REPUBLICA DEL PERU

RESOLUCIÓN PRESIDENCIAL N° 054 -2016-OSINFOR

Lima, 08 JUN. 2016

VISTOS:

El Memorándum Nº 195-2016-OSINFOR/05.1, de fecha 26 de mayo de 2016, del Jefe (e) de la Oficina de Tecnología de la Información, por el cual propone los Lineamientos para el uso de los recursos informáticos en el Organismo de Supervisión de los Recursos Forestales y de Fauna Silvestre – OSINFOR, sustentado en el Informe N°009-2016-OSINFOR/05.1-JPB, de fecha 26 de mayo del 2016; el Memorándum Nº 538-2016-OSINFOR/04.1, de la Jefa (e) de la Oficina de Planeamiento y Presupuesto por el cual hace suyo el Informe N°046-2016-OSINFOR/04.1.1, de fecha 31 de mayo de 2016, elaborado por la Sub Oficina de Planeamiento y el Informe Legal N.º 101-2016-OSINFOR/04.2, de fecha 01 de junio de 2016, de la Oficina de Asesoría Jurídica , y;

CONSIDERANDO:

Que, mediante Decreto Legislativo N. º 1085, se creó el Organismo de Supervisión de los Recursos Forestales y de Fauna Silvestre -OSINFOR, como Organismo Público Ejecutor, adscrito a la Presidencia del Consejo de Ministros, encargado a nivel nacional de la supervisión y fiscalización del aprovechamiento sostenible y la conservación de los recursos forestales y de fauna silvestre, así como de los servicios ambientales provenientes del bosque;

Que, por Decreto Supremo N° 065-2009-PCM, se aprueba el Reglamento de Organización y Funciones – ROF, del Organismo de Supervisión de los Recursos Forestales y de Fauna Silvestre, el cual determina su estructura orgánica y las funciones generales y específicas del mismo, y de cada uno de sus órganos y de sus unidades orgánicas así como de las relaciones de coordinación y control entre órganos y entidades cuando corresponda;

Que, acorde a lo establecido en el artículo 29º del Reglamento indicado, es función de la Oficina de Tecnología de la Información el conducir el desarrollo, implementación, operación, mantenimiento y seguimiento de los sistemas de información y otros vinculados a las funciones del OSINFOR, garantizando su seguridad y confiabilidad;

Que, con Resolución Presidencial N° 183-2010-OSINFOR se aprobó la Directiva N° 001-2010-OSINFOR/SG/OTI, denominada "Normas y Procedimientos para el Uso Adecuado de los Recursos Informáticos del OSINFOR", con la finalidad de garantizar la seguridad e integridad de la información almacenada en los sistemas informáticos y proporcionar al usuario los procedimientos de gestión para el uso adecuado de los recursos informáticos;

Que, con Resolución Presidencial N° 063-2015-OSINFOR, se oficializaron el Informe de Diagnóstico del Sistema de Control Interno del OSINFOR y el Plan de Trabajo para la Implementación del Sistema de Control Interno en el OSINFOR, que establecen la necesidad de actualizar las normas y procedimientos para el uso adecuado de los recursos informáticos del OSINFOR;

Que, consiguientemente, la Oficina de Tecnología de la Información, a través del Memorándum Nº 195-2016-OSINFOR/05.1, dando cumplimiento a la necesidad de actualizar las normas y procedimientos para el uso adecuado de los recursos informáticos del OSINFOR, ha elaborado el proyecto de Directiva Nº 001-2016-OSINFOR/05.1, denominada: "Lineamientos para el uso de los recursos informáticos en el Organismo de Supervisión de los Recursos Forestales y de Fauna Silvestre – OSINFOR", sustentado en el Informe N° 009-2016-OSINFOR/05.1-JPB;

Que, en ese sentido, la Jefa (e) de la Oficina de Planeamiento y Presupuesto a través del Memorándum Nº 538-2016-OSINFOR/04.1, hace suyo el Informe N°046-2016-OSINFOR/04.1.1, el cual opina, entre otros, que el proyecto de Directiva Nº 001-2016-OSINFOR/05.1, denominada: "Lineamientos para el uso de los recursos informáticos en el Organismo de Supervisión de los Recursos Forestales y de Fauna Silvestre – OSINFOR", se enmarca en el Producto/Tarea: 4.01 "Elaboración de documentos de gestión informática (Directivas, POI, Inventario y plan de contingencia)", del Plan Operativo Institucional - POI 2016 reformulado I (aprobado mediante Resolución Presidencial N° 028-2016-OSINFOR), y se encuentra alineado al Objetivo Estratégico General: "Garantizar la calidad de las supervisiones y fiscalizaciones en los títulos habilitantes, adoptando medidas fundadas en la Ley y los Principios del uso sostenible nacional e internacionalmente reconocidos";

