RESOLUCIÓN GERENCIAL GENERAL REGIONAL N° 344 -2021-GRL-GGR.

Belén, 21 de setiembre del 2021

Visto, el Oficio N° 105-2021-GRL-GGR-OEDI, de fecha 13 de setiembre de 2021, de la Oficina Ejecutiva de Desarrollo Institucional, a través del cual remite adjunto el Informe N° 04-2021-GRL-GGR-OEDI-CFSV, de fecha 05 de setiembre de 2021, ampliando el Informe N° 003-2021-GRL-GGR-OEDI-CFSV, de fecha 23 de agosto de 202, sobre propuesta de "Políticas de Seguridad de la Información" y Directiva General N° 001-2021-GRL-GGR-ORTIT sobre Seguridad de la Información del Gobierno Regional de Loreto, para su aprobación mediante acto resolutivo, y;

CONSIDERANDO:

Que, el **artículo 191° de la Constitución Política del Perú**, modificado por la Ley N° 27680, Ley de Reforma Constitucional del Capítulo XIV del Título IV sobre Descentralización, en concordancia con la **Ley N° 27867, Ley Orgánica de Gobiernos Regionales, modificada por la Ley N° 27902**, que en sus **artículos 2° y 4°** respectivamente, establecen que, los Gobiernos Regionales son personas de derecho público, con autonomía política, económica y administrativa en asuntos de su competencia, constituyendo para su administración económica y financiera, un Pliego Presupuestal. Los gobiernos regionales promueven el desarrollo y la economía regional, fomentan las inversiones, actividades y servicios públicos de su responsabilidad, en armonía con las políticas y planes nacionales y locales de desarrollo, y son competentes entre otras atribuciones aprobar su organización interna;

Que, la **Ley N° 27783, Ley de Bases de Descentralización, en su artículo 8°** precisa: "La autonomía es el derecho y la capacidad efectiva del Gobierno en sus tres niveles de normar, regular y administrar los asuntos públicos de su competencia (...)", en concordancia con el artículo 6° que establece como uno de los objetivos de la descentralización, el ordenamiento territorial y del entorno ambiental, desde los enfoques de la sostenibilidad del desarrollo;

Que, mediante **Decreto Legislativo N° 1412, Decreto Legislativo que Aprueba la Ley de Gobierno Digital**, se señala que la presente 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 digitales en la digitalización de procesos y prestación de servicios digitales por parte de las entidades de la Administración Pública en los tres niveles de gobierno. Asimismo, indica 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, y comprende el conjunto de principios, políticas, normas, procedimientos, técnicas e instrumentos utilizados por las entidades de la Administración Pública en la gobernanza, gestión e implementación de tecnologías digitales para la digitalización de procesos, datos, contenidos y servicios digitales de valor para los ciudadanos;

RESOLUCIÓN GERENCIAL GENERAL REGIONAL N° 344-2021-GRL-GGR.

Belén, 21 de setiembre del 2021

Que, con **Resolución Ministerial N° 166-2017-PCM, se Modifica el artículo 5° de la Resolución Ministerial N° 004-2016-PCM** referente al Comité de Gestión de Seguridad de la Información, es así que en el **artículo 2°** se establece la Incorporación del artículo 5-A a la Resolución Ministerial N° 004-2016-PCM. Incorpórese el artículo 5-A a la Resolución Ministerial N° 004-2016-PCM, conforme al siguiente texto: "Artículo 5-A.- De las Funciones del Comité de Gestión de Seguridad de la Información, el Comité de Gestión de Seguridad de la Información debe cumplir, como mínimo, las siguientes funciones: **a) Proponer la política y objetivos de seguridad de la información alineados con el Plan Estratégico Institucional, con la Política Nacional de Gobierno Electrónico y regulación en el ámbito de seguridad de la información;**

Que, **mediante Resolución Ejecutiva Regional N° 151-2021-GRL-GR, de fecha 12 de mayo de 2021**, se resuelve en su artículo 1°: DESIGNAR, el Comité de Gestión de Seguridad de la Información del Gobierno Regional de Loreto (...);

Que, a través del **Acta N° 002-2021-GRL-CGSI, de fecha 21 de julio de 2021**, el Comité de Gestión de Seguridad de la Información del Gobierno Regional de Loreto, Acordó: Aprobar los instrumentos de gestión "Directiva de Seguridad de la Información" y "Políticas de Seguridad de la Información", en el marco 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", elaborado por el equipo técnico de la Oficina Regional de Tecnologías de la Información y Telecomunicación;

