



# Resolución de Presidencia

N° 125 -2012-INGEMMET/PCD

Lima, 22 AGO. 2012

## CONSIDERANDO:

Que, por Resolución Jefatural N° 088-2003-INEI, publicada en el diario Oficial El Peruano el 03 de Abril del 2003, se aprobó la Directiva N° 005-2003-INEI/DTNP "Normas para el uso del servicio de correo electrónico en las entidades de la Administración Pública", de cumplimiento obligatorio por las entidades del Poder Ejecutivo, Legislativo y Judicial, Organismos Autónomos, Organismos Públicos Descentralizados, Gobiernos Regionales, Locales y Empresas Públicas a nivel nacional; la cual tiene por finalidad normar los procedimientos de gestión de los servicios de correo electrónico en las entidades públicas del país, brindando lineamientos para el uso correcto del servicio de correo electrónico oficial;

Que, por Resolución Ministerial N° 073-2004-PCM, se aprueba la "Guía para la Administración Eficiente del Software Legal en la Administración Pública", documento elaborado coordinadamente por el Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual - INDECOPI y la Oficina Nacional de Gobierno Electrónico e Informática - ONGEI, el cual proporciona lineamientos que deben ser tomados en cuenta por las diversas entidades públicas para la administración de la base instalada de software y de esa manera, poder cumplir efectivamente las obligaciones establecidas en el Decreto Supremo N° 013-2003-PCM, que dicta medidas para garantizar la legalidad de la adquisición de programas de software en entidades y dependencias del Sector Público;

Que, por Resolución Ministerial N° 246-2007-PCM, publicada en el diario oficial El Peruano con fecha 25 de Agosto del 2007, se aprobó el 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; disponiendo que las entidades antes mencionadas, consideren las actividades necesarias en sus respectivos Planes Operativos Informáticos (POI), para su implementación;

Que, por Resolución Ministerial N° 129-2012-PCM, publicada en el diario oficial El Peruano con fecha 25 de Mayo del 2012, se aprobó 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"; estableciéndose en su artículo 3°, que la implementación de los Sistemas de Seguridad de la Información en las entidades integrantes del Sistema Nacional de Informática deberá empezar con la aplicación de Norma Técnica Peruana NTP-USO/IEC 27001:2008 EDI "Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la información. Requisitos", cuyos controles deberán ser implementados de acuerdo a las recomendaciones 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", dispuesto por Resolución Ministerial N° 246-2007-PCM;



Que, estando a lo señalado, resulta necesario dictar disposiciones que permitan preservar la confidencialidad, integridad, oportuna disponibilidad y buen uso de las tecnologías de información en el Instituto Geológico, Minero y Metalúrgico – INGEMMET;

De conformidad con las atribuciones previstas en el Decreto Supremo N° 035-2007-EM, Reglamento de Organización y Funciones del Instituto Geológico Minero y Metalúrgico INGEMMET;

Con el visto bueno de la Secretaría General, Oficina de Sistemas de Información, Oficina de Planeamiento y Presupuesto y Oficina de Asesoría Jurídica;

**SE RESUELVE:**

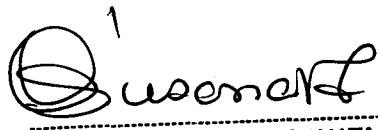
**Artículo Primero.- APROBAR** la Directiva General N° 006-2012-INGEMMET/PCD "Uso de Tecnologías de Información en el Instituto Geológico, Minero y Metalúrgico - INGEMMET".

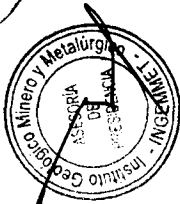
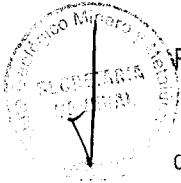
**Artículo Segundo.- DELEGAR** a la Secretaría General del INGEMMET, adoptar las acciones y medidas complementarias que resulten necesarias para la óptima y oportuna consecución de los fines a que se contrae la presente resolución.

**Artículo Tercero.- NOTIFICAR** la presente resolución a la todas las unidades orgánicas del INGEMMET para su conocimiento y fines pertinentes.

**Artículo Cuarto.- ENCARGAR** a la Oficina de Sistemas de Información la publicación de la presente Resolución en el portal institucional.

Regístrese y comuníquese.

