SECTOR ENERGÍA Y MINAS
INGEMMET
INSTITUTO GEOLÓGICO, MINERO Y METALÚRGICO

Firmado digitalmente por DIAZ YOSA Victor Manuel FAU 20112919377 hard
Empresa: Instituto Geológico, Minero y Metalúrgico
Motivo: Firma del documento
Fecha: 2022/01/14 16:32:05-0500

Resolución de Presidencia

N° 0004-2022-INGEMMET/PE

Lima, 14 de enero de 2022

VISTOS: Los Memorandos N° 0764-2021-INGEMMET/GG-OSI y N° 0878-2021-INGEMMET/GG-OSI de la Oficina de Sistemas de Información, el Memorando N° 0491-2021-INGEMMET/GG-OPP de la Oficina de Planeamiento y Presupuesto, y el Informe N° 0008-2022-INGEMMET/GG-OAJ de la Oficina de Asesoría Jurídica; y,

CONSIDERANDO:

Que, el Instituto Geológico, Minero y Metalúrgico (en adelante, INGEMMET) es un Organismo Público Técnico Especializado del Sector Energía y Minas, con personería jurídica de derecho público, goza de autonomía técnica, económica y administrativa, constituyendo un Pliego Presupuestal, conforme a lo señalado en el Reglamento de Organizaciones y Funciones, aprobado por Decreto Supremo N° 035-2007-EM (en adelante ROF del INGEMMET);

Que, mediante el artículo 1 de la Ley N° 27658, Ley Marco de Modernización de la Gestión del Estado, declara al Estado peruano en proceso de modernización en sus diferentes instancias, dependencias, entidades, organizaciones y procedimientos, con la finalidad de mejorar la gestión pública y construir un Estado democrático, descentralizado y al servicio del ciudadano. Asimismo, el artículo 4 de la referida Ley señala que el proceso de modernización de la gestión del Estado tiene como finalidad fundamental la obtención de mayores niveles de eficiencia del aparato estatal, de manera que se logre una mejor atención a la ciudadanía, priorizando y optimizando el uso de los recursos públicos;

Que, por su parte el artículo 1 del Decreto Legislativo N° 1412, Decreto Legislativo que aprueba la Ley de Gobierno Digital, dispone que la referida Ley tiene por objeto establecer el marco de gobernanza del gobierno digital para la adecuada gestión de la identidad digital, servicios digitales, arquitectura digital, interoperabilidad, seguridad digital y datos, así como el régimen jurídico aplicable al uso transversal de tecnologías;

Que, asimismo el artículo 6 del mencionado Decreto Legislativo, señala que el gobierno digital es el uso estratégico de las tecnologías digitales y datos en la Administración Pública para la creación de valor público. Se sustenta en un ecosistema compuesto por actores del sector público, ciudadanos y otros interesados, quienes apoyan en la implementación de iniciativas y acciones de diseño, creación de servicios digitales y contenidos, asegurando el pleno respeto de los derechos de los ciudadanos y personas en general en el entorno digital;

Que, por su parte mediante Resolución Ministerial N° 004-2016-PCM, se 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, el cual tiene como objeto especificar los requisitos para establecer, implementar, mantener y mejorar continuamente un sistema de gestión de seguridad de la información, asimismo, incluye requisitos para la evaluación y tratamiento de los riesgos de seguridad de la información;

Que, mediante Resolución de Gerencia General N° 033-2018-INGEMMET/GG de fecha 6 de setiembre de 2018, se aprueba la Directiva General N° 005-2018-INGEMMET/GG "Uso de Tecnologías de Información en el Instituto Geológico, Minero y Metalúrgico- INGEMMET";

Que, de conformidad con el artículo 19 del ROF del INGEMMET, la Oficina de Sistemas de Información es el órgano de apoyo encargado de conducir, desarrollar y actualizar la base de datos geocientífica y jurisdiccional administrativa minera, así como, brindar apoyo y asesoría en materia de software, hardware y sistemas de información en general al personal de la institución;

Que, de acuerdo al citado artículo, la Oficina de Sistemas de Información tiene entre sus funciones la de desarrollar y/o administrar el hardware, software, redes y comunicaciones como base para mantener la operatividad de los sistemas de información institucionales, así como brindar asistencia técnica a la Alta Dirección, y otros órganos del Instituto Geológico Minero y Metalúrgico en aspectos de su competencia, cuando le sean consultados;

Que, mediante los Memorandos N° 0764-2021-INGEMMET/GG-OSI y N° 0878-2021-INGEMMET/GG-OSI de fechas 22 de octubre de 2021 y 17 de diciembre de 2021 respectivamente, la Oficina de Sistemas de Información, remite el Informe N° 0051-2021-INGEMMET/GG-OSI-GRCY que sustenta la extinción de la Directiva General N° 005-2018-INGEMMET/GG "Uso de Tecnologías de Información en el Instituto Geológico, Minero y Metalúrgico - INGEMMET", concluyendo que se ha elaborado el proyecto de Directiva conforme a los lineamientos establecidos en la Directiva General N° 004-2017-INGEMMET/PCD "Lineamientos para la formulación, aprobación, modificación y extinción de Directivas en el Instituto Geológico, Minero y Metalúrgico – INGEMMET"; así como subsana las observaciones finales formuladas por la Oficina de Asesoría Jurídica;

Que, mediante Memorando N° 0491-2021-INGEMMET/GG-OPP, de fecha 03 de noviembre de 2021, la Oficina de Planeamiento y Presupuesto señala que el proyecto normativo Directiva denominada "Uso de Tecnologías de la Información y Comunicación en el Instituto Geológico, Minero y Metalúrgico-INGEMMET", cumple con la estructura y los lineamientos establecidos en la Directiva General N° 004-2017-INGEMMET/PCD "Lineamientos para la formulación, aprobación, modificación y extinción de directivas en el Instituto Geológico, Minero y Metalúrgico – INGEMMET", aprobada mediante Resolución de Presidencia N° 077-2017-INGEMMET/PCD;

Que, mediante Informe N° 0008-2022-INGEMMET/GG-OAJ, de fecha 13 de enero de 2022, la Oficina de Asesoría Jurídica concluye que resulta legalmente viable aprobar la Directiva General denominada "Uso de Tecnologías de la Información y Comunicación en el Instituto Geológico, Minero y Metalúrgico-INGEMMET" y dejar sin efecto la Resolución de Gerencia General N° 033-2018-INGEMMET/GG, que aprueba por delegación la Directiva General N° 005-2018-

INGEMMET/GG "Uso de Tecnologías de Información en el Instituto Geológico, Minero y Metalúrgico- INGEMMET".

Que, en atención a las consideraciones expuestas, resulta necesario emitir el acto resolutivo que apruebe la Directiva General denominada "Uso de Tecnologías de la Información y Comunicación en el Instituto Geológico, Minero y Metalúrgico - INGEMMET" así como corresponde dejar sin efecto la Resolución de Gerencia General N° 033-2018-INGEMMET/GG, que aprueba por delegación la Directiva General N° 005-2018-INGEMMET/GG "Uso de Tecnologías de Información en el Instituto Geológico, Minero y Metalúrgico - INGEMMET";

Con el visado de la Gerencia General, y de las Oficinas de Sistemas de Información, de Planeamiento y Presupuesto, y de Asesoría Jurídica; y,

De conformidad con lo dispuesto en la Ley N° 27658, Ley Marco de Modernización de la Gestión del Estado; el Decreto Legislativo N° 1412, Decreto Legislativo que aprueba la Ley de Gobierno Digital; Resolución Ministerial N° 004-2016-PCM, se 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"; la Resolución de Presidencia N° 077-2017-INGEMMET/PCD, que aprueba la Directiva General N° 004-2017-INGEMMET/PCD "Lineamientos para la formulación, aprobación, modificación y extinción de directivas en el Instituto Geológico, Minero y Metalúrgico - INGEMMET" y el Reglamento de Organización y Funciones del Instituto Geológico, Minero y Metalúrgico - INGEMMET, aprobado por Decreto Supremo N° 035-2007-EM;

SE RESUELVE:

Artículo 1. APROBAR la Directiva General denominada "Uso de Tecnologías de la Información y Comunicación en el Instituto Geológico, Minero y Metalúrgico-INGEMMET", que como Anexo forma parte integrante de la presente Resolución.

Artículo 2. DEJAR SIN EFECTO la Resolución de Gerencia General N° 033-2018-INGEMMET/GG que aprueba la Directiva General N° 005-2018-INGEMMET/GG "Uso de Tecnologías de Información en el Instituto Geológico, Minero y Metalúrgico - INGEMMET".

Artículo 3. DISPONER que la Oficina de Sistemas de Información, realice la difusión, implementación y supervisión de la Directiva General que se aprueba mediante la presente Resolución.

Artículo 4. DISPONER la publicación de la presente resolución y su Anexo en el Portal Institucional del Instituto Geológico, Minero y Metalúrgico- INGEMMET (www.gob.pe/ingemmet).

Regístrese y comuníquese.

SECTOR ENERGÍA Y MINAS
INGEMMET
INSTITUTO GEOLÓGICO, MINERO Y METALÚRGICO

DIRECTIVA N° 001-2022-INGEMMET/PE

DIRECTIVA GENERAL

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

I. OBJETIVO.

Establecer los lineamientos que regulen el uso de tecnologías de la información y comunicación en el Instituto Geológico, Minero y Metalúrgico – INGEMMET.

II. FINALIDAD.

Garantizar la confidencialidad, integridad y la disponibilidad para el buen uso de las tecnologías de la información y comunicación en el INGEMMET, así como las condiciones necesarias para la operación y preservación de los activos de información, en concordancia con la normatividad vigente.