Que, mediante **Informe N° 015-2021-GRL-GGR-ORTIT, de fecha 26 de julio de 2021,** emitido por el Ing. Edward Javier Sangama Reyna, Jefe de la Oficina Regional de Tecnologías de la Información y Telecomunicaciones al Gerente General Regional, sobre las acciones realizadas por el Comité de Gestión de Seguridad de la Información del Gobierno Regional de Loreto, donde concluye que el Gobierno Regional de Loreto, no cuenta con los instrumentos de gestión elementales para la seguridad de la información de los activos digitales, que siempre están expuestos a vulnerabilidades o ataques cibernéticos. Asimismo, esta acción es el inicio de la implementación del Sistema de gestión de la Seguridad de la Información, por lo que es indispensable su pronta ejecución. Para seguir con el cumplimiento de las normativas de Transformación Digital, se requiere que los instrumentos de gestión "Directiva de Seguridad de la Información" y "Políticas de Seguridad", sean aprobados mediante acto resolutivo;

Que, mediante **Oficio N° 098-2021-GRL-GGR/OEDI, de fecha 26 de agosto de 2021** se adjunta el Informe N° 03-2021-GRL-GGR-OEDI-CFSV, de fecha 23 de agosto de 2021, emitido por Carlos Fernando Salazar Vigo al Jefe de la Oficina Ejecutiva de Desarrollo Institucional sobre propuesta de Políticas de Seguridad de la Información y Directiva General N° 001-2021-GRL-GGR-ORTIT sobre Seguridad de la Información del Gobierno Regional de Loreto, presentado por la Oficina Regional de Tecnologías de la Información y Telecomunicaciones, concluye que es importante contar con un marco normativo actualizado y vigente de carácter regional en el ámbito de la seguridad informática regional que cumple con los estándares y requerimientos de seguridad informática requeridos en el Gobierno Regional de Loreto. Recomendando que se

RESOLUCIÓN GERENCIAL GENERAL REGIONAL Nº 344-2021-GRL-GGR.

Belén, 21 de setiembre del 2021

continúe con su trámite de aprobación para su implementación y cumplir los requisitos de seguridad para el mejor desempeño de las labores que requieren de soporte informático en el Gobierno Regional de Loreto;

Que, mediante **Oficio Nº 105-2021-GRL-GGR-OEDI, de fecha 13 de setiembre de 2021**, la Oficina Ejecutiva de Desarrollo Institucional, remite adjunto el Informe Nº 04-2021-GRL-GGR-OEDI-CFSV, de fecha 05 de setiembre de 2021, de ampliación del Informe Nº 003-2021-GRL-GGR-OEDI-CFSVde fecha 23 de agosto de 2021, emitido por Carlos Fernando Salazar Vigo al Jefe de la Oficina Ejecutiva de Desarrollo Institucional sobre propuesta de Políticas de Seguridad de la Información y Directiva General Nº 001-2021-GRL-GGR-ORTIT sobre Seguridad de la Información del Gobierno Regional de Loreto, señala en sus conclusiones que la propuesta de la directiva cuenta en su formulación con apego a la normativa vigente que le otorga características técnicas de viabilidad, consistencia funcional, y cumple con la Directiva General Nº 011-2017-GRL-GGR/OEDII – Normas para la Formulación, Trámite, Aprobación y Actualización de Directivas;

Que, mediante **Resolución Ejecutiva Regional Nº 163-2017-GRL-P, de fecha 07 de abril de 2017** se aprobó la Directiva General Nº 011-2017-GRL-GGR/OEDII – Normas para la Formulación, Trámite, Aprobación y Actualización de Directivas, donde se establece en el artículo V, numeral V.7), respecto a la aprobación, literal V.7.1) señala: **Las Directivas Generales serán aprobadas por el Gobernador Regional, mediante Resolución Ejecutiva Regional,** facultad que fue delegada a la Gerencia General Regional mediante Resolución Ejecutiva Regional Nº 235-2019-GRL-GR, de fecha 26 de marzo de 2019, en el numeral 1), inciso c) del artículo 1° estableciendo en materia administrativa: Aprobar Directivas e Instructivos para el mejor cumplimiento de las funciones de supervisión, monitoreo y coordinación de ejecución de actividades y proyectos;

Que, en consecuencia, de acuerdo a las normas vertidas líneas arriba, y contando con el Informe favorable de la Oficina Ejecutiva de Desarrollo Institucional respecto a la propuesta de "Políticas de Seguridad de la Información", y Directiva General Nº 001-2021-GRL-GGR-ORTIT sobre Seguridad de la Información del Gobierno Regional de Loreto, el mismo que tiene por objeto establecer el marco general de la Seguridad de la Información en el Gobierno Regional de Loreto y sus áreas descentralizadas, mediante medidas tecnológicas físicas y legales necesarias para proteger la información institucional contra el acceso no autorizado, divulgación, aprovechamiento, intromisión de sistemas o mal uso que se puede producir en forma intencional o accidental, y cumpliendo con todos los requisitos, resulta necesario aprobar mediante acto resolutivo la presente Directiva General;

Estando de acuerdo a la propuesta y al Informe favorable de la Oficina Ejecutiva de Desarrollo Institucional; y con las visaciones de la Oficina Regional de Asesoría Jurídica; y Oficina Regional de Administración del Gobierno Regional de Loreto, y;

Que, en uso de las atribuciones conferidas por el Reglamento de Organización y Funciones del Gobierno Regional de Loreto, aprobado por Ordenanza Regional Nº 022-2017-GRL-CR, de fecha 14 de setiembre de 2017, modificada por la Ordenanza

RESOLUCIÓN GERENCIAL GENERAL REGIONAL N° 344-2021-GRL-GGR.