Que, conforme al numeral 9.4 del artículo 9º del Reglamento de Organización y Funciones – ROF, del Organismo de Supervisión de los Recursos Forestales y de Fauna Silvestre, es función del Presidente Ejecutivo emitir las directivas en el ámbito de su competencia;

Que, mediante el Informe Legal N° 101-2016-OSINFOR/04.2, la Oficina de Asesoría jurídica emitió opinión favorable recomendando la aprobación de la Directiva indicada;

Con las visaciones del Secretario General (e), y de los Jefes (e) de la Oficina de Tecnología de la Información y de la Oficina de Asesoría Jurídica, y;

De conformidad con lo dispuesto en el Decreto Legislativo N.º 1085, Ley que crea el Organismo de Supervisión de los Recursos Forestales y de Fauna Silvestre - OSINFOR y su Reglamento de Organización y Funciones, aprobado por Decreto Supremo N.º 065-2009-PCM;

REPUBLICA DEL PERU

SE RESUELVE:

ARTÍCULO 1°.- APROBAR la Directiva N° 001-2016-OSINFOR/05.1 "Lineamientos para el uso de los recursos informáticos en el Organismo de Supervisión de los Recursos Forestales y de Fauna Silvestre – OSINFOR", el mismo que como anexo forma parte integrante de la presente resolución.

ARTÍCULO 2°.- La Directiva N° 001-2016-OSINFOR/05.1 "Lineamientos para el uso de los recursos informáticos en el Organismo de Supervisión de los Recursos Forestales y de Fauna Silvestre – OSINFOR" entrará en vigencia al día siguiente de la publicación de la presente resolución presidencial en el portal institucional del OSINFOR.

ARTÍCULO 3°.- Dejar sin efecto la Directiva N° 001-2010-OSINFOR/SG/OTI "Normas y Procedimientos para el Uso Adecuado de los Recursos Informáticos del OSINFOR", aprobada por Resolución Presidencial N° 183-2010-OSINFOR.

ARTÍCULO 4°.- NOTIFICAR la presente resolución presidencial y sus anexos a todos los órganos y unidades orgánicas del Organismo de Supervisión de los Recursos Forestales y de Fauna Silvestre – OSINFOR, para su conocimiento.

ARTÍCULO 5°.- ENCARGAR a la Oficina de Tecnología de la Información la publicación de la presente resolución presidencial y sus anexos en el Portal Institucional del Organismo de Supervisión de los Recursos Forestales y de Fauna Silvestre – OSINFOR (www.osinfor.gob.pe).

Regístrese y comuníquese,

MÁXIMO SALAZAR ROJAS
Presidente Ejecutivo (e)
Organismo de Supervisión de los Recursos
Forestales y de Fauna Silvestre -OSINFOR

DIRECTIVA N° 001-2016-OSINFOR/05.1

LINEAMIENTOS PARA EL USO DE LOS RECURSOS INFORMÁTICOS EN EL ORGANISMO DE SUPERVISIÓN DE LOS RECURSOS FORESTALES Y DE FAUNA SILVESTRE - OSINFOR

I. OBJETIVO

Establecer lineamientos para el uso adecuado de los recursos informáticos en el OSINFOR.

II. FINALIDAD

Garantizar la seguridad e integridad de la información institucional que está almacenada en los equipos y sistemas informáticos, y optimizar la disponibilidad de los recursos informáticos para el cumplimiento de las funciones del personal del OSINFOR.