  
Ing. SUSANA G. VILCA ACHATA  
Presidenta del Consejo Directivo  
INGEMMET



TRANSCRIPCIÓN:  
Direcciones y Oficinas

## DIRECTIVA N° 006-2012-INGEMMET/PCD

### DIRECTIVA GENERAL

#### USO DE TECNOLOGÍAS DE INFORMACIÓN EN EL INSTITUTO GEOLÓGICO, MINERO Y METALÚRGICO

##### I. OBJETIVO:

Establecer las disposiciones necesarias para regular el uso de tecnologías de información en el Instituto Geológico, Minero y Metalúrgico.

##### II. FINALIDAD

Preservar la confidencialidad, integridad, oportuna disponibilidad y buen uso de las tecnologías de información en el INGEMMET.

##### III. BASE LEGAL

- Resolución Ministerial N° 246-2007-PCM, que aprueba el 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”.
- Resolución Ministerial N° 129-2012-PCM, que 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”.
- Directiva N° 005-2003-INEI/DTNP, “Normas para el uso de Servicio de Correo Electrónico en las Entidades de la Administración Pública”.
- Resolución Ministerial N° 073-2004-PCM, Aprueban Guía para la Administración Eficiente del Software Legal en la Administración Pública.
- Directiva N° 001-2009-INGEMMET-OA-UL, “Medidas de Ecoeficiencia en INGEMMET”.

##### IV. ALCANCE

La presente directiva es de aplicación obligatoria para el personal del INGEMMET, incluyendo Órganos Desconcentrados, sin restricción de su condición laboral o modalidad de servicio. Asimismo, alcanza a los contratistas y terceros que tengan acceso a la información y sistemas de información de la Institución.

##### V. RESPONSABILIDAD

- 5.1 La OSI es responsable del cumplimiento, revisión y actualización de la presente directiva.
- 5.2 Son responsables del cumplimiento de la presente Directiva, todo el personal que presta servicios, cualquiera sea su régimen laboral en el INGEMMET, comprendido en el encargo de puestos o de funciones.
- 5.3 El incumplimiento por parte del usuario de cualquiera de las disposiciones impartidas en la presente directiva, serán comunicadas al Director correspondiente



del área usuaria, a fin de evaluar las sanciones que pudieran aplicarse según la normativa vigente.

## VI. DISPOSICIONES GENERALES

- 6.1 La Oficina de Sistemas de Información, es el órgano responsable de planear, dirigir, ejecutar, controlar las actividades relacionadas a los TICs y velar por el cumplimiento a las Resoluciones Administrativas, Normas y Directivas emitidas por la Alta Dirección del INGEMMET en el ámbito de su competencia.
- 6.2 La Oficina de Sistemas de Información en coordinación con las unidades orgánicas, es la responsable de:
- 6.2.1 El desarrollo y/o implantación del software necesario para el óptimo funcionamiento de las distintas unidades orgánicas del INGEMMET, siendo además responsable de las pruebas de calidad respecto del desarrollo efectuado.
  - 6.2.2 La implementación y administración adecuada de los servicios de redes y comunicaciones; así como, la administración de bases de datos y gestión de seguridad de información debiéndose asegurar su disponibilidad, integridad, confidencialidad y autenticidad.
  - 6.2.3 La asignación de cuentas de acceso a la red informática, y de correo electrónico, debiendo otorgar los recursos informáticos necesarios a los usuarios del INGEMMET.
  - 6.2.4 Efectuar la reproducción, transmisión, distribución o publicación de los Sistemas de Información, software o servicios informáticos o documentación relacionada a tecnologías de la información.
  - 6.2.5 La implementación y administración del servicio de Soporte Técnico informático.
  - 6.2.6 Proponer y coordinar los lineamientos y Términos de Referencia para la adquisición y ejecución de la infraestructura necesaria (hardware y software); así como, la instalación, correcta administración y estandarización de adquisiciones de software, componentes y /o suministros para el equipamiento informático en el INGEMMET.
- 6.3 Es función de la Oficina de Sistemas de Información elaborar las especificaciones técnicas para la adquisición de todo el equipamiento informático y tecnologías de información a adquirirse en el INGEMMET. Toda unidad orgánica que requiera la adquisición de equipamiento informático deberá coordinar con la Oficina de Sistemas de Información.
- 6.4 Es responsabilidad de la Oficina de Sistemas de Información, dentro del ámbito de su competencia, emitir la Conformidad Técnica por la adquisición de recursos y bienes de tecnologías de información.
- 6.5 Los equipos informáticos asignados a los usuarios pueden estar sujetos a controles selectivos en su condición de bienes de la institución, cuando estén usando la red de INGEMMET; para proteger su propiedad y garantizar la óptima y correcta operatividad de los mismos.
- 6.6 Los funcionarios y servidores públicos del INGEMMET, no deben utilizar los recursos informáticos (hardware, software o datos) para otras actividades que no estén directamente relacionadas con las funciones asignadas.
- 6.7 Los equipos informáticos no pueden moverse ni ser reubicados sin conocimiento y autorización de la OSI.
- 6.8 Los usuarios no deben fumar, comer o beber mientras estén utilizando los equipos de cómputo, a fin de proteger la seguridad humana y de equipamiento informático.
- 6.9 Está prohibido divulgar a canales no autorizados la información generada a través de los sistemas de información sin autorización previa de su Dirección o del propietario de la información.