ALCANCE.

La presente Directiva es de cumplimiento obligatorio para todas las Unidades Orgánicas del INGEMMET, sus servidores civiles y funcionarios (en adelante usuarios) independientemente del régimen laboral al que pertenezcan o el vínculo contractual al que se encuentren sujetos.

IV. BASE LEGAL.

4.1. Ley Nº 27291, Ley de modifica el Código Civil permitiendo la utilización de medios electrónicos para la manifestación de la voluntad y utilización de la firma electrónica.
4.2. Ley N° 27269, Ley de Firmas y Certificados Digitales
4.3. Ley N° 27309, Ley que incorpora los Delitos Informáticos al Código Penal.
4.4. Ley N° 27658, Ley Marco de Modernización de la Gestión del Estado.
4.5. Ley N° 28612, Ley que norma el uso, adquisición y adecuación del software en la Administración Pública.
4.6. Ley N° 27815, Ley del Código de Ética de la Función Pública.
4.7. Ley N° 28493, Ley que regula el uso del correo electrónico comercial no solicitado (SPAM).
4.8. Ley N° 29733, Ley de Protección de Datos Personales.
4.9. Ley N° 30096, Ley de Delitos Informáticos.
4.10. Decreto Legislativo N° 1412, Decreto Legislativo que aprueba la Ley de Gobierno Digital.
4.11. Decreto Legislativo N° 822, Ley sobre Derechos de Autor.
4.12. Decreto Supremo N° 082-2019-EF que aprueba el Texto Único Ordenado de la Ley de Contrataciones del Estado.
4.13. Decreto Supremo N° 344-2018-EF que aprueba el Reglamento de la Ley N° 30225, Ley de Contrataciones del Estado.
4.14. Decreto Supremo N° 029-2021-PCM, Decreto Supremo que aprueba el Reglamento del Decreto Legislativo N° 1412, Decreto Legislativo que aprueba la Ley de Gobierno Digital, y establece disposiciones sobre las condiciones, requisitos y uso de las tecnologías y medios electrónicos en el procedimiento administrativo.
4.15. Decreto Supremo N° 021-2019-JUS, que aprueba el Texto Único Ordenado de la Ley N° 27806, Ley de Transparencia y Acceso a la Información Pública.
4.16. Decreto Supremo N° 011-2018-JUS, Decreto Supremo que modifica el Reglamento del

En el presente documento se utilizan de manera inclusiva términos tales como "usuario", "Jefe", "Director" y sus respectivos plurales para referirse a varones y mujeres. Esta opción se basa en una convención idiomática y tiene por objetivo evitar formas complejas de aludir a ambos géneros en el idioma castellano ("o/a", "los/las", "los/las usuarios/as", "los Jefes y las Jefas" "Directores y Directoras" y otras similares), debido a que implican una saturación gráfica que puede dificultar la comprensión lectora.

Siempre con el pueblo

Decreto Legislativo N° 1353, Decreto Legislativo que crea la Autoridad Nacional de Transparencia y Acceso a la Información Pública, fortalece el Régimen de Protección de Datos Personales y la Regulación de la Gestión de Intereses, aprobado por el Decreto Supremo N° 019-2017-JUS.

4.17. Decreto Supremo N° 003-2013-JUS, que aprueba el Reglamento de la Ley N° 29733, Ley de Protección de Datos Personales.

4.18. Decreto Supremo N° 033-2005-PCM, que aprueba el Reglamento de la Ley del Código de Ética de la Función Pública.

4.19. Decreto Supremo N° 072-2003-PCM, que aprueba el Reglamento de la Ley de Transparencia y Acceso a la Información Pública.

4.20. Decreto Supremo N° 024-2006-PCM que aprueba el Reglamento de la Ley N° 28612 Ley que norma el uso, adquisición y adecuación del Software en la Administración Pública

4.21. Decreto Supremo N° 035-2007-EM, que aprueba el Reglamento de Organización y Funciones del Instituto Geológico, Minero y Metalúrgico – INGEMMET.

4.22. Resolución Ministerial Nº 073-2004-PCM, que aprueba la Guía para la Administración Eficiente del Software Legal en la Administración Pública.

4.23. Resolución Ministerial Nº 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.

4.24. Resolución de Contraloría General N° 146-2019-CG, que aprueba la Directiva N° 006-2019-CG/INTEG "Implementación del Sistema de Control Interno en las entidades del Estado".

4.25. Resolución de Contraloría N° 320-2006-CG, que aprueba las Normas de Control Interno.

4.26. Resolución de Presidencia N° 077-2017-INGEMMET/PCD, aprueba la Directiva General N° 004-2017-INGEMMET/PCD, "Lineamientos para la Formulación, Aprobación y Modificación de Directivas en el Instituto Geológico, Minero y Metalúrgico".

4.27. Resolución de Presidencia N° 072-2017-INGEMMET/PCD, que aprueba la Directiva N°003-2017- INGEMMET/PCD, Directiva General "Régimen Disciplinario y Procedimiento Sancionador del INGEMMET"

4.28. Resolución de Secretaria General N° 020-2018-INGEMMET/SG, aprueba la Directiva General "Medidas de Ecoeficiencia en el Instituto Geológico, Minero y Metalúrgico - INGEMMET".

4.29. Resolución de Gerencia General Nº 019-2020-INGEMMET-GG, que aprueba el "Procedimiento para el préstamo de estaciones de trabajo y/o dispositivos periféricos para su utilización fuera del INGEMMET (domicilio del servidor) y sus anexos."

4.30. Resolución Jefatural N° 347-2001-INEI, que aprueba la Directiva "Normas y Procedimientos Técnicos para garantizar la Seguridad de la Información publicadas por las entidades de la Administración Pública".

4.31. Resolución Jefatural N° 088-2003-INEI, que aprueba la Directiva "Normas para el uso del servicio de correo electrónico en las entidades de la Administración Pública ".

Las referidas normas incluyen sus respectivas disposiciones ampliatorias, modificatorias y conexas, de ser el caso.

V. RESPONSABILIDADES.

5.1 Usuario

Cumplir con las disposiciones establecidas en la presente directiva, asumiendo total responsabilidad por el uso y de todo aquello que realice con los activos informáticos

En el presente documento se utilizan de manera inclusiva términos tales como "usuario", "Jefe", "Director" y sus respectivos plurales para referirse a varones y mujeres. Esta opción se basa en una convención idiomática y tiene por objetivo evitar formas complejas de aludir a ambos géneros en el idioma castellano ("o/a", "los/las", "los/las usuarios/as", "los Jefes y las Jefas" "Directores y Directoras" y otras similares), debido a que implican una saturación gráfica que puede dificultar la comprensión lectora.

Siempre con el pueblo

asignados.

5.2 Coordinador Informático
Realiza la gestión, coordinación de requerimientos asociados a los activos informáticos desarrollo y mantenimientos de sistemas y solicitudes.

Solicita la creación, actualización o desactivación de los accesos a los activos informáticos, según las normas internas de personal y la presente directiva, previa aprobación del titular de la unidad orgánica solicitante.

5.3 Oficina de Sistemas de Información (OSI)
Es responsable de operar, monitorear, evaluar, cautelar y capacitar en la correcta utilización de las tecnologías de la información.
Órgano de apoyo encargado de validar la adquisición, instalación o configuración de los activos informáticos.

5.4 El Oficial de Seguridad Digital (CSD)
Es responsable de revisar y controlar la implementación de los lineamientos establecidos en la presente directiva.

.5 Oficina de Unidad de Personal (UP)
Comunicar oportunamente a la OSI sobre el ingreso, ausencia temporal, desplazamiento o cese del personal del INGEMMET, a fin que dicha oficina active o desactive los accesos a los activos informáticos que corresponde.

.6 Titulares de los órganos y unidades orgánicas del INGEMMET
Solicitar la creación, actualización o desactivación de los accesos a los activos informáticos, según las normas internas de personal y la presente directiva.

VI. DISPOSICIONES GENERALES.

6.1 La OSI deberá administrar las Tecnologías de la Información y Comunicación (TIC) y velar por el cumplimiento de la normativa en este ámbito.

6.2 Para realizar cualquier requerimiento mencionado en la presente Directiva será solicitado por su Coordinador Informático, previa aprobación del Director de la Unidad Orgánica; mediante correo electrónico o documento oficial.

Mediante el aplicativo Mesa de Ayuda los usuarios podrán solicitar asistencia técnica a la OSI, previo conocimiento y aprobación de su Coordinador Informático de su respectiva Unidad Orgánica.

6.3 La OSI, en coordinación con las unidades orgánicas, está a cargo de:

6.3.1 El desarrollo o implantación del software necesario de las distintas unidades orgánicas del INGEMMET.

6.3.2 La implementación y administración adecuada de los servicios de redes y comunicaciones; así como, la administración de bases de datos.

6.3.3 La asignación de cuentas de acceso a la red informática y activos informáticos.

6.3.4 La OSI asesora, propone, coordina los lineamientos y elabora las Especificaciones Técnicas o Términos de Referencia para la adquisición, ejecución, instalación, administración y mantenimiento del software, equipamiento informático y las tecnologías de la información del INGEMMET, de acuerdo a la ley de contrataciones con el Estado.

6.3.5 Los servicios solicitados a la OSI se realizarán de acuerdo al cuadro de necesidades aprobado y ejecutado por las unidades orgánicas solicitante. Caso contrario, deberán gestionar el requerimiento ante las instancias correspondientes.

6.3.6 Supervisar y validar la tercerización u outsourcing de bienes o servicios referidos a tecnologías de información y comunicación.