Belén, 21 de setiembre del 2021

Regional N° 014-2018-GRL-CR, de fecha 10 de mayo del 2018, y a la delegación de facultades a la Gerencia General Regional, mediante Resolución Ejecutiva Regional N° 235-2019-GRL-GR, de fecha 26 de marzo de 2019.

SE RESUELVE:

ARTÍCULO 1°.- APROBAR, la **Directiva General N° 001-2021-GRL-GGR-ORTIT sobre Seguridad de la Información y las Políticas de Seguridad de la Información del Gobierno Regional de Loreto,** cuyo objeto es establecer el marco general de la Seguridad de la Información en el Gobierno Regional de Loreto y sus áreas descentralizadas, mediante medidas tecnológicas físicas y legales necesarias para proteger la información institucional contra el acceso no autorizado, divulgación, aprovechamiento, intromisión de sistemas o mal uso que se puede producir en forma intencional o accidental, los mismos que forman parte integrante de la presente Resolución; en mérito a los fundamentos expuestos en la presente resolución.

ARTICULO 2°.- NOTIFICAR la presente Resolución a las instancias administrativas correspondientes del Gobierno Regional de Loreto.

Regístrese, comuníquese y cúmplase.

GOBIERNO REGIONAL DE LORETO
Econ. Mario Fernando López Tejerina
Gerente General Regional

GOBIERNO REGIONAL DE LORETO

GERENCIA GENERAL REGIONAL

Comité de Gestión de Seguridad de la Información

"POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN DEL GOBIERNO REGIONAL DE LORETO"

(Resolución Gerencial Regional N°344-2021-GRL-GGR)

Oficina Regional de Tecnologías de la Información y Telecomunicación

BELÉN, JUNIO DEL 2021

Contenido

Antecedentes

La información es un activo valioso para el Gobierno Regional de Loreto, y en consecuencia requiere una protección adecuada. La seguridad de la información protege a esta de un amplio rango de amenazas para asegurar la continuidad de las actividades de la Entidad y minimizar daños, y esto se consigue implantando un conjunto adecuado de controles, que pueden ser políticas, normas, procedimientos, estructuras organizativas, herramientas informáticas, entre otros.

La Secretaría de Gobierno Digital de la Presidencia de Consejo de Ministros a dispuesto a través de la Resolución Ministerial Nº 004-2016-PCM, aprueba el uso obligatorio de la Norma Técnica Peruana "NTP ISO/IEC 27001 :2014 Tecnología de la Información. Técnicas de Seguridad. Sistema de Gestión de Seguridad de la Información. Requisitos. 2ª Edición", en todas las entidades integrantes del Sistema Nacional de Informática.

1. Objetivo

Los Lineamientos de Seguridad de la Información tienen como objetivo proteger los recursos de la información del Gobierno Regional de Loreto, y las Tecnologías utilizadas para su procesamiento, frente a amenazas, internas o externas, deliberadas o accidentales, con el fin de minimizar los riesgos de daño y asegurar la confidencialidad, integridad y disponibilidad de la información; así como también garantizar la continuidad de los sistemas de información que la soportan.

Asimismo, debe constituirse en parte de la cultura organizacional del Gobierno Regional de Loreto y las Unidades Ejecutoras, para lo cual se debe asegurar un compromiso manifiesto de los funcionarios y servidores del Gobierno Regional, para la difusión, consolidación y cumplimiento de la presente Política.

De igual manera, el Gobierno Regional de Loreto y las Unidades Ejecutoras, enuncian su compromiso con la Mejora Continua.

2. Alcance

Los Lineamientos de Seguridad de la Información tienen alcance a todos los servidores, funcionarios y proveedores de servicio bajo contrato que tengan acceso o que desarrollen, adquieran o usen sistemas de información, sistemas y/o datos del Gobierno Regional de Loreto y las Unidades Ejecutoras.

Comprende toda la información producida, manejada, transmitida, almacenada y propiedad del Gobierno Regional de Loreto, Unidades Ejecutoras, asimismo, todos los sistemas y datos asociados con el almacenamiento, procesamiento y transmisión de la información, generada por y a favor del Gobierno Regional de Loreto y sus Unidades Ejecutoras.