- 6.10 INGEMMET por motivos de seguridad ha dispuesto el uso controlado de memorias de almacenamiento del tipo USB.

## VII. PROCEDIMIENTO.

### 7.1 Sobre el uso de la cuenta de acceso a la red de cómputo

- 7.1.1 La Oficina de Sistemas de Información, es el único órgano de apoyo encargado de validar la adquisición, instalar o configurar los recursos de TIC del INGEMMET.
- 7.1.2 Los funcionarios y trabajadores del INGEMMET que utilizan los servicios TIC deben respetar y no modificar la configuración de hardware y software establecida por personal de soporte técnico o las personas que hagan sus veces. Los usuarios no tendrán privilegios de administrador para el sistema operativo asignado.
- 7.1.3 Para solicitar la generación de una nueva cuenta de acceso a la red de cómputo del INGEMMET, el usuario deberá requerir la creación de la cuenta de usuario y una clave o contraseña de acceso, para lo cual es necesario que el Director responsable de la respectiva Oficina remita a la OSI un correo electrónico solicitando su creación.
- 7.1.4 La OSI procederá a crear el usuario teniendo en cuenta que el nombre de la cuenta de usuario de la red institucional deberá estar conformado por la letra inicial del nombre del usuario, seguido inmediatamente del apellido paterno. En el caso de existir dos construcciones similares, una de ellas llevará después del apellido paterno, la primera letra del apellido materno. Por ejemplo, para el trabajador Roberto Torres Fernández, su cuenta de usuario será RTORRES. Pero también existe el trabajador Raúl Torres Pérez, entonces su cuenta de usuario deberá ser RTORRESP. Para los demás casos particulares, consultar con el "Estándar de Creación de Objetos en el Directorio Activo", publicado en la intranet.
- 7.1.5 Una vez creada la cuenta de usuario y contraseña, los usuarios deberán cambiar la contraseña provisional asignada.
- 7.1.6 Las claves o contraseñas de las cuentas de usuario caducarán cada ciento veinte (120) días calendario.
- 7.1.7 Las contraseñas deberán de cumplir las características mínimas indicadas en el "Manual de Procedimientos de Cambio de Contraseñas", documento publicado en la intranet.
- 7.1.8 Queda prohibido el intento de acceso por parte de los usuarios a recursos no autorizados (base de datos, sistemas de información, etc.).
- 7.1.9 Los perfiles de acceso a los sistemas de información software o servicios informáticos solo deberán ser creados o modificados por la OSI con autorización del Director de la Oficina solicitante.
- 7.1.10 La Unidad de Personal comunicará mensualmente a la OSI el cese de los funcionarios y servidores públicos del INGEMMET, para la revocación de los derechos de acceso correspondientes.

### 7.2 Sobre el desarrollo de software

- 7.2.1 Es función de la Oficina de Sistemas de Información el análisis, diseño, construcción, pruebas e implantación de sistemas alineados a los procesos y objetivos de la institución. Todas las unidades orgánicas que requieran desarrollo de nuevas aplicaciones, deben solicitarlo formalmente, su atención será según priorización del caso.
- 7.2.2 Es función de la Oficina de Sistemas de Información mantener actualizadas las aplicaciones en producción. Todas las unidades orgánicas que

requieran modificación o adecuaciones de los sistemas y/o aplicativos, deben solicitarlo directamente a la Oficina de Sistemas de Información quien evaluará la viabilidad y el impacto que esto genere sobre el conjunto de sistemas de información institucionales.

- 7.2.3 En el caso de que el desarrollo de aplicaciones sea contratado como un servicio de terceros, será supervisado por la Oficina de Sistemas de Información, quien elaborará las Especificaciones Técnicas y posteriormente la Conformidad del Servicio en coordinación con el área usuaria.
- 7.2.4 Esta totalmente prohibido y bajo ninguna circunstancia que el personal técnico de desarrollo tenga acceso a la Base de Datos de Producción para realizar la inserción, modificación y eliminación de registros. El mantenimiento o desarrollo de sistemas debe hacerse en un ambiente de trabajo distinto al ambiente que se opera producción.
- 7.2.5 Todos los aplicativos que se encuentren en producción, deben contar con sus respectivos niveles de accesos y la posibilidad de cambiar las contraseñas de acceso periódicamente.