6.4 Es responsabilidad de la OSI, dentro del ámbito de su competencia, emitir la Conformidad Técnica por la adquisición de bienes o contratación de servicios de tecnologías de la información y comunicación.

6.5 Los activos informáticos asignados a los usuarios pueden estar sujetos a controles selectivos de acuerdo a la normativa vigente en su condición de bienes de la entidad, cuando estén usando la red de INGEMMET.

Los controles selectivos de la red interna de INGEMMET son:

6.5.1 Perfil de usuario de acceso a las unidades de Red.
Permite al personal del INGEMMET acceder a la red y a los diferentes sistemas, servicios y activos tecnológicos del INGEMMET; para lo cual se asignará al personal una cuenta de usuario y una contraseña, a fin de darle un uso personal e intransferible velando por su custodia.

6.5.2 Acceso a las Aplicaciones
El usuario líder de una aplicación es el responsable de definir los diferentes perfiles de acceso de un usuario.
Las aplicaciones, que contienen información secreta, reservada o confidencial contarán con bloqueo automático frente a la inactividad de la aplicación por el usuario mayor a 10 minutos o según la necesidad requerida.
El acceso del personal de la Entidad a las aplicaciones listadas en el DTIC-005 Inventario de aplicativos del INGEMMET, es de acuerdo a la función que desempeña; para lo cual se asignará una cuenta de usuario y una contraseña; a finde darle un uso correcto para el desempeño de sus labores.

6.5.3 Perfil de usuario de navegación a internet.
Permite a los usuarios poder navegar en distintas páginas web con fines estrictamente laborales. Con la finalidad de acceder a la información de otras instituciones y aquellas que permitan completar las funciones de las distintas direcciones, órganos y unidades orgánicas del INGEMMET.

Los accesos a internet tendrán diferentes niveles de acceso de acuerdo a los privilegios establecidos, que serán los siguientes:

Nivel de Acceso	Privilegios de Accesibilidad	Tipo de Usuario
A	Acceso para la navegación sin restricciones o filtro alguno (radio de noticias en línea, correo externo, mensajería instantánea, accesos, ftp, etc.) Bajo responsabilidad del usuario durante la navegación.	Presidencia de Consejo Directivo, Miembros del Consejo Directivo, Gerencia General, Asesores de Presidencia.

B	Acceso para la navegación con ciertos filtros de web de categorías y capacidad técnica de enlaces de comunicación como radio, tv en línea. Bajo responsabilidad del usuario durante la navegación.	Directores de Línea y Jefes de Unidades Orgánicas
C	• Acceso a navegación será asignado a los trabajadores que desarrollen labores administrativas u operativas en las unidades orgánicas del INGEMMET. • Los filtros web incluirán redes sociales, radio en línea, juegos, recreación y otros relacionados que se determine. • Se permitirá cierta flexibilidad a usuarios que por labor requieran perfiles menos restrictivos, ello debidamente fundamentado y documentado. • Los perfiles serán creados con restricciones y/o permisos en base a la labor que realizan.	Personal que labora en el INGEMMET
D	• Acceso limitado a internet y correo institucional. • Este perfil será activado para una determinada dependencia (limitado), grupo, comité o usuario, que no va contar con acceso a internet o en todo caso, con acceso a páginas web específicas, la intranet y correo institucional determinadas por la Dependencia y/o OSI. Bajo responsabilidad del usuario durante la navegación.	Otros
E	Acceso limitado a internet	Invitado

6.5.4 Control ANTIVIRUS.

6.6 Los usuarios del INGEMMET no deben utilizar los activos informáticos para otras actividades que no estén directamente relacionadas con las funciones asignadas.

6.7 Los activos informáticos no pueden ser reubicados sin conocimiento previo del coordinador informático o Director; y autorización de la OSI, mediante correo electrónico o documento oficial.

6.8 Los usuarios que ingieran alimentos cerca de los activos informáticos o equipos electrónicos deben tomar medidas de seguridad a fin evitar dar origen a incidentes u ocasionar daños a los activos informáticos. Existe el riesgo grave de electrocución por entrada de agua, aceite o suciedad en los activos informáticos.

En el presente documento se utilizan de manera inclusiva términos tales como "usuario", "Jefe", "Director" y sus respectivos plurales para referirse a varones y mujeres. Esta opción se basa en una convención idiomática y tiene por objetivo evitar formas complejas de aludir a ambos géneros en el idioma castellano ("o/a", "los/las", "los/las usuarios/as", "los Jefes y las Jefas" "Directores y Directoras" y otras similares), debido a que implican una saturación gráfica que puede dificultar la comprensión lectora.

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 Está prohibido realizar copias parciales o totales de información, a través de cualquier dispositivo o medio electrónico, sin la autorización previa de su Director.

VII. DISPOSICIONES ESPECÍFICAS.

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

7.1.1 Los usuarios del INGEMMET que utilizan los servicios de TIC se encuentran prohibidos de modificar la configuración de hardware y software establecido por la OSI. Los usuarios no tienen privilegios de administrador para los sistemas operativos asignados.

7.1.2 Para solicitar acceso a un activo informático el Director o Jefe de la Unidad Orgánica debe remitir a la OSI el Formato "OSI-F-222 Gestión de Accesos a la Red" firmado, pudiendo ser enviado por correo electrónico o documento oficial.

7.1.3 La Oficina de Sistemas de Información atenderá las solicitudes de creación de cuentas de usuarios dentro de las 24 horas de haber recibido dicho formato.

7.1.4 La OSI procede a crear la cuenta de acceso a la red, internet y a las aplicaciones teniendo en consideración el siguiente formato:

Inicial Primer Nombre	Apellido Paterno	@	Dominio
n	mmmm	@	ingemmet.gob.pe

En caso de existir dos usuarios con nombres similares o duplicidad y demás casos particulares, el personal de OSI se regirá según lo establecido en el "DTIC-001 Estándar de Creación de Objetos en el Directorio Activo del dominio INGEMMET.INT", documento digital publicado en la intranet.

7.1.5 Los perfiles de acceso a los activos informáticos solo son creados o modificados por la OSI a solicitud del Director o Jefe de la Unidad Orgánica.

Se procede según el instructivo OSI-I-009 Control y Registro de Permisos a los Recursos de la Red y sus documentos ISO de apoyo.

7.1.6 Creada la cuenta de usuario y contraseña, los usuarios en su primer acceso deben cambiar la contraseña provisional asignada.

7.1.7 Las claves de acceso (contraseña) tienen uso de carácter de personal, intransferible y confidencial.

7.1.8 La contraseña podrá ser reestablecida por el dueño de la cuenta; en su equipo de cómputo asignado, requiriéndolo según lo establecido en el numeral 6.2 de la presente Directiva.

7.1.9 La modificación o cancelación de accesos a la red, internet, contraseñas y/o aplicaciones del INGEMMET, se especificarán según lo siguiente:

Acción	Detalle de la Solicitud

En el presente documento se utilizan de manera inclusiva términos tales como "usuario", "Jefe", "Director" y sus respectivos plurales para referirse a varones y mujeres. Esta opción se basa en una convención idiomática y tiene por objetivo evitar formas complejas de aludir a ambos géneros en el idioma castellano ("o/a", "los/las", "los/las usuarios/as", "los Jefes y las Jefas" "Directores y Directoras" y otras similares), debido a que implican una saturación gráfica que puede dificultar la comprensión lectora.

Modificación	Especificar los accesos que deben ser modificados.
Cancelación	Especificar los usuarios a los que se cancelarán los accesos.

La Oficina de Sistemas de Información efectuará la modificación o cancelación de los accesos solicitados, según lo establecido en el OSI-I-009 Control de Accesos y Recursos de la Red. La OSI comunicará la atención del requerimiento al titular del órgano o unidad orgánica solicitante.

Asimismo, la OSI podrá cancelar accesos a la red, internet y/o aplicaciones por razones fundamentadas que atenten a la seguridad de la información o cuando se detecte el mal uso de los servicios.

7.1.10 La inactividad en un terminal, estación de trabajo o PC por un periodo de tiempo, suspenderá la sesión de trabajo inmediatamente, activándose el protector de pantalla.

7.1.11 Las claves o contraseñas de las cuentas de usuario caducan cada ciento veinte (120) días calendario.

7.1.12 Las contraseñas deben cumplir con las características indicadas en el "DTIC-002 Manual y cambio de contraseñas.

7.1.13 Queda prohibido el intento de acceso por parte de los usuarios a los activos informáticos no autorizados.

7.1.14 La Unidad de Personal y Unidad de Logística, según corresponda, comunica de manera formal física o correo electrónico a la OSI que desactive la cuenta de usuario del personal que se ausente por motivo de vacaciones, descanso médico, licencia y otros motivos, durante el tiempo de ausencia; sin perjuicio de ello, el titular del órgano o unidad orgánica, por causas justificadas, podrá solicitar que la cuenta del usuario continúe activa precisando la fecha de activación y desactivación.

7.2 Sobre el uso de las estaciones de trabajo y portátiles.

7.2.1 Los usuarios del INGEMMET suscribirán el formato denominado "Ficha de Responsabilidad de Asignación de Bienes Patrimoniales" cuyo procedimiento está establecido en el documento UL-FP.3-014 "Alta y Asignación de Bienes Patrimoniales S02.03.01.01", emitido por el área de Control Patrimonial de la Unidad de Logística, en la cual se aceptan las condiciones de uso de los bienes asignados

7.2.2 Las cuentas de usuarios no tienen privilegios de tipo administrador para el sistema operativo del equipo asignado, excepto que sea un requisito indispensable para realizar sus labores, lo cual es sustentado técnicamente y autorizado por la Unidad Orgánica solicitante.