El presente documento comprende las siguientes políticas específicas:

- Política de Seguridad de la Información.
- Política de Organización de la Seguridad de la Información.
- Política de Seguridad Relativa a los Recursos Humanos.
- Política de Gestión de Seguridad de Activos de Información.
- Política de Control de Accesos.
- Política de Seguridad Física y del Entorno.
- Política de Seguridad de las Operaciones.
- Política de Seguridad de las Comunicaciones.
- Política de Adquisición, Desarrollo y Mantenimiento de Sistemas.
- Política de Relación con Proveedores.
- Política de Gestión de Incidentes de Seguridad de la Información.
- Política de Continuidad de Seguridad de la Información.
- Política de Cumplimiento.

3. Base Legal

- Ley N° 27658, Ley Marco de Modernización de la Gestión del Estado.
- Ley N° 27815, Ley del Código de Ética de la Función Pública.
- Ley Nº 29733, Ley de Protección de Datos Personales.
- Ley Nº 1031, Ley que promueve la eficiencia de la actividad empresarial del Estado y su Reglamento.
- Decreto Supremo Nº 109-2012-PCM, que aprueba la Estrategia para la Modernización de la Gestión Pública.
- Resolución N° 129-2014/CNB-INDECOPI, que aprueba 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"
- 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. Sistema de Gestión de Seguridad de la Información. Requisitos 2ª Edición", en todas las entidades integrantes del Sistema Nacional de Informática.
- Resolución Ejecutiva Regional N°141-2021-GRL-GR, de fecha 03/05/2021; Designación del Funcionario Responsable del Software del GOREL
- Resolución Ejecutiva Regional N°151-2021-GRL-GR, de fecha 03/05/2021; Conformación del Comité de Gestión de la Seguridad de la Información y Designación del Oficial de Seguridad de la Información del GOREL.
- Resolución Ejecutiva Regional N°168-2021-GRL-GR, de fecha 31/05/2021; conformación del Equipo de Respuestas ante Seguridad Digital del GOREL.
- Reglamento Interno de Trabajo / RIT - GOREL

4. Lineamientos

5.1 Responsabilidades Generales

Los Lineamientos de Seguridad de la Información son de cumplimiento obligatorio para todos los servidores designados o asignados bajo cualquier régimen laboral o modalidad contractual, considerando a los proveedores de servicio bajo contrato que tengan acceso o que desarrollen, adquieran o usen sistemas de información.

5.2 Sanciones por Incumplimiento

El Gobierno Regional de Loreto y Unidades Ejecutoras se reservan el derecho de tomar medidas administrativas disciplinarias de los servidores que incumplan con lo dispuesto en los Lineamientos de Seguridad de la Información conforme a las disposiciones señaladas en los documentos normativos de la Entidad, sin perjuicio de las acciones civiles y/o penales que pudieran corresponder.

5.3 Política General de la Seguridad de la Información

El Gobierno Regional de Loreto y sus Unidades Ejecutoras consideran a la información como un activo de vital importancia de la población, promovidos en el ejercicio de sus derechos, el acceso a oportunidades y el desarrollo de sus propias capacidades. En ese contexto, preserva la confidencialidad, integridad y disponibilidad de la información en cada uno de los procesos, a través de incorporación de controles, procedimientos y metodologías definidas, personal capacitado, tecnologías adecuadas y mecanismos de mejora continua en el cumplimiento del marco legal vigente y los estándares internacionales.

5.4 Objetivos de Seguridad de la Información

- Proteger la confidencialidad de la información asegurando que sea accesible a Entidades o Personas debidamente autorizadas.
- Salvaguardar la integridad de la información para garantizar su exactitud y totalidad, así como sus métodos de procesamiento.
- Mantener la disponibilidad de la información y los sistemas de información que soportan los procesos del Gobierno Regional de Loreto y las Unidades Ejecutoras que garantiza que las Entidades o personas debidamente autorizadas tengan acceso a la información cuando lo requieran.
- Establecer, implementar, mantener y mejorar el sistema de gestión de seguridad de la información del Gobierno Regional de Loreto y sus Unidades Ejecutoras.

5.5 Política de Seguridad de la Información

5.5.1 Objetivos

Crear un marco normativo de cumplimiento obligatorio, proporcionar orientación y apoyo a la gestión para la seguridad de la información en concordancia con los requisitos de la operatividad y, las leyes y regulaciones relevantes.

5.5.2 Política

a) Políticas de Seguridad de la Información:

i. El Gobierno Regional de Loreto y sus Unidades Ejecutoras deben elaborar documentos normativos de Seguridad de la Información a fin proteger la información de la Entidad, de considerarlo pertinente.

ii. Los documentos normativos de Seguridad de la Información deben estar alineados a la estrategia de la operatividad, las regulaciones, leyes, normas y amenazas a que estén sujetos como Entidad.

iii. El Oficial de seguridad de la Información del Gobierno Regional de Loreto y sus Unidades Ejecutoras debe monitorear el cumplimiento de la presente política, periódicamente.

b) Revisión de Políticas de Seguridad de la Información:

El Gobierno Regional de Loreto y sus Unidades Ejecutoras debe revisar por lo menos una vez al año, cuando la Entidad lo determina o cuando se produzcan cambios significativos, a fin de asegurar que se mantenga su idoneidad, adecuación y eficacia, en un contexto de mejora continua.