### **7.3 Sobre el uso de los servidores de cómputo**

- 7.3.1 Los usuarios cuentan con un directorio asignado a su oficina o área en la red, para almacenar la información generada como parte de sus labores. Es responsabilidad del usuario mantenerlo depurado, para lo cual se debe de verificar el documento "Procedimiento de Administración de Carpetas Públicas y Privadas", publicado en la intranet.
- 7.3.2 Este directorio es de uso exclusivo para fines laborales por lo que NO se deben almacenar software, juegos, videos, música, archivos de índole personal entre otros.
- 7.3.3 La OSI mantendrá copias de respaldo de los directorios asignados a los usuarios en el servidor de archivos de acuerdo al instructivo ISO OSI-I-003 "Respaldo de Datos y Recuperación de la Información del INGEMMET".

### **7.4 Sobre el uso de las estaciones de trabajo y portátiles**

- 7.4.1 Los funcionarios y servidores públicos del INGEMMET suscribirán el formato denominado "Ficha de Responsabilidad de Asignación de Bienes patrimoniales", documento elaborado y emitido por la Oficina de Control Patrimonial de la Unidad de Logística, en la cual aceptan las condiciones de uso de lo asignado. Verificar el Procedimiento ISO UL-P-011 "**Registro, Administración y Control de Bienes Muebles**".
- 7.4.2 Los funcionarios y servidores públicos del INGEMMET deberán respetar y no modificar la configuración de hardware ni software establecida por personal de soporte técnico de la OSI.
- 7.4.3 Los usuarios no tendrán privilegios de usuario administrador para el sistema operativo del equipo asignado, a menos que ello sea un requisito indispensable para realizar sus labores, lo cual será sustentado técnicamente por el usuario solicitante.
- 7.4.4 Toda solicitud de instalación de software adicional deberá estar debidamente justificada y autorizada por el Director del usuario solicitante. Una vez aceptada la solicitud, el personal de Soporte Técnico de la OSI procederá a ejecutar la instalación, siempre que exista la disponibilidad de licencias y el equipo cumpla con las características técnicas mínimas requeridas.



- 7.4.5 Se prohíbe que los usuarios de las diferentes unidades orgánicas, instalen software que no sea proporcionado por el INGEMMET con las debidas licencias de uso, bajo responsabilidad.
- 7.4.6 Está prohibida la instalación y uso de software para sistemas de tipo chat, música, videos ó juegos.
- 7.4.7 Los usuarios internos del INGEMMET no podrán utilizar herramientas de hardware o software que podrían ser utilizados para evaluar o comprometer la seguridad de los sistemas de información (escaneo de vulnerabilidades, sniffer de red, entre otros).
- 7.4.8 Los usuarios no podrán copiar el software proporcionado por el INGEMMET en algún medio de almacenamiento (disquete, CD, DVD, memoria de almacenamiento USB, cinta magnética, etc.), transferir o instalar dicho software a otra computadora, o divulgarlo a personas ajenas a la institución.
- 7.4.9 Los usuarios que tienen asignada una computadora son responsables de la información que existe en los discos duros.
- 7.4.10 Todas las computadoras están protegidas con un antivirus corporativo, el mismo que se actualiza diariamente de forma automática. Los usuarios no podrán desactivar o desinstalar el software antivirus instalado.
- 7.4.11 Todos los archivos obtenidos de fuentes externas al INGEMMET, incluyendo archivos copiados en dispositivos magnéticos (diskettes, memorias de almacenamiento USB, etc.), transferidos desde Internet, archivos incluidos en mensajes de correo, archivos provistos por clientes o proveedores, deberán ser revisados por el usuario con el antivirus corporativo instalado en cada equipo de cómputo. En caso el usuario ingrese información sin la revisión correspondiente y afecte la red institucional, asumirá las responsabilidades del caso.
- 7.4.12 Cuando no esté en uso la computadora los usuarios deben asegurar que se encuentre debidamente protegida utilizando una contraseña para el protector de pantalla o bloqueando su sesión haciendo uso simultáneo de las teclas CTRL+ALT+SUPR.
- 7.4.13 Para la reasignación de una computadora a un usuario se debe asegurar su buen funcionamiento, así como el respaldo de la información almacenada en su disco duro para luego proceder al borrado seguro y reinstalación del software necesario para su utilización.
- 7.4.14 Está prohibida la conexión a la red de INGEMMET, mediante computadoras personales portátiles, unidades de almacenamiento extraíbles, equipos de comunicaciones y otros equipos que no pertenezcan al INGEMMET o que no estén incluidos en un contrato de servicios, sin previa coordinación con la OSI y autorización expresa del Director del área respectiva.
- 7.4.15 Para el caso de ingreso de computadoras portátiles de propiedad de los usuarios o de proveedores, se solicitará el permiso al Director del área quien coordinará con la Dirección OSI para la revisión respectiva, de tal forma que no implique un riesgo de seguridad, en conformidad con el Procedimiento OSI-P-022 "Control para el Ingreso de Computadoras Portátiles".
- 7.4.16 Las computadoras personales, portátiles, impresoras y otros que sean trasladados y reubicados por algún motivo justificado deberán ser hechos con conocimiento de la Oficina de Administración a través de la Unidad de Logística – Área de Control Patrimonial- así como los equipos informáticos del INGEMMET, quienes deberán llevar un registro manual o automatizado a fin de informar a la Oficina de Sistemas de Información, el control sobre la reubicación de este tipo de bienes.