7.2.3 Toda solicitud de instalación de software adicional debe estar debidamente justificada y autorizada por la Unidad Orgánica solicitante (siempre y cuando haya sido adquirido por el solicitante). Aceptada la solicitud, la OSI procede previamente a ejecutar la instalación, siempre que el equipo cumpla con los requerimientos técnicos mínimos requeridos según la documentación oficial del´ software.

7.2.4 Se prohíbe que los usuarios instalen software que no se encuentre debidamente licenciado para INGEMMET.

7.2.5 Se prohíbe la instalación de software free (libre/gratis) o trial (evaluación/prueba), sin conocimiento del coordinador informático o Director; previa coordinación y autorización de la OSI, mediante correo electrónico o documento oficial según lo establecido en el ítem 6.2.

7.2.6 La OSI evalúa y registra el uso de Software Libre que utilizan los servidores para cumplir con sus labores relacionadas con la entidad.

7.2.7 Está prohibida la instalación y uso de redes sociales, música, videos o juegos, a excepción los usuarios de la Unidad de Relaciones Institucionales autorizados por su Director, en el marco de sus funciones.

7.2.8 Los usuarios del INGEMMET no deben utilizar herramientas de hardware o software que comprometa la seguridad de los sistemas de información (escaneo de vulnerabilidades, analizadores de red, entre otros).

7.2.9 Los usuarios están prohibidos de copiar el software proporcionado por el INGEMMET en algún dispositivo de almacenamiento externo, transferir o instalar dicho software a otra computadora, divulgarlo a personas ajenas a la institución o transferirlos a repositorios en Internet (nube de internet).

7.2.10 Los usuarios que tienen asignada uno o más activos informáticos son los únicos responsables de la información almacenada en los discos duros locales de dichos activos informáticos.

7.2.11 Todas las computadoras están protegidas con un antivirus corporativo, el que se actualiza diariamente de forma automática. Los usuarios se encuentran prohibidos de desactivar o desinstalar el software antivirus.

7.2.12 Todos los archivos obtenidos de fuentes externas al INGEMMET, incluyendo archivos copiados en dispositivos de almacenamiento externo transferidos desde Internet, archivos incluidos en mensajes de correo, repositorios en Internet (nube de internet) u otros archivos provistos por clientes o proveedores deben 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 asume las responsabilidades del caso.

7.2.13 Cuando el equipo de cómputo no esté en uso los usuarios deben asegurar que se encuentre debidamente protegido utilizando una contraseña para el protector de pantalla o bloqueando su sesión haciendo uso simultáneo de las teclas CTRL+ALT+SUPR.

7.2.14 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 conocimiento previo del coordinador informático o Director; y previa autorización de la OSI mediante correo electrónico o documento oficial según lo establecido en el ítem 6.2.

7.2.15 El traslado y reubicación de equipos de cómputo es según lo establecido en el UL-FP.3-015 Ficha de Procesos Nivel 3 - Desplazamiento Interno de Bienes – S02.03.01.02, quien informará a la OSI y elevará un registro manual o digital de éstos.

7.2.16 No está permitido guardar Información secreta, reservada o Confidencial en una computadora portátil, a menos que haya cifrado o encriptado dicha

información.

7.2.17 No está permitido guardar información personal (fotos, videos, documentos, etc.) en la estación de trabajo o portátil asignada.

7.2.18 La OSI realiza copias de seguridad de la información secreta, reservada, confidencial o de uso público (unidades de red relevantes asignadas a cada Unidad Orgánica y son las unidades de trabajo: W, O, Y, Z, L, H, e I, entre otras) de manera programada;las cuales son guardadas en un lugar seguro; dichas copias son almacenadas en cintas magnéticas en una bóveda externa, administradas por un proveedor externo que cumple con todas medidas se seguridad requeridas por la norma NTP ISO/IEC 27001:2014 referida en el marco legal de la presente Directiva.

7.2.19 La OSI, no realiza copias de respaldo ni restauración de la información almacenada ubicada en los discos duros locales.

7.2.20 Personal de la OSI son los indicados de abrir los equipos de cómputo, previo conocimiento del coordinador informático o Director; mediante correo electrónico.

7.3 Cámaras Web

7.3.1 La instalación o el uso de cámaras Web personales o tecnología similar están prohibidos en cualquier área de la institución.

7.4 Dispositivos de red inalámbricos

7.4.1 La Institución prohíbe la conexión de dispositivos de red inalámbricos, como enrutadores inalámbricos, a la red de la Institución en sus instalaciones.

7.5 Dispositivos móviles.

7.5.1 La Institución prohíbe la conexión de dispositivos móviles personales a la red inalámbrica (wi-fi) institucional. La OSI, realizará únicamente la configuración autorizada en los dispositivos móviles propios de la entidad.

7.6 De la adquisición de licencias de software e instalación.

7.6.1 La adquisición de licencias de software requiere del DTIC-006 Informe Técnico Previo de Evaluación de Software (ITES), el cual, es elaborado por la OSI en coordinación con la unidad orgánica solicitante. El informe es aprobado y firmado por el director de la OSI.

La OSI actualiza y publica en la intranet los aplicativos de uso institucional y los de servicio al ciudadano que se encuentran en el documento DTIC-005 Inventario de Aplicativos del INGEMMET.

7.6.2 El ITES forma parte del Plan Anual de Contrataciones.

7.6.3 El ITES es publicado en la sección de transparencia de la página web de la institución, antes de convocarse al proceso de selección correspondiente, bajo responsabilidad de la OSI.

7.6.4 La instalación, actualización o desinstalación de software es solicitado según lo establecido en el numeral 6.2 de la presente directiva. El referido requerimiento debe especificar los siguientes datos: nombre completo del usuario,

identificación del equipo, nombre del software solicitado (entiéndase que la Unidad Orgánica solicitante cuenta con el software solicitado licenciado).

7.6.5 Los usuarios no deben realizar copia o distribución de software licenciado por la institución.

7.6.6 Los recursos de software deben ser utilizados para labores relacionadas con la Entidad.

7.6.7 Las Unidades Orgánicas que adquieren software o lo reciben por donación u otras formas deben informar a la OSI para su registro y control respectivo.

7.6.8 La OSI hace revisiones periódicas al menos una vez al año del software instalado en los equipos informáticos, procediendo a la desinstalación de aquellos que no cuentan con la licencia respectiva.

7.6.9 La OSI instruye y concientiza a los usuarios del INGEMMET sobre el correcto uso del software legal, teniendo en cuenta la garantía, seguridad y soporte que se brinda, los riesgos y sanciones a los que el INGEMMET se expone cuando el software o su uso es ilegal.

7.6.10 La OSI evalúa y registra el uso de software propietario o libre, adquirido, obtenido y/o utilizado sin contravenir la legislación sobre el derecho de autor, que utilizan los servidores para cumplir sus labores relacionadas con la entidad.

7.6.11 LA OSI ejecuta las acciones correctivas pertinentes cuando se detecte software ilegal instalado en los activos informáticos asignados a los usuarios, poniendo en conocimiento al Coordinador Informático o Director de la Unidad Orgánica involucrada, mediante correo electrónico o documento oficial, reservándose el derecho a tomar medidas administrativas en coordinación con la Oficina de Administración.

7.7 Sobre el uso de dispositivos de almacenamiento externo.

7.7.1 Los dispositivos removibles (USB y CD/DVD) de las estaciones de trabajo y portátiles deben de estar bloqueados.

7.7.2 La habilitación de las unidades removibles (USB y/o CD/DVD) debe ser solicitada a la OSI, previa autorización del jefe y/o director de la Unidad Orgánica mediante documento oficial y/o correo electrónico institucional según lo establecido en el ítem 6.2.

7.7.3 La OSI no es responsable por la pérdida de información contenida en los dispositivos de almacenamiento externo, ni de repararlos en caso suceda algún desperfecto.

7.7.4 Los dispositivos de almacenamiento externo deben ser revisados previamente por el usuario con el antivirus corporativo instalado en su equipo de cómputo.

7.7.5 No se debe copiar, transferir, descargar o distribuir Información reservada o secreta en cualquier Dispositivo de Almacenamiento Portátil, se necesita la autorización de su director y que la información sea cifrada o encriptada.

7.8 Sobre el uso de las impresoras y equipos multifuncionales.

7.8.1 Está prohibido el uso de impresoras o equipos multifuncionales para otros fines o usos que no son inherentes a sus funciones.

7.8.2 Está prohibido manipular o alterar la configuración de impresoras o equipos de cómputo.

En el presente documento se utilizan de manera inclusiva términos tales como “usuario”, “Jefe”, “Director” y sus respectivos plurales para referirse a varones y mujeres. Esta opción se basa en una convención idiomática y tiene por objetivo evitar formas complejas de aludir a ambos géneros en el idioma castellano (“o/a”, “los/las”, "los/las usuarios/as", "los Jefes y las Jefas" “Directores y Directoras” y otras similares), debido a que implican una saturación gráfica que puede dificultar la comprensión lectora.

Siempre con el pueblo

7.8.3 Los usuarios son responsables del uso correcto de las impresoras y equipos de cómputo.

7.8.4 Está prohibido la administración de suministros no autorizados por OSI.

7.9 Sobre el servicio de préstamo de activos informáticos.

7.9.1 La OSI puede disponer limitadamente (según disponibilidad) de algunos equipos informáticos para préstamo temporal a las Unidades Orgánicas.

7.9.2 La Unidad Orgánica que recibe el equipo en calidad de préstamo es la responsable de devolver el bien a la OSI en las mismas condiciones que le fue entregado. Cualquier incidente registrado con el equipo, desde la entrega hasta la recepción del bien es responsabilidad de la Unidad Orgánica.