5.6 Política de Organización de la Seguridad de la Información

5.6.1 Objetivos

Establecer un marco de referencia de la gestión para iniciar y controlar la implementación y operación de la seguridad de la información dentro de cada unidad orgánica y órgano desconcentrado.

5.6.2 Política

a) Roles y Responsabilidades:

El Gobierno Regional de Loreto y sus Unidades Ejecutoras debe definir roles y responsabilidades de Seguridad de la Información para la protección de los activos de información, la gestión de riesgos de Seguridad de la Información y la aceptación de los riesgos residuales.

b) Segregación de Funciones:

El Gobierno Regional de Loreto y sus Unidades Ejecutoras debe segregar funciones para reducir oportunidades de modificación no autorizada o no intencional o mal uso de los activos de la organización.

c) Seguridad de la Información en la gestión de proyectos:

La Oficina Regional de Tecnologías de la Información y Telecomunicación del Gobierno Regional de Loreto o la que haga de sus veces y sus Unidades Ejecutoras debe integrar la seguridad de la información en el proceso de gestión de proyectos de la Entidad, para garantizar que los riesgos de seguridad de la información sean identificados y tratados pertinentemente.

5.7 Política de Seguridad Ligada a los Recursos Humanos

5.7.1 Objetivo

Asegurar una correcta gestión de los recursos humanos en el Gobierno Regional de Loreto y sus Unidades Ejecutoras, siendo los servidores parte fundamental del resguardo de la Seguridad de la Información.

5.7.2 Política

a) Antes de la Contratación

i. La Oficina Ejecutiva de Recursos Humanos del Gobierno Regional de Loreto, o la que haga sus veces en las Unidades Ejecutoras, debe verificar los antecedentes laborales y las competencias requeridas para el puesto.

ii. La Oficina Ejecutiva de Recursos Humanos del Gobierno Regional de Loreto, o la que haga sus veces en las Unidades Ejecutoras, deberán establecer en los acuerdos contractuales de empleo, las cláusulas de confidencialidad respecto a la Seguridad de la Información, cláusula respecto a las leyes de derecho de autor o protección de datos, según corresponda.

b) Durante la Contratación

i. La Oficina Ejecutiva de Recursos Humanos del Gobierno Regional de Loreto, o la que haga sus veces en las Unidades Ejecutoras, debe comunicar a los servidores del Gobierno Regional de Loreto, o la que haga sus veces en las Unidades Ejecutoras, sus responsabilidades con respecto a la Seguridad de la Información, siendo responsables de la Seguridad de la Información a la que tienen acceso, según las funciones o actividades que realicen.

ii. La Oficina Ejecutiva de Recursos Humanos del Gobierno Regional de Loreto, o la que haga sus veces en las Unidades Ejecutoras en su interés por proteger su información y los recursos de procesamiento de la misma debe establecer su compromiso de la Entidad, a través de programas de inducción para los nuevos servidores, así como, actualizaciones regulares sobre Políticas y procedimiento.

iii, La Oficina Ejecutiva de Recursos Humanos del Gobierno Regional de Loreto, o la que haga sus veces en las Unidades Ejecutoras, debe comunicar a la Oficina Regional de Tecnologías de la Información y Telecomunicación del Gobierno Regional de Loreto, o la que haga sus veces en las Unidades Ejecutoras, cuando corresponda, el inicio, rotación del vínculo laboral de los servidores para el otorgamiento de acceso a los Sistemas de Información.

iii. La Oficina Ejecutiva de Recursos Humanos del Gobierno Regional de Loreto, o la que haga sus veces en las Unidades Ejecutoras puede iniciar procesos disciplinarios y/o acciones legales pertinentes a los servidores que incumplan las Políticas de Seguridad de la Información y Normativas de Seguridad de la Información establecidos.

c) Después de la Contratación

La Oficina Ejecutiva de Recursos Humanos del Gobierno Regional de Loreto, o la que haga sus veces en las Unidades Ejecutoras, debe comunicar a la Oficina Regional de Tecnologías de la Información y Telecomunicaciones del Gobierno Regional de Loreto, o la que haga sus veces en las Unidades Ejecutoras, cuando corresponda, la finalización del vínculo laboral del servidor al día siguiente de tomado conocimiento de la culminación del vínculo laboral a fin de realizar la desactivación de los accesos a los Sistemas de Información y demás recursos.

5.8 Política de Gestión de Seguridad de Activos de Información

5.8.1 Objetivo

Identificar los activos de información de la Entidad y definir las responsabilidades de protección apropiadas.