## **7.5 Sobre el uso de memorias del Tipo USB**

- 7.5.1 El Instituto Geológico, Minero y Metalúrgico por motivos de seguridad ha dispuesto el uso controlado de memorias de almacenamiento del tipo USB.
- 7.5.2 Para su uso en las computadoras del INGEMMET, estos dispositivos deberán ser revisados por el usuario con el antivirus corporativo instalado en su equipo de cómputo, caso contrario asumirá las responsabilidades del caso.
- 7.5.3 La OSI podrá asignar memorias de de almacenamiento del tipo USB a usuarios autorizados para su uso exclusivo y con fines laborales, siendo responsabilidad del usuario mantenerlo en óptimo estado, caso contrario asumirán el costo del mismo.

## **7.6 Sobre el uso de las impresoras y equipos multifuncionales**

- 7.6.1 Los usuarios están prohibidos de disponer de las impresoras o equipos multifuncionales para otros fines y/o usos que no sean inherentes a sus funciones.
- 7.6.2 Los usuarios están prohibidos de realizar la manipulación, alteración de la configuración, instalación de tóner, cintas o cartuchos en cualquier impresora matricial, inyección, láser o equipo multifuncional de la institución. La OSI es la única oficina autorizada a realizar estas tareas.
- 7.6.3 Los usuarios son responsables del uso correcto de las impresoras y equipos multifuncionales.
- 7.6.4 Se recomienda usar el formato de doble cara y dos (02) hojas por cara para borradores de impresión, de acuerdo a la directiva **001-2009-INGEMMET-OA/UL "Medidas de Ecoeficiencia en INGEMMET"**.

## **7.7 Sobre el servicio de préstamo de computadoras y proyectores.**

- 7.7.1 La OSI dispone de equipos de TI para préstamo. Entre ellos se cuenta con computadoras portátiles y proyectores, los cuales podrán ser prestadas para realizar reuniones o presentaciones.
- 7.7.2 Los usuarios que reciben un equipo en calidad de préstamo serán los responsables de entregar el bien al personal de Soporte Técnico en las mismas condiciones con las que el mismo les fue entregado. Cualquier incidente registrado con los equipos, desde la entrega al usuario hasta la recepción del bien por parte del equipo de Soporte Técnico, será responsabilidad del usuario.
- 7.7.3 En caso estos equipos sean requeridos para su uso fuera de las instalaciones del INGEMMET, los funcionarios y servidores públicos suscribirán el formato denominado "Orden de Salida de Bienes", elaborado y emitida por el Área de Control Patrimonial de la Unidad de Logística, verificando el cumplimiento del Procedimiento ISO UL-P-011 "Registro, Administración y Control de Bienes Muebles".

## **7.8 Sobre el uso del correo electrónico institucional**

- 7.8.1 Los usuarios del INGEMMET previa autorización del Director del área respectiva, son sujetos de asignación de una cuenta de correo electrónico institucional.
- 7.8.2 La OSI es la encargada de la administración del Correo Electrónico, garantizando la integridad, operatividad y confidencialidad de la información.