7.9.3 No está permitido guardar información laboral, ni personal, en el equipo prestado. Devuelto el bien, de inmediato, será sometido a una depuración.

7.9.4 No está permitido instalar ningún tipo de software, en el equipo prestado, sin coordinación y autorización previa con OSI.

7.9.5 No está permitido modificar la configuración del equipo prestado, sin coordinación y autorización previa de la OSI.

7.9.6 Todo equipo requerido para su uso fuera de las instalaciones de la Entidad debe ser registrado; para ello, el servidor beneficiado con el préstamo, debe cumplir el formato denominado “Orden de Salida de Bienes”, elaborado y emitido por el Área de Control Patrimonial de la Unidad de Logística, en cumplimiento UL-FP.3-015 Ficha de Procesos Nivel 3 - Desplazamiento Interno de Bienes - S02.03.01.02.

Para los requerimientos de préstamo de un activo informático para el desarrollo de trabajo remoto, la Unidad Orgánica debe cumplir con lo establecido en el DTIC-009 “Procedimiento para el préstamo de activos informáticos para trabajo remoto.”

7.10 Sobre el desarrollo de software.

Lineamientos Generales

7.10.1 Está prohibido que el personal de la OSI tenga acceso a las bases de datos de producción para realizar la inserción, modificación y eliminación de registros.

7.10.2 Todos los aplicativos que se encuentren en producción deben contar con niveles de acceso y la posibilidad de cambiar las contraseñas de acceso periódicamente.

7.10.3 Todos los aplicativos desarrollados de manera interna o la implantación de software será documentado, a fin de que personas no familiarizadas con las mismas puedan ejecutarlos y/o utilizarlos de ser el caso.

7.10.4 Todo desarrollo es propiedad intelectual de INGEMMET, en tal sentido, no se debe realizar copia parcial o total de sus fuentes para su distribución.

7.10.5 La OSI, dentro del ámbito de sus funciones, realiza el análisis, diseño, desarrollo, pruebas de calidad e implementación de sistemas, alineados a los procesos, objetivos y normativa de la Entidad.

7.10.6 La OSI evalúa la viabilidad y el impacto sobre el conjunto de sistemas de información institucionales y el Plan Anual de Desarrollo y Mantenimiento de Sistemas.

7.10.7 El desarrollo de software en cualquier plataforma (cliente servidor, web, móvil, etc.), contratado como un servicio de terceros, es supervisado por la OSI, quien elabora y/o valida los términos de referencia; y posteriormente otorga la Conformidad Técnica del Servicio en coordinación con la Unidad Orgánica requirente.

7.10.8 La atención a los requerimientos será según la priorización otorgada por la Unidad Orgánica responsable de la implementación y en concordancia con la priorización Institucional, siguiendo el procedimiento establecido en el documento "OSI-P-001 Desarrollo y Mantenimiento de Software".

Requerimientos de software

7.10.9 Inicio de proyecto

La Unidad Orgánica que requiere el desarrollo de nuevas aplicaciones o mejoras a aplicaciones existentes, debe utilizar el formato vigente "OSI-F-053 Requerimiento de Software" que se encuentra suscrito a la aplicación Requerimiento de Software vía INTRANET, constituyéndose en la única vía de recepción de requerimientos.

Con ello queda designado el solicitante, como el gestor de proyecto de la Unidad Orgánica.

La asignación de un gestor de proyecto - OSI tiene un plazo de 15 días hábiles, contando a partir del día siguiente de confirmada la viabilidad o aprobación del requerimiento de software.

El gestor del proyecto - OSI conjuntamente con el gestor de proyecto de la Unidad Orgánica conforman el Equipo de Proyecto.

7.10.10 Planificación del proyecto

El equipo de proyecto evaluará el proceso y los criterios de aceptación de los productos o servicios, los componentes, paquetes y actividades en los que se desglosará el proyecto.

El equipo de proyecto debe definir los procesos de gestión, supervisión, control de cambios, aceptación del usuario, gestión de problemas y escalamiento. También se debe tomar en cuenta procedimientos para el control de calidad, comunicaciones, respuesta a riesgos, adquisiciones, entre otros.

El equipo de proyecto debe elaborar el cronograma, definir las actividades, secuencia de actividades y estimación de recursos y tiempos de duración de las actividades.

El equipo de proyecto deberá estimar los costos y preparar el presupuesto del proyecto de forma detallada.

El equipo de proyecto dará visto bueno al plan de desarrollo de proyecto, cronograma resumido de las fases y se firmará el OSI-F-114 Formato de Especificaciones del Requerimiento.

Una vez firmado el OSI-F-114 Formato de Especificaciones del Requerimiento, la OSI tiene un plazo de 15 días hábiles para publicar el cronograma del proyecto aprobado en el aplicativo Requerimiento de Software ubicado en la Intranet.

7.10.11 Ejecución del proyecto

Los integrantes del equipo de proyecto deberán realizar sus actividades según los roles competentes y responsabilidades asignadas.

El equipo de proyecto dirige la ejecución del proyecto. Si el proyecto es de Desarrollo o Mantenimiento o Implementación de Software, la metodología de trabajo debe ser acorde a la naturaleza del proyecto.

El equipo de proyecto deberá validar el cumplimiento del alcance y el cronograma en los escenarios y tiempos establecidos.

Para conocer el avance del requerimiento o cronograma, el área solicitante lo puede consultar en la intranet por el link “Requerimiento de Software”, cuyo ingreso se autentica con el perfil de cada usuario.

La Unidad Orgánica solicitante debe someter a pruebas la aplicación, en el plazo establecido, desencadenando la retroalimentación de mejora o conformidad respectiva.

7.10.12 Cierre de Proyecto

El gestor de proyecto (OSI) debe elaborar una comunicación y/o informe dando a conocer la aceptación (o rechazo definitivo, si se trata de cancelación del proyecto) de los entregables del proyecto.

Si la comunicación y/o informe es conforme, el visto bueno es dada por el gestor de proyecto (Unidad Orgánica solicitante), el plazo establecido para la conformidad es de 5 días hábiles pasado este plazo se considerará conforme.

El gestor de proyecto (OSI) genera el formato “OSI-F-010 Pase a Producción” del proyecto, obtenida la conformidad.

7.11 Sobre la información almacenada en la red

7.11.1 El usuario del INGEMMET cuenta con una unidad de red para almacenar la información generada como parte de sus labores. Es su responsabilidad mantener depurada la unidad de red. Considerar el documento “DTIC-003 Procedimiento de Administración de Carpetas Públicas y Privadas”.

7.11.2 La unidad de red es de uso exclusivo para almacenamiento de datos o información laboral. Está prohibido almacenar software, juegos, fotos, videos, música, archivos de índole personal u otros.

7.11.3 La OSI respalda la información relevante (unidades de trabajo/red asignadas a cada Unidad Orgánica tales como W, O, Y, Z, L, H, I entre otras) contenida en los diferentes servidores del Data Center aplicando lo establecido en el instructivo OSI-P-007 Generación de Copias de Respaldo y Recuperación de la Información.

7.11.4 La OSI no realiza copias de respaldo o backup de los directorios asignados a los usuarios, en el servidor de archivos, para las carpetas públicas y privadas (unidad de red "P:"), las mismas que cada 30 días (quinto día de cada mes) son depuradas por personal de OSI, de modo automático.

7.11.5 Las unidades orgánicas tienen una cuota asignada de 180 Gigas como espacio mínimo de almacenamiento en una unidad de red; el cual debe ser administrado de manera adecuada.

Asimismo, se recomienda que la depuración de los archivos almacenados debe ser realizado por el usuario cada 30 días.

7.11.6 La OSI no se responsabiliza de la pérdida y/o daño de la información almacenada en el disco local de su computador.

7.11.7 No se incrementará el espacio de almacenamiento asignado por usuario, salvo solicitud expresa y justificada de su Director, evaluando la factibilidad de dicha solicitud en referencia a la infraestructura tecnológica.

7.12 Sobre el uso de correo electrónico institucional

7.12.1 La OSI administra y gestiona el servicio de Correo Electrónico Institucional del INGEMMET.

Actualiza las características de los servicios de correo electrónico proporcionado por el INGEMMET como parte del proceso de mejora continua. Atender las solicitudes de creación, actualización o desactivación de cuentas de correo electrónico, garantizando la integridad operatividad y confidencialidad de la información.

7.12.2 La estructura de la cuenta de correo electrónico utiliza el formato mencionado en el numeral 7.1.4. de la presente directiva.

7.12.3 Una cuenta de correo electrónico institucional es una herramienta de comunicación e intercambio de información oficial, interna y externa, es decir:

- Entre personal del INGEMMET
- Entre el personal del INGEMMET y otras entidades públicas y/o privadas, así como con personas naturales.

7.12.4 El uso del correo electrónico se circunscribe, de manera exclusiva, para el ejercicio de sus funciones en la entidad, siendo su uso personal e intransferible, sólo pueden ser usadas por los propietarios de las mismas. El propietario de la cuenta de correo es el responsable directo de la confidencialidad de la contraseña correspondiente.

7.12.5 La OSI se encargará de definir el software para el servicio del correo electrónico, teniendo en cuenta las tecnologías actuales y es configurado por la OSI en la computadora del usuario. Está prohibido alterar la configuración del software o remplazarlo por otro software sin previa coordinación. El usuario debe considerar el "DTIC-004 Manual de Uso del Software de Correo Electrónico", publicado en la intranet.

7.12.6 El usuario es responsable de los mensajes de correo electrónico que se descarguen en su equipo de cómputo, desde el servidor de correo al acceder al servicio.

7.12.7 Los usuarios son los únicos responsables de guardar copias de seguridad de los correos electrónicos almacenados en las carpetas personales del disco duro

del activo informático asignado.