III. BASE LEGAL

- Ley N° 27444, Ley del Procedimiento Administrativo General
- Decreto Legislativo N° 822, Ley sobre el Derecho de Autor
- Ley N° 30096, Ley de Delitos Informáticos
- Ley N° 30171, Ley que modifica la Ley N° 30096
- Ley N° 28716, Ley de Control Interno de las entidades del Estado
- Resolución de Contraloría General N° 320-2006-CG, Normas de Control Interno
- Resolución Presidencial N° 063-2015-OSINFOR, que oficializa el Informe de Diagnóstico del Sistema de Control Interno del OSINFOR y el Plan de Trabajo para la Implementación del Sistema de Control Interno en el OSINFOR
- Decreto Legislativo N° 1085 – Ley que crea el Organismo de Supervisión de los Recursos Forestales y de Fauna Silvestre – OSINFOR
- Decreto Supremo Nº 024-2010-PCM, Reglamento del Decreto Legislativo N° 1085
- Decreto Supremo N° 065-2009-PCM, que aprueba el Reglamento de Organización y Funciones del Organismo de Supervisión de los Recursos Forestales y de Fauna Silvestre – OSINFOR
- Resolución Presidencial N° 135-2010-OSINFOR, que aprueba el Manual de Organización y Funciones del Organismo de Supervisión de los Recursos Forestales y de Fauna Silvestre – OSINFOR
- Resolución Presidencial N° 068-2013-OSINFOR, que aprueba el Manual de Procesos y Procedimientos – MAPRO de la Oficina de Tecnología de la Información
- Resolución Presidencial N° 124-2015-OSINFOR, que aprueba el Reglamento Interno de los Servidores Civiles del Organismo de Supervisión de los Recursos Forestales y de Fauna Silvestre – OSINFOR
- Resolución Ministerial Nº 246-2007-PCM, Aprueba uso obligatorio de la Norma Técnica Peruana "NTP-ISO/IEC 17799:2007 EDI. Tecnología de la Información. Código de buenas prácticas para la gestión de la seguridad de la información. 2a. Edición" en todas las entidades integrantes del Sistema Nacional de Informática.

PRESIDENCIA DEL CONSEJO DE MINISTROS
V°B°
OSINFOR
OFICINA DE TECNOLOGÍA DE LA INFORMACIÓN

- Resolución Ministerial N° 129-2012-PCM, Aprueba el uso obligatorio de la Norma Técnica Peruana "NTP-ISO/IEC 27001:2008 EDI Tecnología de la Información. Técnicas de Seguridad. Sistemas de gestión de seguridad de la Información. Requisitos" en todas las entidades integrantes del Sistema Nacional de Informática
- Resolución N° 129-2014/CNB-INDECOPI, Aprueba 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", que reemplaza a la NTP-ISO/IEC 27001:2008 (revisada el 2013).
- Resolución Ministerial Nº 004-2016-PCM, Aprueban 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.
- Decreto Supremo N° 050-2006-PCM, Prohíben en las entidades del Sector Público la impresión, fotocopiado y publicaciones a color para efectos de comunicaciones y/o documentos de todo tipo
- Decreto Supremo N° 009-2009-MINAM, Medidas de Ecoeficiencia para el Sector Público
- Decreto Supremo Nº 011-2010-MINAM, Modifican artículos del Decreto Supremo Nº 009-2009-MINAM
- Guía de Ecoeficiencia para Instituciones Públicas 2012, aprobada por el MINAM.
- Ley N° 29733, Ley de Protección de Datos Personales
- Decreto Supremo N° 003-2013-JUS, Aprueba Reglamento de la Ley Nº 29733, Ley de Protección de Datos Personales
- Resolución Directoral Nº 019-2013-JUS/DGPDP, Aprueba la Directiva de Seguridad de la Información Administrada por los Bancos de Datos Personales
- Resolución Presidencial N° 033-2013-OSINFOR, Conforma el Comité de Gestión de Seguridad de la Información del OSINFOR
- Resolución Presidencial N° 129-2015-OSINFOR, Designa al coordinador que hará las veces de Oficial de Seguridad de la Información del OSINFOR.
- Resolución Presidencial N° 017-2016-OSINFOR, Conforma el Comité de Gestión de Seguridad de la Información del OSINFOR
- Política de Seguridad de la Información (SGSI-006-Politica_de_Seguridad.docx), aprobada por el Comité de Gestión de Seguridad de la Información del OSINFOR.
- Resolución Ministerial N° 150-2006-PCM, "Lineamientos para la formulación y aprobación de directivas de la Presidencia del Consejo de Ministros"
- Resolución Presidencial N° 100-2012-OSINFOR, Aprobar la Directiva N° 001-2012-OSINFOR "Normas para la Generación de Documentos Oficiales en el Organismo de Supervisión de los Recursos Forestales y de Fauna Silvestre – OSINFOR"
- Resolución Presidencial N° 112-2012-OSINFOR, Aprobar la Directiva N° 005-2012-OSINFOR/01.1 "Normas y procedimientos para el oportuno registro, control, uso adecuado, custodia física y seguridad de los bienes muebles del Organismo de Supervisión de los Recursos Forestales y de Fauna Silvestre – OSINFOR"

PRESIDENCIA DEL CONSEJO DE MINISTROS
V°B°
OSINFOR
OFICINA DE TECNOLOGÍA DE LA INFORMACIÓN

IV. ALCANCE

La presente Directiva es de aplicación a todo el personal del OSINFOR, incluyendo a los practicantes preprofesionales y profesionales así como a los contratistas y terceros que hagan uso de los recursos informáticos del OSINFOR.