- 7.8.3 La estructura de la cuenta de correo electrónico esta conformada por el nombre de usuario (descrito en el numeral 7.1 b) seguido del símbolo “@” y el nombre del dominio de Internet “**ingemmet.gob.pe**”.
- 7.8.4 La cuenta de correo electrónico asignada a los usuarios del INGEMMET deberá ser utilizada exclusivamente con propósitos laborales, constituyéndose en responsables de todas las actividades que realicen con su cuenta de correo electrónico.
- 7.8.5 Las cuentas de correo electrónico serán personales e intransferibles, por lo que únicamente pueden ser usadas por los propietarios de las mismas, siendo el poseedor de la clave el responsable directo de la confidencialidad de la contraseña correspondiente.
- 7.8.6 El software cliente de correo electrónico es configurado por la OSI en cada computadora de los usuarios internos del INGEMMET. Éste no deberá ser alterado en su configuración ni mucho menos remplazado por otro software, sin previa coordinación. El usuario deberá considerar el “**Manual de Uso del software de correo electrónico**”, publicado en la intranet.
- 7.8.7 El usuario es responsable de los mensajes de correo electrónico que se descarguen en su computadora, desde el servidor de correo al acceder al servicio. La OSI no realizará bajo ninguna modalidad, copias de seguridad de las casillas de correo de los usuarios en el servidor.
- 7.8.8 Los usuarios son responsables de guardar copias de seguridad de los correos electrónicos almacenados en las carpetas personales del disco duro de la computadora asignada; para ello deberán coordinar con el personal de soporte técnico de la OSI.
- 7.8.9 El uso del correo electrónico institucional puede efectuarse en las instalaciones del INGEMMET o desde Internet a través del Correo Web en la dirección <http://correoweb.ingemmet.gob.pe>, en este último caso tener en cuenta lo siguiente:
- 7.8.9.1 Cada usuario tiene asignado en el servidor de correo, 2 GB de espacio de almacenamiento y 15 MB para enviar o recibir mensajes en su casilla de correo electrónico. Solo a solicitud del Jefe inmediato superior se podrá ampliar este espacio por un periodo de tiempo determinado.
- 7.8.9.2 El usuario deberá depurar constantemente los mensajes de carácter no laboral, para liberar espacio en el servidor y en su cuenta, con el propósito de poder recibir sus mensajes correctamente.
- 7.8.9.3 Todos los mensajes que se envíen fuera del dominio del INGEMMET deberán mostrar un aviso de confidencialidad que señale que la información contenida en los mensajes es privilegiada, confidencial y sólo de interés para el destinatario, de acuerdo al aviso de confidencialidad “Aviso de confidencialidad del Correo Institucional”.
- 7.8.9.4 Los usuarios deberán evitar el uso de las confirmaciones de lectura y de entrega a menos que el mensaje sea muy importante, pues podría generar tráfico en la red.
- 7.8.9.5 Queda prohibido el envío de mensajes cuya información sea del tipo publicitario o que incluya lenguaje inapropiado, declaraciones de discriminación de cualquier tipo, lesivos a la moral, apología del terrorismo, todo tipo de pornografía, amenazas, estafas, esquemas de enriquecimiento piramidal, distribución de malware, actividades político partidarias u otras que se consideren no alineadas con los objetivos de la institución.



- 7.8.9.6 Los correos electrónicos que adjunten documentos que no son propios del remitente, deberán citar siempre la fuente de origen y autores, a fin de respetar los derechos de propiedad intelectual.
- 7.8.9.7 No se deberá responder los mensajes de usuarios desconocidos ya que ello confirma sus direcciones electrónicas y genera correo no solicitado.
- 7.8.9.8 En caso que algún usuario reciba correos de tipo ofensivo proveniente de una cuenta de correo externa, deberá reportarlo a la OSI para su bloqueo y monitoreo correspondientes.
- 7.8.9.9 Se eliminará todos los archivos adjuntos que ingresen al INGEMMET mediante el correo electrónico proveniente de fuente externa, que tengan extensiones de archivos ejecutables (exe, bat, com), u otros archivos similares, debido a que son susceptibles a contener virus informáticos.

## 7.9 Sobre el uso del acceso al INTERNET

- 7.9.1 La OSI es responsable de la administración de los servicios de acceso a Internet, para lo cual podrá hacer uso de herramientas especializadas de monitoreo del uso de Internet a fin de detectar las acciones que realizan con el permiso otorgado, pudiendo restringirse el acceso a determinadas páginas Web y la descarga de archivos por disposiciones de seguridad y uso.
- 7.9.2 Los usuarios están prohibidos de disponer del acceso a Internet para otros fines y/o usos que no sean inherentes al ejercicio de sus actividades laborales.
- 7.9.3 Está prohibido el ingreso a páginas web de música, radio, televisión en línea, chat, juegos, contenido pornográfico, software ilegal, terrorismo, mensajería instantánea en línea. Asimismo, el uso de herramientas para evadir las políticas aplicadas para la navegación en Internet o acceder a sistemas remotos. Para el caso del uso de las redes sociales, se deberá contar con la autorización de director correspondiente.
- 7.9.4 Los usuarios quedan prohibidos de utilizar los servicios proporcionados para uso de Internet para enviar información de INGEMMET a personas no autorizadas.
- 7.9.5 Los usuarios no deben descargar y/o archivar software no autorizado de Internet. Si por razones de sus labores se requiere descargar algún aplicativo o archivo de gran volumen, éste debe ser autorizado por la OSI.
- 7.9.6 Cada usuario del INGEMMET es responsable de las acciones que se ejecuten con su autorización de acceso a Internet.
- 7.9.7 Si un proveedor o consultor externo requiere de uso de Internet por motivos de alguna labor a realizar, el personal de OSI le brindará el acceso requerido utilizando para tal fin una cuenta temporal de uso restringido, para lo cual se requerirá la autorización del Director del área usuaria correspondiente.
- 7.9.8 Queda prohibido realizar conexiones a Internet en las computadoras y equipos portátiles utilizando medios diferentes a los que tiene la institución, a menos que sean autorizados por la OSI.