7.12.8 La capacidad del buzón de correo, la OSI definirá el tamaño máximo de buzones de correo, tomando en consideración la capacidad de almacenamiento físico de los servidores que brindan este servicio, en proporción a los siguientes niveles:

Nivel A: El tamaño del buzón de correo correspondiente a Presidencia de Consejo Directivo, Asesores de Presidencia y Gerencia General será 7GB.

Nivel B: El tamaño máximo del buzón de correo será hasta 5Gb para los siguientes puestos: Director de Línea, Jefe de Unidad Orgánica, miembros delComités, secretarias de los puestos mencionados en el Nivel A y Nivel B y lascuentas de servicio o cuentas genéricas.

Nivel C: El tamaño máximo del buzón de correo será hasta 3Gb para los demás puestos no mencionados en los niveles anteriores: Profesionales, técnicos, secretarias y auxiliares.

Nivel D: El tamaño máximo del buzón de correo será hasta 2Gb, para los demás puestos no mencionados en los niveles anteriores: practicantes y otros trabajadores cuya vinculación laboral sea aprobada por la Unidad de Personal.

La OSI, a petición del titular del órgano o unidad orgánica usuaria y previa evaluación de cada caso, podrá establecer cuotas máximas del buzón de correo electrónico diferentes a las establecidas en la presente directiva.

7.12.9 La información contenida en el correo electrónico del usuario es de acceso público siempre que se trate de información institucional de naturaleza pública. Existe un deber funcional de entregar aquella información institucional que se repute de naturaleza pública, previo consentimiento del funcionario o servidor público, deacuerdo a lo establecido en la Ley de Transparencia y Acceso a la Información Pública vigente.

7.12.10 El uso del correo electrónico institucional se efectúa en las instalaciones del INGEMMET o desde Internet a través del Correo Web en la dirección https://correoweb.ingemmet.gob.pe, en este último caso tener en cuenta lo siguiente:

7.12.10.1 Cada usuario tiene 2 GB de espacio de almacenamiento y 23 MB para enviar o recibir mensajes en su casilla de correo electrónico. Sólo a solicitud del Director o Jefe de Unidad Orgánica se puede ampliar la capacidad de almacenamiento y/o envío por un periodo de tiempo determinado.

7.12.10.2 El usuario realizará actividades de mantenimiento periódico a su buzón de correo, eliminado mensajes que no requiera almacenar para mantener su buzón siempre disponible, no sobre pasar su cuota asignada y asegurarse de contar con una copia personal.

7.12.10.3 Los mensajes de correo electrónico que no se relacionen con las funciones del usuario, deberán ser eliminados inmediatamente por el usuario, para no ocupar espacio innecesario que afecte la capacidaddel buzón asignado.

7.12.10.4 La OSI podrá crear cuentas de correo electrónico genéricas o de servicio para una mejor disposición técnica El Director o Jefe de la Unidad Orgánica debe remitir a la OSI el Formato “OSI-F-222 Gestión de Accesos a la Red” precisando los responsables de administrar dicha cuenta genérica/servicio, así comoel periodo de caducidad de la misma, de ser necesario. Para el caso de comités institucionales deberá solicitarlo el presidente o representante asignado.

7.12.10.5 Las cuentas de correo electrónico genéricas/servicio contarán con el permiso de envío masivo de correo a todo el personal de la entidad (alluser). Los usuarios que requieran el permiso de envío masivo de correos electrónicos deberán contar con autorización de su Jefe inmediato.

Las cuentas de correo electrónico genéricas/servicio son para el envío de mensajes que se relacionen con el objeto de su creación.

7.12.10.6 Todos los mensajes que se envíen fuera del dominio del INGEMMET deben mostrar un aviso de confidencialidad, dicha configuración está a cargo de la OSI. El aviso de confidencialidad se configura al momento de configurar el correo electrónico y debe señalar que la información contenida en los mensajes es privilegiada, confidencial y sólo de interés para el destinatario, de acuerdo al aviso de confidencialidad “DTIC-007 Aviso de confidencialidad del Correo Institucional”.

7.12.10.7 Está 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 Entidad.

7.12.10.8 Para reducir la recepción de correos electrónicos masivos, el sistema de protección de correo electrónico ANTISPAM podrá colocar los mensajes en “listas negras” de restricción y para evitar que el servicio sea afectado, la OSI adoptará las acciones técnicas y realizará las coordinaciones necesarias con el proveedor del servicio.

7.12.10.9 Cuando un usuario reciba algún mensaje que considere que transgrede lo dispuesto en la presente directiva, deberá informar inmediatamente a la OSI según lo establecido en el numeral 6.2 de la presente directiva.

7.12.10.10 Está prohibido la afiliación o suscripción del correo institucional a servicios no relacionados con sus responsabilidades y funciones.

7.12.10.11 Está prohibido registrar los correos institucionales en redes sociales (Facebook, Twitter, Instagram, Tick Tock, Mercado Libre, etc)

7.12.10.12 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.

7.12.10.13 Está prohibido responder los mensajes de usuarios desconocidos para evitar confirmación de direcciones electrónicas y recibir correo no solicitado.

En el presente documento se utilizan de manera inclusiva términos tales como “usuario”, “Jefe”, “Director” y sus respectivos plurales para referirse a varones y mujeres. Esta opción se basa en una convención idiomática y tiene por objetivo evitar formas complejas de aludir a ambos géneros en el idioma castellano (“o/a”, “los/las”, "los/las usuarios/as", "los Jefes y las Jefas" “Directores y Directoras” y otras similares), debido a que implican una saturación gráfica que puede dificultar la comprensión lectora.

7.12.10.14 Está prohibido conductas que vulneren la seguridad de la infraestructura tecnológica.

7.12.10.15 La recepción de correos de tipo ofensivo proveniente de una cuenta de correo externa debe ser reportado a la OSI para su bloqueo y monitoreo correspondiente.

7.12.10.16 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 archivossimilares son automáticamente eliminados, debido a que son susceptibles de contener virus informáticos.

7.12.10.17 Autofirmas

- La firma deberá ser breve e informativa, debiendo ocupar siete (7) líneas para puestos que dependen directamente de una dirección y puestos que dependen de una unidad orgánica.
- La firma de correo electrónico debe considerar el logo del INGEMMET, nombres y apellidos del usuario, área al que corresponde, unidad orgánica y/o dirección, nombre de la entidad, dirección, teléfono y anexo asignado, utilizando el siguiente modelo:

Modelo para puestos que dependen directamente de una dirección:

Victoria Mendoza Correa
Unidad Técnico Normativa
Dirección de Concesiones Mineras
Instituto Geológico, Minero y Metalúrgico
Av. Canadá 1470 – San Borja
Telf.: 01-618 9800 Anexo: 201
www.gob.pe/ingemmet

SECTOR ENERGÍA Y MINAS
INGEMMET
INSTITUTO GEOLÓGICO, MINERO Y METALÚRGICO

Modelo para puestos que dependen de una unidad orgánica

Victoria Mendoza Correa
Analista de Desarrollo de Sistemas
Oficina de Sistemas de Información
Oficina de Administración
Av. Canadá 1470 – San Borja
Telf.: 01-618 9800 Anexo: 202
www.gob.pe/ingemmet

SECTOR ENERGÍA Y MINAS
INGEMMET
INSTITUTO GEOLÓGICO, MINERO Y METALÚRGICO

El tipo de letra para los nombres y apellidos es Calibri de tamaño de

En el presente documento se utilizan de manera inclusiva términos tales como "usuario", "Jefe", "Director" y sus respectivos plurales para referirse a varones y mujeres. Esta opción se basa en una convención idiomática y tiene por objetivo evitar formas complejas de aludir a ambos géneros en el idioma castellano ("o/a", "los/las", "los/las usuarios/as", "los Jefes y las Jefas" "Directores y Directoras" y otras similares), debido a que implican una saturación gráfica que puede dificultar la comprensión lectora.

Siempre con el pueblo

fuente 10 y para los demás datos es Calibri de tamaño de fuente 9.

La dirección de correo electrónico no se incluirá en la firma, porque ésta se incluye de manera automática en la parte superior del mensaje.

7.13 Sobre el uso del acceso al Internet

7.13.1 La OSI es responsable de la administración de los servicios de acceso a Internet, para lo cual hace uso de herramientas especializadas de monitoreo del uso de Internet a fin de detectar las acciones que se realizan con el permiso otorgado, pudiendo restringirse el acceso a determinadas páginas web y la descarga de archivos por disposiciones de seguridad y uso.

7.13.2 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.

7.13.3 Está prohibido el ingreso a páginas web de música, radio, televisión y/o películas en línea (Repelis, Netflix, Movistar-Play y otros similares), chat, juegos, contenido pornográfico, software ilegal o de dudosa procedencia, terrorismo y 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 tener acceso a las redes sociales, se debe solicitar la autorización del Director de la Unidad Orgánica correspondiente.

7.13.4 Está prohibido utilizar los servicios proporcionados para uso de Internet para enviar información del INGEMMET a personas no autorizadas.

7.13.5 Está prohibido descargar y/o archivar software no autorizado de Internet. Si por motivos laborales se requiere descargar algún aplicativo o archivo de gran volumen, éste debe ser coordinado y autorizado por la OSI.

7.13.6 Cada usuario es responsable de las acciones que se ejecuten con su autorización de acceso a Internet.

7.13.7 La autorización de uso de Internet a proveedores o consultores externos, se proporciona temporalmente, previa autorización del Director de la Unidad Orgánica correspondiente.

7.13.8 Está 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, previa autorización del Director de la Unidad Orgánica correspondiente.