V. DISPOSICIONES GENERALES

5.1. LINEAMIENTOS GENERALES

a. La Oficina de Tecnología de la Información (OTI) es el órgano encargado de supervisar el cumplimiento de esta Directiva. Cualquier acto de infracción se comunicará a la Dirección u Oficina respectiva, para el inicio de las acciones que correspondan.
b. Los recursos 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 usuario responsable.
c. Los usuarios deben utilizar los recursos informáticos del OSINFOR de manera responsable y ética, cuidando la integridad de los equipos e instalaciones, con respeto a los otros usuarios, a los acuerdos y contratos con terceros y a la legislación vigente.
d. La información de propiedad del OSINFOR, así esté almacenada en dispositivos electrónicos e informáticos pertenecientes o arrendados por el OSINFOR, el usuario o una tercera parte, sigue siendo propiedad únicamente del OSINFOR. El usuario debe asegurarse de que la información del OSINFOR esté protegida de acuerdo con la Política de Seguridad de la Información del OSINFOR.
e. El OSINFOR se reserva el derecho a auditar sistemas y redes periódicamente y/o en cualquier momento para asegurar el cumplimiento de esta directiva.
f. Los equipos informáticos no deberán ser desplazados de un lugar a otro sin el conocimiento de la Oficina de Tecnología de la Información y la autorización de la Sub Oficina de Logística, de acuerdo a los lineamientos y procedimientos en la normativa institucional vigente.
g. La Oficina de Tecnología de la Información es la única autorizada a efectuar la instalación y reinstalación de software.
h. La Oficina de Tecnología de la Información es la única autorizada a abrir los equipos informáticos.
i. 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, como parte de su entrega de cargo, cuando concluya la relación laboral o sea destacada a otra unidad orgánica. Está prohibido eliminar o adulterar archivos de trabajo. El incumplimiento de esta disposición dará lugar a las acciones civiles o penales correspondientes o a sanciones internas, dependiendo del caso.

5.2. USO NO ACEPTABLE

Bajo ninguna circunstancia está autorizado un servidor del OSINFOR a involucrarse en cualquier actividad que sea ilegal de acuerdo a la legislación y normativas vigentes mientras utiliza recursos de propiedad del OSINFOR.

Las siguientes actividades están, en general, prohibidas, pero pueden existir excepciones por una legítima necesidad de la institución (por ejemplo, el personal de la Oficina de Tecnología de la Información puede necesitar deshabilitar el acceso a red de un equipo si este está interfiriendo con servicios en producción).

Las listas a continuación no son exhaustivas, pero intentan brindar un marco de las actividades que caen dentro de la categoría de uso inaceptable.

a. Violaciones de los derechos de cualquier persona natural o jurídica protegida por leyes y regulaciones de derechos de autor, secreto comercial, patentes u otra propiedad intelectual, o similares, lo cual incluye, pero no está limitado a, la instalación o distribución de productos de software "pirata" u otros que no estén apropiadamente licenciados para su uso por el OSINFOR.
b. La copia no autorizada de material sujeto a derechos de autor, incluyendo, pero sin limitarse a, la digitalización y distribución de fotografías de revistas, libros u otras fuentes sujetas a derechos de autor, música sujeta a derechos de autor, y la

instalación de cualquier software para el cual el OSINFOR no tenga una licencia activa.