## 7.10 Sobre el uso de la mensajería interactiva instantánea (CHAT)

- 7.10.1 El uso de mensajería interactiva (Live Messenger MSN, Yahoo Messenger, Google Talk, Skype, etc.) se encuentra prohibido, y solamente será proporcionado a aquellos usuarios que por motivo de sus funciones

requieran hacer uso de esta herramienta, con autorización del Director del área respectiva.

- 7.10.2 La autorización de acceso a este servicio será solicitada por los Directores de cada oficina con la respectiva justificación al Director de la OSI por medio de un correo electrónico.
- 7.10.3 No se debe utilizar la mensajería instantánea para conversaciones de índole privado.
- 7.10.4 No se deberá enviar o recibir archivos utilizando mensajería instantánea.

## 7.11 Sobre el acceso a los ambientes de Tecnologías de la Información

- 7.11.1 El acceso al Centro de Cómputo del INGEMMET debe seguir los lineamientos establecidos en el instructivo ISO OSI-I-007 “Acceso al Data Center del INGEMMET”.
- 7.11.2 Está prohibido el acceso al Almacén de Recursos Informáticos para todo usuario del INGEMMET, excepto al personal de la OSI – Equipo de Soporte Técnico, Redes y Comunicaciones.

## 7.12 Sobre el uso de la telefonía IP

- 7.12.1 Para contar con un equipo telefónico IP, el Director del área respectiva deberá hacer la solicitud mediante documento o correo electrónico al Director OSI.
- 7.12.2 El número de anexo es definido y administrado por la OSI.
- 7.12.3 La bolsa de minutos asignada por usuario o por oficina, está regulado por la Oficina de Administración de acuerdo a la tarificación vigente por el proveedor de servicios.
- 7.12.4 Inicialmente los anexos telefónicos tienen acceso sólo a llamadas internas del INGEMMET. Es potestad de los Directores de las áreas respectivas solicitar a la OSI, atributos adicionales sobre los anexos a su cargo, siempre enmarcados sobre la bolsa de minutos asignada.
- 7.12.5 Los atributos adicionales a las llamadas telefónicas son los siguientes:
  - Fijo local
  - Fijo Nacional
  - Fijo Internacional
  - Celular
  - Celular internacional
- 7.12.6 Cada atributo o grupo de atributos es representado por una clave de cinco (5) dígitos que la OSI asigna a los usuarios responsables.
- 7.12.7 La clave asignada a los usuarios responsables es intransferible, sólo podrá ser cambiada por temas de seguridad a solicitud del Director del área respectiva.
- 7.12.8 Los Directores podrán solicitar a la OSI el reporte de consumo por anexo por clave asignada, del personal a su cargo.

## 7.13 Sobre el uso de los puntos de red

- 7.13.1 Las especificaciones técnicas de los puntos de red estará a cargo de la OSI, por lo que ninguna otra área del INGEMMET instalará ni habilitará puntos de red sin el previo consentimiento.
- 7.13.2 La OSI será responsable de la activación o desactivación de los puntos de red en el Cuarto de Comunicaciones.
- 7.13.3 La OSI mantendrá actualizados los planos de ubicación de puntos de red, rutas del cableado y ubicación de los Cuartos de Comunicaciones.



7.13.4 No se deberá instalar equipos que incremente los puntos de conexiones de red como son los SWITCHES o HUBS ya sea alámbricos o inalámbricos en las oficinas usuarias sin el conocimiento o autorización de la dirección de la OSI. Estos equipos degradan el rendimiento de la red por lo que su instalación deberá ser realizada por especialistas.

7.13.5 No se deberá tender cables de red ni realizar servicios de ampliación de puntos de red sin el conocimiento previo y autorización de la OSI.