7.14 Sobre el uso de la mensajería interactiva instantánea (chat)

7.14.1 El uso de mensajería interactiva se encuentra prohibido, y solamente será proporcionado a aquellos usuarios con autorización del Director de la Unidad Orgánica correspondiente.

7.14.2 El chat o mensajería interactiva no es considerado como medio oficial de comunicación.

7.14.3 Está prohibido enviar o recibir información privilegiada (secreta, reservada y confidencial) de la entidad utilizando mensajería instantánea; no es un medio de comunicación segura.

En el presente documento se utilizan de manera inclusiva términos tales como “usuario”, “Jefe”, “Director” y sus respectivos plurales para referirse a varones y mujeres. Esta opción se basa en una convención idiomática y tiene por objetivo evitar formas complejas de aludir a ambos géneros en el idioma castellano (“o/a”, “los/las”, "los/las usuarios/as", "los Jefes y las Jefas" “Directores y Directoras” y otras similares), debido a que implican una saturación gráfica que puede dificultar la comprensión lectora.

7.15 Sobre el acceso a los ambientes de Tecnologías de la Información y Comunicación

7.15.1 El Centro de Datos del INGEMMET está ubicado en área restringida.

7.15.2 El acceso al Centro de Datos del INGEMMET debe seguir los lineamientos establecidos en el instructivo OSI-I-007 Acceso al Data Center del INGEMMET previo ingreso del formulario OSI-F-163 Solicitud de Acceso al Data Center.

7.16 Seguridad física ambiental del Centro de Datos

7.16.1 El Centro de Datos debe de estar provisto de lo siguiente:

- Sistema de Aire acondicionado de Precisión para atender la demanda de enfriamiento necesaria para los equipos del centro de Datos.
- Sistema de Detección y extinción contra incendios, instalados en todos los ambientes del centro de Datos.
- Sensores de temperatura y humedad para prevenir el sobrecalentamiento de los equiposdel centro de Datos.
- Disponer de grupo electrógeno con capacidad suficiente para soportar la demanda de energía del centro de Datos.
- Disponer de luces de emergencia con baterías en todos los ambientes del centro de Datos.
- Los equipos principales y de respaldo como UPS y Grupo Electrógeno deben ser periódicamente conectados y probados con carga real para garantizar su disponibilidad.

7.17 Sobre el uso de la telefonía IP

7.17.1 La solicitud de un equipo telefónico IP es requerido por la Unidad Orgánica mediante documento oficial o correo electrónico dirigido a la OSI.

7.17.2 Los equipos telefónicos son administrados por la Unidades Orgánicas respectivas. Los usuarios no pueden trasladar dicho equipo a otra Unidad Orgánica sin la autorización de la Unidad Orgánica y el conocimiento de la OSI.

7.17.3 El número de anexo es definido y administrado por la OSI.

7.17.4 El número de minutos asignado por usuario o por oficina, está regulado por la Oficina de Administración de acuerdo a la tarificación vigente por el proveedor de servicios.

7.17.5 Los anexos telefónicos tienen acceso sólo a llamadas internas. Las Unidades Orgánicas deben solicitar mediante documento o correo electrónico dirigido a la OSI, atributos adicionales sobre los anexos a su cargo dentro de la bolsa de minutos asignada.

7.17.6 Los atributos adicionales a las llamadas telefónicas internas son los siguientes:

- Fijo local
- Fijo Nacional
- Fijo Internacional
- Celular
- Celular internacional

Se encuentran restringidas las llamadas de los tipos LDN (larga distancia

nacional) y LDI (larga distancia internacional).

7.17.7 La clave asignada a los usuarios es personal e intransferible, sólo podrá ser cambiada por temas de seguridad a solicitud de la Unidad Orgánica respectiva.

7.17.8 La Unidad Orgánica puede solicitar mediante documento oficial a la OSI el reporte de consumo por anexo y por clave asignada del personal a su cargo.

7.17.9 Las Unidades Orgánicas deben informar a la OSI la eliminación del anexo telefónico del Directorio Institucional, inmediatamente se determine el cese de funciones del personal a su cargo, a fin de poder reasignarlo o reubicarlo según aplique. En caso se determine que el equipo telefónico se encuentra en desuso, personal de la OSI procederá a retirarlo, previa coordinación entre el Director OSI y el Director de dicha unidad orgánica.

7.18 <u>Sobre el uso de los puntos de red y tomas eléctricas estabilizadas.</u>

7.18.1 Los términos de referencia para la implementación de puntos de red y red eléctrica estabilizada están a cargo de la OSI. Está prohibido instalar, habilitar o realizar servicios de ampliación de puntos de red y red eléctrica estabilizada sin previa coordinación con la OSI.

7.18.2 Las unidades orgánicas no deben instalar equipos que incrementen los puntos de red como: concentradores o conmutadores de red. Estos equipos degradan el rendimiento de la red.

7.18.3 El mantenimiento de la red de datos y de la red eléctrica estabilizada en las Sedes de Lima está a cargo de la OSI.

7.18.4 El mantenimiento de la red de datos y de la red eléctrica estabilizada en los Órganos Desconcentrados está a cargo de la Coordinación de los Órganos Desconcentrados.

7.18.5 Los usuarios no deben conectar equipos domésticos (hervidores, microondas, ventiladores, etc.) a la red eléctrica estabilizada.

7.18.6 Los usuarios no están autorizados a manipular las conexiones de red, debido a que existe un orden en la conexión, el cual debe de ser respetado y así evitar problemas en la red de la institución.

7.18.7 Las conexiones de los equipos a la red de la institución deben ser solicitados mediante documento o correo electrónico dirigido a la (OSI).

7.18.8 Ningún equipo externo debe ser conectado a un punto de red habilitado.

7.19 <u>De la Privacidad y Confidencialidad de la Información.</u>

7.19.1 Todos los usuarios del INGEMMET deben acceder únicamente a la información a la que estén debidamente autorizados por su Director.

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

7.20 <u>Sobre el incumplimiento de las disposiciones contenidas en la presente directiva.</u>

El incumplimiento de las disposiciones contenidas en la presente Directiva, en función a la gravedad de las mismas, podrán ser comunicadas al Jefe inmediato superior de la

En el presente documento se utilizan de manera inclusiva términos tales como "usuario", "Jefe", "Director" y sus respectivos plurales para referirse a varones y mujeres. Esta opción se basa en una convención idiomática y tiene por objetivo evitar formas complejas de aludir a ambos géneros en el idioma castellano ("o/a", "los/las", "los/las usuarios/as", "los Jefes y las Jefas" "Directores y Directoras" y otras similares), debido a que implican una saturación gráfica que puede dificultar la comprensión lectora.

Siempre con el pueblo

Unidad Orgánica donde labora el infractor, para la adopción de las medidas correctivas pertinentes. En la eventualidad que el incumplimiento revista de gravedad, deberá ser puesta a conocimiento de la Secretaría Técnica de los Órganos Instructores del Procedimiento Administrativo Disciplinario, mediante denuncia formulada por la Dirección de la Oficina de Sistemas de la Información, conforme a los formatos y procedimientos establecidos en la Directiva "Régimen Disciplinario y Procedimiento Sancionador del INGEMMET", aprobada por Resolución de Presidencia N° 072-2017-INGEMMET/PCD, norma que la modifique o sustituya; a fin de iniciar el procedimiento de deslinde correspondiente".

7.21 Obsolescencia Tecnológica

7.21.1 La OSI es responsable de emitir informe técnico de obsolescencia tecnológica de un activo informático cuyo ciclo de vida útil es como mínimo de 4 años, el cual debe ser dirigido a Control Patrimonial para su baja respectiva.

7.21.2 El software y las licencias de los equipos informáticos considerados de baja por obsolescencia tecnológica serán incluidos en el informe técnico de obsolescencia.

VIII. DISPOSICIONES COMPLEMENTARIAS.

8.1 De la Difusión y Vigencia de la presente Directiva.

8.1.1 La OSI, en coordinación con la Unidad de Personal, debe remitir por medio digital, al personal que ingrese a laborar en la Institución, 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 y Comunicación en el INGEMMET.

8.1.2 La presente Directiva tiene vigencia desde la fecha de su publicación en la página web institucional.

IX. ANEXOS

ANEXO N° 01 GLOSARIO DE TÉRMINOS

1. **Activo de Información:** Cualquier información o sistema relacionado con el tratamiento de la misma que tenga valor para la organización. Es susceptible de ser atacado deliberada o accidentalmente con consecuencias para la organización. Tipos de Activos de Información:

Secreta:	Información que debe ser encriptada y con los niveles de seguridad adecuados.
Reservada:	De acceso y uso de una determinada Unidad Orgánica.
Confidencial:	De uso interno de la Entidad
Pública:	Información de acceso al público en general.

2. **Activos Informáticos**: Son aquellos recursos (físico y digital) con los que cuenta una entidad. Es decir, todo elemento que compone el proceso completo de comunicación, partiendo desde la información, el emisor, el medio de transmisión y receptor. Comprende infraestructura, hardware, controles del entorno de tecnologías de la información, base de datos, copias de seguridad, claves, red informática software de sistema, sistemas operativos, aplicaciones y soportes de información.

3. **Antispam**: Aplicación o herramienta informática que se encarga de detectar y eliminar los correos no deseados.

4. **Antivirus:** Programa o software cuya función es detectar y eliminar programas maliciosos (malware) como son virus informáticos, entre otros.

5. **Autenticación:** Procedimiento de comprobación de la identidad de un usuario.

6. **Aplicativo Informático:** Tipo de programa informático diseñado como herramienta o para un fin determinado, para facilitar o permitir a un usuario realizar uno o diversos tipos de trabajo en un dispositivo informático.