5.8.2 Política

a) Inventario de Activos de Información

La Oficina Regional de Tecnologías de la Información y Telecomunicación del Gobierno Regional de Loreto, o quien haga sus veces en las Unidades Ejecutoras, debe mantener un inventario de activos de información actualizada y revisada periódicamente, asimismo, dicho inventario debe contar con un propietario de activo de información que es responsable de la gestión del activo de información durante todo su ciclo de vida.

b) Uso de Activos de Información

i. Los servidores deben usar los activos de información para los fines y objetivos del Gobierno Regional de Loreto y sus Unidades Ejecutoras, de acuerdo con los documentos normativos, la política, y procedimientos que se definan, y considerando criterios de buen uso.

i. En el marco de las relaciones que el Gobierno Regional de Loreto y sus Unidades Ejecutoras establezca con terceros, los convenios, contratos y órdenes, según corresponda, consignarán cláusulas o disposiciones referidas a la confidencialidad de la información que se entregue o a la que tengan acceso.

iii. Todos los órganos y unidades orgánicas del Gobierno Regional de Loreto y sus Unidades Ejecutoras deben cumplir con los requisitos legales, contractuales y normativos relativos al uso de activos de información, incluyendo los lineamientos de seguridad de la información que deben mantenerse alineados con la normatividad vigente.

c) Retorno de Activos de Información

i. La Oficina Ejecutiva de Bienes Registro y Patrimonio del Gobierno Regional de Loreto o quien haga sus veces en las Unidades Ejecutoras debe establecer el procedimiento para el retorno de los activos de información de la Entidad de los servidores que dejan de laborar en la Entidad.

d) Clasificación de la información

i. Los propietarios de activos de información son responsables de clasificar la información que manejan en cada proceso o proyecto, de acuerdo a lo establecido en la Ley de Transparencia y Acceso a la Información Pública.

ii. Los propietarios de los activos de información deberán etiquetar la información según la clasificación realizada, y que sea conforme a los lineamientos que se establezcan en la Entidad.

	DEFINICIÓN	EJEMPLO
Información Confidencial	Aquella información que es considerada como confidencial de acuerdo a lo establecido en el Texto Único Ordenado de la Ley N° 27806 Ley de Transparencia y Acceso a la Información	Incluye a los datos de carácter personal y sensible de servidores, clientes y demás personas naturales sobre las que el Gobierno Regional de Loreto efectúa algún tratamiento de información para un fin determinado declarado como banco de datos personales. Este tipo de información debe estar protegido del acceso no y autorizado.
Información Pública	Aquella información que es de acceso público de acuerdo a lo establecido: en el Texto Único Ordenado de la Ley N°27806, Ley Transparencia y Acceso a la Información Pública El Gobierno Regional de Loreto cataloga esta. información en Información Publicada e Información de Uso Interno	Información Publicada: aquella que de acuerdo a la normativa nacional vigente se encuentra publicada en el Portal de Transparencia estándar. información de Uso Interno: aquella información pública que se encuentra en la Intranet de la Entidad

e) Gestión de Medios Removibles:

i. La Oficina Regional de Tecnologías de la Información y Telecomunicación del Gobierno Regional de Loreto, o quien haga sus veces en las Unidades Ejecutoras, debe establecer el procedimiento para la gestión de medios removibles considerando las labores realizadas por los servidores de acuerdo a la necesidad de uso.

ii. La Oficina Regional de Tecnologías de la Información y Telecomunicación del Gobierno Regional de Loreto, o quien haga sus veces en las Unidades Ejecutoras, debe establecer controles a todo tipo de transferencia de información por medios físicos,

manteniendo lineamientos para los servicios de mensajería y transporte de información en distintos soportes.

5.9 Política de Control de Accesos

5.9.1 Objetivos

a. Garantizar que la autorización de acceso a la información se realice de acuerdo con las atribuciones, funciones y/o tareas a desarrollar por el servidor.
b. Controlar los accesos a la información.
c. Prevenir accesos no autorizados a los sistemas de información y a los servicios de red.

5.9.2 Política

a) Requerimientos para el control de accesos:

La Oficina Regional de Tecnologías de la Información y Telecomunicaciones del Gobierno Regional de Loreto, o la que haga sus veces en las Unidades Ejecutoras, debe establecer que todos los accesos a los recursos de información deben basarse en la necesidad y rol del usuario, tomando en cuenta los siguientes aspectos:

i. Los requerimientos de seguridad de cada una de las aplicaciones.
ii. Identificación de toda la información relacionada con las aplicaciones y los riesgos a la está expuesta.
iii. Uso de perfiles de usuarios estandarizados definidos según roles.
iv. Revisión periódica de los controles de acceso.
v. Revocación de los derechos de acceso.