#### **7.14 De la Privacidad y Confidencialidad de la Información**

7.14.1 Todos los usuarios del INGEMMET accederán únicamente a la información a la que estén debidamente autorizados.

7.14.2 Los usuarios deberán mantener confidencialidad de la información que creen y/o almacenen, utilizando el equipo informático asignado y los servicios asociados, tanto internos como externos, correo electrónico e Internet solamente para propósitos institucionales.



#### **VIII. DISPOSICIONES FINALES.**

- El incumplimiento por parte del usuario del cualquiera de las disposiciones impartidas en la presente directiva, son consideradas faltas administrativas y serán objeto de sanciones por parte de las instancias pertinentes.
- En caso de producirse alguna infracción por parte de los trabajadores se comunicará al Jefe inmediato superior de la unidad orgánica donde labora el infractor, con copia a la Unidad de Personal de la Oficina de Administración; de ser un funcionario el infractor se comunicará a la Secretaría General.
- La Oficina de Sistemas de Información se encuentra obligada a proporcionar una copia de la presente directiva así como de las Normas o Resoluciones que regulan los aspectos específicos del uso de las Tecnologías de la Información al personal que ingrese a laborar y se solicite la asignación de credenciales para el acceso a la red.
- La presente directiva tiene vigencia desde la fecha de su aprobación y publicación en la página web institucional.



#### **IX. ANEXOS**

##### **Anexo N° 01: Glosarios de Términos**



## ANEXO N° 01

### GLOSARIO DE TÉRMINOS

1. **Acceso autorizado:** Autorización concedida a un usuario para la utilización de los diversos recursos informáticos.
2. **Antivirus:** Programa o software cuya función es detectar y eliminar programas maliciosos (malware) como son virus informáticos, entre otros.
3. **Autenticación:** Procedimiento de comprobación de la identidad de un usuario.
4. **Confidencialidad:** La confidencialidad de la información es la necesidad de que la misma sea conocida solo por personas autorizadas.
5. **Contraseña o clave:** Información confidencial, constituida frecuentemente por una cadena de caracteres, que puede ser usada en la autenticación de un usuario.
6. **Control de acceso:** Mecanismo que en función a la identificación ya autenticada permite acceder a datos o recursos.
7. **Infraestructura TI:** Todo el hardware, software, instalaciones etc. requeridas para desarrollar, probar, proveer, monitorear, controlar o soportar los Servicios de TI.
8. **Dato:** Pueden ser cualquier forma de información como registros, archivos y base de datos, texto, hojas de cálculo, imágenes, video, etc.
9. **Disponibilidad de Información:** Es la capacidad de la información de estar siempre disponible para ser procesada. Para ello, se requiere que se encuentre correctamente almacenada en los formatos preestablecidos y que el hardware que la contiene funcione normalmente.
10. **Equipos Multifuncionales:** Equipos de cómputo que pueden ser utilizados para más de una función, como por ejemplo: scanner, impresora y copiadora.
11. **Identificación:** Procedimiento de reconocimiento de la identidad de un usuario.
12. **Información Confidencial:** Información de los usuarios que pueda comprometer la integridad intelectual y tecnológica de la institución.
13. **Integridad:** Es la característica de la información que hace que su contenido permanezca invariable a menos que sea modificado por una persona autorizada.
14. **Licencia:** Registro obtenido por la compra de un software o hardware, cuya posesión faculta el uso del mismo, estableciendo las reglas básicas para su utilización y sus limitaciones.
15. **Malware:** Conocido también como programa o software malicioso. Tiene como objetivo infiltrarse o dañar la información que se encuentran en las computadoras sin el conocimiento del usuario.



16. **Red Informática:** conjunto de equipos de cómputo que interconecta física y lógicamente para intercambio de información y de recursos informáticos.
17. **Sistema de Información:** es el conjunto independiente de recursos de información organizados para la recopilación, procesamiento, mantenimiento, transmisión y difusión de información, según procedimientos determinados.
18. **Seguridad de la Red Informática:** acciones que permiten identificar, validar, autorizar y realizar el seguimiento de las transacciones que se realizan en la red informática
19. **Software:** Son los componentes lógicos necesarios para hacer posible la realización de una tarea específica en una computadora.
20. **Tecnología de Información (TI):** Se refiere al hardware y software operados por la organización o por un tercero sin tener en cuenta la tecnología utilizada.
21. **Usuario:** Personal del INGEMMET que se encuentra registrado en el sistema informático a través de una cuenta de acceso, cuya validación están determinadas por la aplicación de un usuario y una contraseña.