7. **Cliente Servidor:** Modelo de comunicación que vincula a varios dispositivos informáticos a través de una red. El cliente realiza peticiones de servicios al servidor, que se encarga de satisfacer dichos requerimientos.

8. **Correo Electrónico:** Servicio que permite el intercambio de mensajes, archivos, imágenes y texto entre usuarios del servicio.

9. **Confidencialidad de la información**: Es la necesidad de que la información sea conocida solo por las personas autorizadas.

10. **Contraseña o clave:** Información confidencial, constituida frecuentemente por una cadena de caracteres, que puede ser usada en la autenticación de un usuario.

11. **Control de acceso:** Mecanismo que en función a la identificación ya autenticada permite acceder a datos o recursos.

12. **Infraestructura TI:** Todo el hardware, software, instalaciones etc. requeridas para desarrollar, probar, proveer, monitorear, controlar o soportar los Servicios de TI.

13. **Dato:** Pueden ser cualquier forma de información como registros, archivos y base de datos, texto, hojas de cálculo, imágenes, video, etc.

14. **Documento Oficial:** Son una comunicación escrita o digital de carácter formal que se utiliza tanto en la administración pública, con la finalidad de dar cumplimiento al sistema de gestión que utiliza la entidad.

15. **Dominio**: Es la representación de la entidad pública en la red de internet, correspondiendo al INGEMMET, el nombre del @ingemmet.gob.pe.

16. **Discos Duros Locales:** Dispositivos de almacenamiento interno de las computadoras escritorio o computadoras portátiles.

17. **Dispositivo de Almacenamiento:** Todo aparato que se utilice para grabar los datos de la computadora de forma permanente temporal. Son de dos clases: Dispositivos de almacenamiento primario, que son los usados por la CPU directamente (memoria principal, memoria caché entre otros); y, dispositivos de almacenamiento secundario, a los cuales la CPU no accede directamente, sino que deben ser almacenados previamente en dispositivos. Es el caso de los discos magnéticos, discos ópticos, cintas magnéticas, tambores magnéticos, disquetes, cartuchos, entre otros.

18. **Equipo Móvil inteligente:** Dispositivos móviles con capacidades computacionales, capaces de ofrecer integración con sistemas de correo, ERP, CRM y otros orientados

al concepto.

19. **Equipos Multifuncionales:** Equipos de cómputo que pueden ser utilizados para más de una función como, por ejemplo: scanner, impresora y copiadora.

20. **Especificaciones Técnicas:** Descripciones elaboradas por la Entidad de las características fundamentales de los bienes, suministros u obras a contratar. Estas características serán brindadas por la Oficina de Sistemas de Información.

21. **File Transfer Protocol - FTP** es un protocolo de red o aplicación de software para la transferencia de archivos entre sistemas conectados a una red

22. **Identificación:** Procedimiento de reconocimiento de la identidad de un usuario.

23. **Información**: es un activo de información en físico o en digital que según su tipo de confidencialidad o criticidad se da el tratamiento de seguridad.

24. **Integridad:** Es la característica de la información que hace que su contenido permanezca invariable a menos que sea modificado por una persona autorizada.

25. **Intranet:** es una red de computadoras similar a internet, para uso exclusivo de una determinada organización, pudiendo solamente las PC de la institución acceder a ella.

26. **Libreta de direcciones:** Servicio que permite al usuario de correo electrónico, crear, ordenar y administrar sus contactos. Dicha herramienta puede ser sincronizada con sistemas Outlook y equipo móviles inteligentes.

27. **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.

28. **Perfil de usuario:** Conjunto de características que se asigna a un usuario para restringir o ampliar sus niveles de acceso.

29. **Malware:** es la abreviatura de “Malicious software”. Término que engloba a todo tipo de programa o código informático malicioso cuya función es dañar un sistema o causar un mal funcionamiento.

30. **Nube de Internet:** Es un modelo para la utilización de los recursos informáticos que está completamente basado en Internet. Dichos recursos, son aplicaciones software, almacenamiento de archivos, bases de datos, correo electrónico, etc., residen en servidores remotos, de modo que el usuario puede acceder a ellos desde cualquier lugar del mundo, siempre que cuente con un navegador y una conexión a Internet.

31. **Outsourcing:** Consiste en movilizar recursos hacia una empresa externa o persona natural a través de un contrato. De esta forma, la empresa/persona subcontratada desarrolla actividades en nombre o solicitud de la primera.

32. **Recursos Compartidos**: Es la función que permite al usuario compartir con otros usuarios, dentro del sistema de correo electrónicos, información. Esta información puede ser: contactos, correos electrónicos, notas y calendarios.

33. **Red Informática:** Conjunto de equipos de cómputo que interconecta física y lógicamente para intercambio de información y de recursos informáticos.

34. **Red de Datos**: Es la infraestructura cuyo diseño posibilita la transmisión de información a través del intercambio de datos (puntos de red, cable de red, equiposde comunicación, entre otros.)

35. **Repositorios en Internet:** Un repositorio, depósito o archivo es un sitio centralizado que almacena y mantiene información digital, habitualmente bases de datos o archivos informáticos. Tales como: SkyDrive (Hotmail), Drive (Google), Dropbox, u otros.

36. **Sistema:** Es el conjunto independiente de recursos de información organizados para la recopilación, procesamiento, mantenimiento, transmisión y difusión de información, según procedimientos determinados.

37. **Software:** Son los componentes lógicos necesarios para hacer posible la realización de una tarea específica en una computadora.

38. **Software libre (Open Source):** Conjunto de software (programa informático) que, por elección manifiesta de su autor, puede ser copiado, estudiado, modificado, utilizado libremente con cualquier fin y redistribuido con o sin cambios o mejoras.

39. **Software legal:** En el INGEMMET se considera software legal a los siguientes:

    a. Aquel software del que es propietario, con licencia adquirida.
    b. Aquel software que es desarrollado por la OSI del INGEMMET.
    c. Aquel software que es open source (software libre), cuya relación se encuentra publicada en la intranet del INGEMMET.

40. **Software propietario:** Cualquier programa informático en el que los usuarios tienen limitadas las posibilidades de usarlo, modificarlo o redistribuirlo (con o sin modificaciones), o cuyo código fuente no está disponible o el acceso a éste se encuentra restringido.

41. **SPAM:** Mensajes electrónicos no solicitados, no deseados o de remitente desconocido (anónimo). Por lo general son de carácter publicitario y enviados de manera masiva.

42. **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.

43. **Términos de Referencia:** Descripción de las características técnicas y condiciones en que se ejecuta la prestación de servicios y de consultoría.

44. **Tomas eléctricas estabilizadas:** Tomacorrientes eléctricos cuya energía eléctrica ha sido estabilizada, filtrada y protegida a fin de proporcionar fluido eléctrico adecuado y uso exclusivo para dispositivos de cómputo.

45. **Usuario:** Servidores del INGEMMET que se encuentran registrados en el sistema informático a través de una cuenta de acceso cuya validación está determinada por la aplicación de un usuario y una contraseña.

46. **Usuario Líder:** Responsable funcional de una aplicación.

ANEXO N° 02 DOCUMENTOS DE USO

Documentos que, son de cumplimiento y aplicación conjunta. Es la documentación del Sistema de Gestión de Calidad y documentos de tecnología de la información y comunicación (DTIC) disponibles en el en la intranet.

1. OSI-F-222 Gestión de Accesos a la Red
2. OSI-F-053 Requerimiento de Software.
3. OSI-I-007 Acceso al Data Center del INGEMMET.
4. OSI-I-009 Control de Accesos y Recursos de la Red.
5. OSI-P-007 Generación de copias de Respaldo y Recuperación.
6. OSI-P-001 Desarrollo y Mantenimiento de Software.
7. OSI-F-114 Formato de Especificaciones del Requerimiento.
8. OSI-F-010 Pase a Producción
9. DTIC-001 Estándar de Creación de Objetos en el Directorio Activo del Dominio ingemmet.int.
10. DTIC-002 Manual de Cambio de Contraseñas.
11. DTIC-003 Procedimiento de Administración de Carpetas Públicas y Privadas.
12. DTIC-004 Manual de Uso del Software de Correo Electrónico.
13. DTIC-005 Inventario de Aplicativos del INGEMMET.
14. DTIC-006 Informe Técnico Previo de Evaluación de software ITES
15. DTIC-007 Aviso de Confidencialidad del Correo Institucional.
16. DTIC-009 Procedimiento para el préstamo de activos informáticos para trabajo remoto
17. UL-FP.3-014 Alta y Asignación de Bienes Patrimoniales S02.03.01.01.08
18. UL-FP.3-015 Ficha de Procesos Nivel 3 - Desplazamiento Interno de Bienes - S02.03.01.02
19. Ficha de Responsabilidad de Asignación de Bienes patrimoniales.
20. Orden de Salida de Bienes.

ANEXO N° 03: LISTA DE DOCUMENTOS DE REFERENCIA

Los siguientes documentos complementarios a los documentos de uso no son parte de la directiva, pero son referidos en ella.

1. OSI-F-163 Solicitud de Acceso al Data Center.
2. DTIC-008 Manual del Aplicativo Mesa de Ayuda

ANEXO N° 04: OBSOLESCENCIA TECNOLÓGICA DE LOS EQUIPOS INFORMÁTICOS

TIPO DE EQUIPO	OBSOLECENCIA TECNOLÓGICA DE USO
Computadoras de escritorio	04 años
Impresoras	04 años
Plotters	08 años
Escáner	04 años
Computadoras portátiles	04 años
Proyector multimedia	04 años
Pantalla táctil interactiva	15 años
Servidores	04 años
Switches	04 años