b) Gestión de acceso del personal:

i. Con el propósito de impedir accesos no autorizados a los recursos de información, la Oficina Regional de Tecnologías de la Información y Telecomunicaciones del Gobierno Regional de Loreto, o la que haga sus veces en las Unidades Ejecutoras, debe establecer procedimientos formales para asignar los derechos de acceso a los sistemas.
ii. Los responsables de las unidades orgánicas son los encargados de autorizar el acceso del servidor a su cargo, a los recursos de tecnologías de información, conforme al procedimiento que se establezca para tal efecto.
iii. La Oficina Regional de Tecnologías de la Información y Telecomunicaciones del Gobierno Regional de Loreto, o la que haga sus veces en las Unidades Ejecutoras, debe asignar un usuario y

contraseña que identifique única y exclusivamente al servidor para el uso de los recursos informáticos, ya sea de forma temporal o permanente.

iv. La Oficina Regional de Tecnologías de la Información y Telecomunicaciones del Gobierno Regional de Loreto, o la que haga sus veces en las Unidades Ejecutoras, debe definir normas y procedimientos de control a nivel de sistema operativo de red, de manera que no se compartan identificadores entre diferentes usuarios ni pueda detectarse la duplicidad de sesiones de usuarios.

v. La Oficina Regional de Tecnologías de la Información y Telecomunicaciones del Gobierno Regional de Loreto, o la que haga sus veces en las Unidades Ejecutoras, debe establecer, en sus respectivos ámbitos, las normas y procedimientos para la asignación y cambio de contraseñas. Al respecto, se informa al servidor sobre lo siguiente:

- Debe seleccionar secuencias de caracteres o palabras claras y fáciles de recordar. Se debe considerar una longitud mínima de 8 caracteres considerando un número, un carácter alfanumérico y caracteres especiales cuando menos.
- No debe considerar información relacionada directamente con el usuario (nombre, fecha de nacimiento, teléfono, etc.).
- Cada servidor es responsable de la confidencialidad de la contraseña asignada, y de las consecuencias por las acciones que, mediante su uso, terceras personas pueden realizar.
- Las contraseñas son estrictamente personal e intransferible y el servidor es responsable de mantener su confidencialidad.

c) Control de acceso a las redes informáticas:

i. El acceso a los recursos de red, internos y externos, debe ser controlado por la Oficina Regional de Tecnologías de la Información y Telecomunicaciones del Gobierno Regional de Loreto o la que haga sus veces en las Unidades Ejecutoras, de manera que el servidor no comprometa la seguridad de los activos de información.

ii. Para la seguridad en las redes informáticas, se deben tener en cuenta los siguientes aspectos:
- Lineamientos de uso de la red.
- Segmentación de redes.
- Control de conexiones a redes en base a la política.
- Controles de enrutamiento de redes.

d) Control de acceso a los sistemas operativos:

i. El acceso a los sistemas operativos de las estaciones de trabajo del Gobierno Regional de Loreto, o la que haga sus veces en las Unidades Ejecutoras, debe ser debidamente controlado por la Oficina Regional de Tecnologías de la Información y Telecomunicaciones del

Gobierno Regional de Loreto, o la que haga sus veces en las Unidades Ejecutoras, a fin de evitar accesos no autorizados a recursos o información.

ii. Dentro de los aspectos que deben ser tomados en consideración para definir los controles, se incluyen:
- Identificación automática de estación de trabajo.
- Procedimientos de inicio de sesión seguros.
- Identificación y autenticación de usuarios.
- Sistema de gestión de contraseñas.
- Restricción del uso de herramientas utilitarias del sistema operativo con capacidades de eludir y/o sobrescribir los controles de seguridad.

e) Control de acceso a las aplicaciones:

I. La Oficina Regional de Tecnologías de la Información y Telecomunicaciones del Gobierno Regional de Loreto o la que haga sus veces en los Programas Sociales, debe establecer los lineamientos de control de accesos a la información y a las aplicaciones, restringiendo para uso exclusivo del personal debidamente autorizado; asimismo, revisar periódicamente los accesos concedidos, revocando los derechos cuya vigencia de autorización haya caducado.

II. Se deben aislar los sistemas identificados con información sensible, asignándoles un entorno de procesamiento dedicado, creado a partir de métodos físicos o lógicos.

f) Conexiones externas:

En cualquier caso, para el acceso remoto (todo acceso a la información del Gobierno Regional de Loreto y sus Unidades Ejecutoras fuera del centro de trabajo) se debe utilizar la tecnología y acceso seguro (VPN) y su uso debe ser autorizado solo en caso de ser necesario por el jefe del órgano o unidad orgánica y la Oficina Regional de Tecnologías de la Información y Telecomunicación, o la que haga sus veces en las Unidades Ejecutoras, con el conocimiento del Oficial de Seguridad de la Información.

5.10 Política de Seguridad Física y del Entorno

5.10.1 Objetivo

Tomar las medidas necesarias para evitar el acceso físico no autorizado, los daños e interferencia a la información de la Entidad y a los recursos de tratamiento de la información.

