por el OSINFOR, la misma que opera desde la fecha de suscripción del presente documento y se mantendrá vigente incluso hasta cinco (5) años posteriores a la extinción de mi relación laboral y/o contractual con [Entidad en la que trabaja] .....

Atentamente,

Firma:

.....
[Nombres y apellidos completos]

[1] Datos/Información, Aplicaciones -Software, Equipo Informático - Hardware, según corresponda.