c. Acceder a datos, servidores o cuentas de usuario para cualquier propósito fuera de las labores del OSINFOR, incluso si cuenta con acceso autorizado.
d. La exportación de software, información técnica, software o tecnología de encriptación en violación de las leyes internacionales o regionales de control de exportaciones.
e. La introducción de programas maliciosos en las redes o servidores (por ej., virus, gusanos, troyanos, etc.).
f. Revelar la contraseña de sus cuentas a otros o permitir el uso de sus cuentas por otros. Esto incluye a los familiares u otros miembros del hogar cuando se realice trabajo en casa.
g. Utilizar un recurso informático del OSINFOR para participar activamente en la obtención y transmisión de material que viole las leyes sobre acoso sexual y hostilidad laboral.
h. Hacer ofertas fraudulentas de productos, artículos o servicios desde cualquier cuenta del OSINFOR.
i. Realizar brechas de seguridad o disrupciones de la comunicación en red. Las brechas de seguridad incluyen, pero no se limitan a, acceder a datos no destinados al usuario, o ingresar a un servidor o cuenta para la cual el usuario no cuenta con autorización expresa, a menos que esto sea parte del alcance de sus labores ordinarias. Para los propósitos de este documento, el término "disrupción" incluye pero no está limitado a inspección de paquetes de red, suplantación de paquetes, denegación de servicio e información falsificada de enrutamiento con propósitos maliciosos.
j. El escaneo de puertos o de vulnerabilidades es actividad exclusiva de la Oficina de Tecnología de la Información y está expresamente prohibido a menos que sea necesario para las labores institucionales y se cuente con la autorización y coordinación previa con el Oficial de Seguridad de la Información y la Oficina de Tecnología de la Información
k. Ejecutar cualquier forma de monitoreo de red que intercepte datos no dirigidos a la estación del usuario, a menos que esta actividad sea parte de las labores normales del usuario, controlada y autorizada por la Oficina de Tecnología de la Información.
l. Eludir la autenticación o seguridad de usuario de cualquier estación, red o cuenta.
m. Utilizar cualquier programa/script/comando, o enviar mensajes de cualquier tipo, con la intención de interferir o deshabilitar la sesión de un usuario, vía cualquier medio, localmente o a través de Intranet/Internet/Extranet.
n. Envío de mensajes de correo electrónico no solicitado, incluyendo el envío de "correo basura" u otro material publicitario a individuos que no lo han requerido específicamente (spam).
o. Cualquier forma de acoso vía correo electrónico, teléfono o mensajería, sea a través del lenguaje empleado, frecuencia o volumen de los mensajes.
p. Uso no autorizado o manipulación de la información de las cabeceras de correo electrónico.
q. Creación o retransmisión de "cartas cadena", esquemas "Ponzi" o "piramidales" de cualquier tipo.

VI. DISPOSICIONES ESPECÍFICAS

6.1. SOBRE LA SEGURIDAD DE LA INFORMACIÓN

a. El usuario debe asegurar sus equipos informáticos (mediante bloqueo de pantalla o cierre de sesión) siempre que necesite ausentarse por un tiempo indefinido de su puesto de trabajo.
b. Los equipos informáticos deben ser apagados completamente al finalizar la jornada laboral.

c. Las computadoras portátiles deben ser protegidas con un cable de seguridad o guardadas bajo llave.
d. Los medios de almacenamiento removibles como CDROM, DVD o unidades USB deben ser considerados como sensibles y almacenados bajo llave.
e. Las impresiones deben ser retiradas de las impresoras tan pronto como sean impresas; esto ayuda a asegurar que los documentos sensibles dejados en las bandejas de las impresoras no sean cogidos por las personas incorrectas.
f. La Oficina de Tecnología de la Información realizará periódicamente el respaldo de la información en los servidores de los Centros de Datos de la institución. El usuario debe almacenar la información crítica en las carpetas compartidas en red que correspondan a su unidad orgánica. El usuario puede también solicitar el apoyo de la Oficina de Tecnología de la Información para obtener su propia copia de seguridad, para lo cual puede solicitar el apoyo de la Oficina de Tecnología de la Información. 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). La OTI está facultada a eliminar esta información sin previo aviso.
g. Todo archivo que provenga del exterior, 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 de la Oficina de Tecnología de la Información. El equipo no debe volver a ser utilizado hasta que el personal de la OTI haya confirmado la solución a la incidencia de seguridad.

6.2. SOBRE LA CONSTRUCCIÓN Y PROTECCIÓN DE CONTRASEÑAS

6.2.1. LINEAMIENTOS DE CONSTRUCCIÓN DE CONTRASEÑAS

a. Las contraseñas deben contener al menos 8 caracteres (se recomienda emplear al menos 12 caracteres).
b. Las contraseñas deben cumplir los siguientes requisitos mínimos de complejidad:
   - 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: *, !, $, #, %)
   - No contener el nombre de cuenta del usuario o partes del nombre completo del usuario en más de dos caracteres consecutivos
c. Las contraseñas débiles suelen tener las siguientes características que deben evitarse:
   - Pueden ser encontradas en un diccionario, incluso de idiomas extranjeros, o pertenecen a una jerga o dialecto
   - Contienen información personal como fechas de nacimiento, direcciones, números telefónicos o nombres de parientes, mascotas, amigos y personajes de fantasía.
   - Contienen información relacionada con el trabajo como nombres de edificio, comandos de sistemas, sitios, compañías, hardware o software.
   - Contienen patrones como **aaaabbb**, **qwerty**, **zyxwvuts**, o **123321**.
   - Contienen palabras comunes deletreadas hacia atrás, o precedidas o seguidas por un número (por ejemplo, **oterces**, **secreto1** o **1secreto**).
d. Se recomienda utilizar frases en lugar de palabras individuales. Las frases de contraseña son similares a las contraseñas de una sola palabra; sin embargo, al ser comparativamente más largas y ser construida con varias palabras, brindan mayor seguridad contra ataques de diccionario. Las frases de contraseña fuertes deben seguir las mismas pautas generales de construcción de contraseñas e incluir letras mayúsculas, minúsculas, números y caracteres especiales (por ejemplo, **ElTraficoEnJavierPradoEstuvoHorribleALa1DeLaTarde!**).

PRESIDENCIA DEL CONSEJO DE MINISTROS
V°B°
OSINFOR
OFICINA DE TECNOLOGÍA DE LA INFORMACIÓN

6.2.2. PROTECCIÓN DE CONTRASEÑAS

a. Los usuarios no deben utilizar la misma contraseña para cuentas del OSINFOR que para otros accesos que no sean del OSINFOR (por ejemplo, cuentas personales de Internet, correo web, etc.)
b. Todas las contraseñas de usuario (por ejemplo, correo electrónico, aplicaciones web, computadora de escritorio) deben ser cambiadas al menos cada TRES meses.
c. Periódica o aleatoriamente, la OTI puede realizar pruebas de descifrado de contraseñas. Si durante una de estas pruebas se consigue descifrar una contraseña, se requerirá que el usuario la cambie en cumplimiento de los lineamientos de construcción de contraseñas.
d. Las contraseñas no deben ser compartidas con nadie. Todas las contraseñas deben ser tratadas como información sensible y confidencial del OSINFOR.
e. Las contraseñas no deben ser insertadas en mensajes de correo electrónico o cualquier otra forma de comunicación electrónica.
f. Las contraseñas no deben ser reveladas telefónicamente a nadie.
g. No revele contraseñas en cuestionarios o formularios.
h. No brinde indicios del formato de una contraseña (por ejemplo, "mi apellido").
i. Cuando esté de vacaciones, no comparta las contraseñas del OSINFOR con nadie, incluyendo asistentes administrativos, secretarias, jefes o colegas, ni familiares.
j. No escriba las contraseñas ni las almacene en cualquier parte de su oficina. No almacene contraseñas en un archivo en un sistema informático o dispositivo móvil (teléfono, tableta) sin encriptación.
k. No utilice la característica "Recordar contraseña" de las aplicaciones (por ejemplo, navegadores web).
l. Cualquier usuario que sospeche que su contraseña pueda haber sido comprometida, debe reportar el incidente de inmediato y cambiar todas sus contraseñas.
m. La OTI podrá generar y utilizar contraseñas iniciales cuando se creen cuentas nuevas o mientras se realice la configuración inicial de un equipo, pero estas contraseñas deberán ser modificadas inmediatamente por el propio usuario. Cualquier modificación futura también deberá ser realizada por el mismo usuario. Solo por razones de soporte técnico, y de ser estrictamente necesario, el usuario podrá brindarle sus credenciales al personal de la OTI. Una vez superada la incidencia que ocasionó la necesidad de que revelara sus credenciales al personal de la OTI, el usuario debe modificarlas.
n. En el caso de los sistemas que cuenten con la funcionalidad de expiración automática de contraseñas tras un periodo de vigencia, el usuario deberá comunicarse con la OTI para el desbloqueo de la cuenta correspondiente.
o. En el caso de que un usuario olvide una contraseña, la OTI lo asistirá para su modificación. Se asistirá a realizar la modificación de la contraseña de una cuenta solo por solicitud directa del usuario titular, o por indicación y autorización expresa de su jefe inmediato.

6.3. SOBRE LOS EQUIPOS INFORMÁTICOS

a. Los equipos informáticos se asignarán a sus respectivos usuarios, quienes son responsables de su cuidado y debida utilización debiendo asumir el resarcimiento de los daños y perjuicios que pudiesen ocasionar por negligencia o la indebida manipulación. Cada usuario es responsable de las atenciones preventivas básicas a 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.
b. Los usuarios no deben, bajo responsabilidad, manipular los equipos informáticos (abrirlos, cambiar componentes, insertar dispositivos), siendo pasibles, en caso de

daño a los equipos, de la sanciones que al respecto establezca el OSINFOR. El jefe inmediato debe velar por el cumplimiento de la presente disposición y disponer las directrices pertinentes al personal a su cargo. En caso de atascamiento de papel o mensajes de advertencia en los equipos de impresión, se debe comunicar a la Oficina de Tecnología de la Información.

c. Está prohibido guardar equipos informáticos que no se estén usando. Todo equipo informático que no esté en uso deberá ser puesto a disposición de la Sub Oficina de Logística, con conocimiento de la Oficina de Tecnología de la Información, para su distribución según las necesidades técnicas de la institución.
d. 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.
e. Todos los equipos deben contar con un protector de sobretensión (no solo tomacorrientes eléctricos) o UPS (respaldo de baterías) adecuados y de buena calidad.
f. Cada usuario debe encender y apagar correctamente todos los equipos informáticos y componentes asignados para el cumplimiento de sus funciones. Nunca se debe mover equipos informáticos ni desconectar bruscamente los cables de energía eléctrica cuando estén encendidos.
g. Si se observa alguna anomalía durante los procesos de encendido y apagado, se debe comunicar a la Oficina de Tecnología de la Información.
h. 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 las estaciones que posean UPS, el tiempo en batería le permitirá al usuario 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 sus equipos.

6.4. SOBRE LAS APLICACIONES INFORMÁTICAS

a. El software de base que se instalará en las estaciones de trabajo del OSINFOR es el siguiente:
- Sistema operativo: Microsoft Windows o equivalente
- Suite ofimática: Microsoft Office Standard o equivalente
- Software antivirus
- Navegadores web
- Lector de archivos PDF
- Compresor de archivos
- Software SIG (supervisores forestales y de fauna silvestre, especialistas de Geomática y personal autorizado)
- Software de diseño gráfico (especialistas en diagramación, comunicaciones, imagen institucional y personal autorizado)
- Software de desarrollo de sistemas (analistas de sistemas, programadores y personal autorizado)

b. La instalación de software adicional solo será posible cuando se adquieran sus respectivas licencias, las mismas que deberán contar con el visto bueno de la Oficina de Tecnología de la Información. Las solicitudes de productos de software serán canalizadas a través de la Oficina de Administración, la que tramitará su adquisición previa evaluación y opinión técnica por parte de la Oficina de Tecnología de la Información respecto a las características y especificaciones requeridas, de acuerdo a las normas y procedimientos vigentes del OSINFOR.
c. La Oficina de Tecnología de la Información conservará los medios de instalación y manuales originales.
d. Está prohibida la instalación de software sin licencia por parte del usuario. Se efectuarán revisiones periódicas del software instalado en los equipos.
e. El personal del OSINFOR no deberá obtener o enviar software ilegal a través de Internet.

PRESIDENCIA DEL CONSEJO DE MINISTROS
V°B°
OSINFOR
OFICINA DE TECNOLOGÍA DE LA INFORMACIÓN

f. La OTI administrará y hará seguimiento de las licencias, probará si existen conflictos e incompatibilidades entre el nuevo software y las aplicaciones existentes, y realizará la instalación.

6.5. SOBRE LOS SERVICIOS DE INTERNET Y TELEFONÍA FIJA

a. Los servicios de Internet y telefonía fija deben ser utilizados exclusivamente para las labores del OSINFOR.
b. Se encuentra prohibido para todos los usuarios los siguientes actos al utilizar el servicio de Internet:
   - Descargar o acceder a sitios de música o videos, y 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.
   - 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.
   - Utilizar sitios web o aplicaciones de chat y mensajería instantánea.
c. Cada usuario 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 computadora y/o cuenta de usuario asignada.
d. Está prohibido conectarse a redes inalámbricas internas sin la autorización del jefe inmediato y la OTI. Esta acción debe ser realizada por el personal de la OTI.
e. La Oficina de Tecnología de la Información en coordinación con la Sub Oficina de Logística 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.
f. El usuario que, para el cumplimiento de sus funciones, necesite accesos adicionales a Internet, o autorización para llamadas telefónicas, deberá sustentarlo ante su jefe inmediato, quien solicitará dicho acceso a la OTI.

6.6. SOBRE EL SERVICIO DE CORREO ELECTRÓNICO

SUBSECRETARÍA DEL CONSEJO DE MINISTROS
V°B°
OSINFOR
OFICINA DE TECNOLOGÍA DE LA INFORMACIÓN

a. La cuenta de correo electrónico institucional debe ser usada exclusivamente para propósitos relacionados con la labor del OSINFOR.
b. El sistema de correo electrónico del OSINFOR no debe ser utilizado para la creación y distribución de cualquier mensaje perturbador u ofensivo, incluyendo comentarios ofensivos acerca de raza, género, color de cabello, discapacidades, edad, orientación sexual, pornografía, creencias y prácticas religiosas, creencias políticas o país de origen. Los usuarios que reciban cualquier mensaje con este contenido de parte de cualquier otro usuario del OSINFOR deben reportarlo de inmediato a su superior o responsable de unidad orgánica.
c. Los usuarios están prohibidos de configurar el reenvío automático de correos electrónicos del OSINFOR a un sistema de correo electrónico de terceros (ver punto siguiente). Los mensajes individuales que sean individualmente reenviados por el usuario no deben contener información confidencial del OSINFOR.
d. Los usuarios están prohibidos de utilizar sistemas y servidores de almacenamiento de correo electrónico de terceros (tales como Google, Yahoo y Hotmail) para llevar a cabo labores oficiales del OSINFOR, para crear o dejar constancia de cualquier transacción vinculante, o para almacenar o retener mensajes en nombre del OSINFOR. Estas comunicaciones y transacciones deben guiarse a través de los canales apropiados utilizando las normas vigentes del OSINFOR.
e. Por razones de seguridad, los usuarios del OSINFOR no deben tener expectativa de privacidad sobre lo que almacenen, envíen o reciban en el sistema de correo institucional.

f. Excepcionalmente, la OTI puede monitorear los mensajes en el sistema de correo institucional cuando las circunstancias lo ameriten o por disposición superior.
g. Para la creación de los nombres de correo se utilizará la inicial del nombre, seguido por el apellido paterno. Por ejemplo, a un nuevo usuario con nombre **Juan Pérez Fernández** le correspondería la dirección electrónica jperez@osinfor.gob.pe. En el caso de que exista homonimia parcial se agregará la inicial del apellido materno. En el ejemplo anterior, de existir previamente la dirección jperez@osinfor.gob.pe, al nuevo usuario le correspondería la dirección jperezf@osinfor.gob.pe.
h. Los usuarios podrán adjuntar archivos en cada mensaje de correo electrónico hasta el límite técnico determinado por la OTI. En el caso de que la información por ser remitida supere este límite, se debe consultar con la Oficina de Tecnología de la Información la alternativa más adecuada según el caso. Si la información debe remitirse entre áreas de una misma sede, esto puede ser realizado mediante la compartición de una carpeta en red u otro medio de grabación de información.

6.7. SOBRE LAS MEDIDAS DE ECOEFICIENCIA

a. Siempre que sea posible, la impresión de documentos debe realizarse por ambas caras de la hoja de papel.
b. Siempre que sea posible, 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.
c. 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.
d. Los equipos informáticos deben ser apagados y desenchufados cuando no se vayan a utilizar, siempre que sea posible.
e. Los equipos informáticos deben ser apagados durante los períodos de refrigerio. En el caso de que algunos equipos no se puedan apagar por completo, se recomienda que por lo menos se apaguen los monitores.
f. 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.

PRESIDENCIA DEL CONSEJO DE MINISTROS
V°B°
OSINFOR
OFICINA DE TECNOLOGÍA DE LA INFORMACIÓN

VII. DISPOSICIONES COMPLEMENTARIAS

a. Cualquier acción o aspecto no contemplado en la presente Directiva será resuelto por la Oficina de Tecnología de la Información en coordinación con la Alta Dirección.

VIII. RESPONSABILIDADES

La Oficina de Tecnología de la Información, conjuntamente con los Directores y Jefes de las Direcciones y Oficinas del OSINFOR, serán responsables del cumplimiento de lo dispuesto en la presente Directiva.