5.10.2 Política

a) El servidor del Gobierno Regional de Loreto y sus Unidades Ejecutoras que atienda a personas externas a la Entidad (incluyendo suministradores) debe asegurar que los datos de todas las visitas de personas externas a la Entidad quedan anotados en el registro de visitas.

b) La Oficina Regional de Tecnologías de la Información y Telecomunicaciones del Gobierno Regional de Loreto, o la que haga sus veces en las Unidades Ejecutoras, debe implementar controles Biométricos al Centro de Datos para su debida protección.

c) La Oficina Regional de Tecnologías de la Información y Telecomunicaciones del Gobierno Regional de Loreto o la que haga sus veces en las Unidades Ejecutoras, debe establecer una clasificación de las áreas para definir el nivel de seguridad de las mismas, las cuales se describen a continuación:

AREA	DESCRIPCION
Restringida	Son zonas seguras donde la información que se genera, trata o almacena es crítica para la Entidad. Los accesos a estos despachos son controlados
Común	Son zonas de uso común para el servidor del Gobierno Regional de Loreto
Pública	Son zonas que son de utilización pública y de recepción de personas externas a la Entidad

c) Toda persona externa al Gobierno Regional de Loreto y sus Unidades Ejecutoras puede acceder a las áreas definidas como restringidas, siempre que cuente con la autorización respectiva del jefe del órgano o unidad orgánica y debe estar siempre acompañado por un servidor de la Entidad.

d) El servidor del Gobierno Regional de Loreto y en sus Unidades Ejecutoras debe portar en todo momento su fotocheck para su debida identificación.

e) Los visitantes que ingresan a las instalaciones del Gobierno Regional de Loreto y en sus Unidades Ejecutoras deben portar en todo momento su pase de visita.

f) El personal de Gobierno Regional de Loreto y sus Unidades Ejecutoras debe seguir el procedimiento establecido de Gestión de Bienes establecido en cada Entidad para el retiro de un equipo de cómputo.

g) Todos los equipos de cómputo que ingresan al Gobierno Regional de Loreto y a sus Unidades Ejecutoras debe ser previamente registrados por el personal de seguridad responsable.

i) El Gobierno Regional de Loreto y a sus Unidades Ejecutoras a través de los Órganos u Unidades Orgánicas de acuerdo a su responsabilidad debe de implementar medidas de protección contra amenazas externas y ambientales, dichas medidas de protección, debe incluir:
   - Controles de acceso y seguridad física
   - Detectores de humo. Extintores
   - Sistema de alimentación ininterrumpida (UPS)
   - Sistema de puesta a Tierra
   - Sensores de aniego
   - Grupo Electrógeno
   - Pararrayos (Unidades ubicadas en las zonas que el clima lo requiera)

j) La Oficina Regional de Tecnologías de la Información y Telecomunicaciones del Gobierno Regional de Loreto o la que haga sus veces en las Unidades Ejecutoras, debe proteger los equipos de Tecnologías de la Información de fallas por falta de suministro de energía y otras anomalías eléctricas.

k) La Oficina Regional de Tecnologías de la Información y Telecomunicaciones del Gobierno Regional de Loreto o la que haga sus veces en las Unidades Ejecutoras, debe proteger el cableado de la red de comunicaciones y suministro de energía para evitar intercepción o daño.

l) El cableado de suministro de energía eléctrica y telecomunicaciones en las zonas de tratamiento de información, debe contar con un sistema de pozo a tierra, el que debe ser revisado periódicamente para garantizar su adecuado funcionamiento.

m) La Oficina Regional de Tecnologías de la Información y Telecomunicaciones del Gobierno Regional de Loreto, o la que haga sus veces en las Unidades Ejecutoras, debe mantener un programa de mantenimiento de los equipos de Tecnologías de información y de los sistemas de acondicionamiento de temperatura, humedad y filtrado de aire, sistemas de energía ininterrumpida (UPS) y sistemas de detección y extinción de fuego del Data Center, a fin de garantizar la continuidad de los servicios.

n) La Oficina Regional de Tecnologías de la Información y Telecomunicación del Gobierno Regional de Loreto, o la que haga sus veces en las Unidades Ejecutoras, debe implementar una Política de Escritorio Limpio y Pantalla Limpia, a fin de evitar el acceso no autorizado y el uso indebido de la información.

5.11 Política de Seguridad de las Operaciones

5.11.1 Objetivo

Asegurar que las operaciones de instalaciones de procesamiento de la información sean correctas y seguras

5.11.2 Política

a) Procedimientos Operativos Documentados:

La Oficina Regional de Tecnologías de la Información y Telecomunicaciones del Gobierno Regional de Loreto o la que haga sus veces en las Unidades Ejecutoras, debe documentar procesamientos operativos, estableciendo las responsabilidades y los recursos utilizados para su ejecución eficiente, asimismo, estos deberán estar a disposición de los servidores autorizados.

b) Gestión de Cambios:

I. La Oficina Regional de Tecnologías de la Información y Telecomunicación del Gobierno Regional de Loreto o la que haga sus veces en los Programas Sociales, debe mantener un registro de control de cambios de los sistemas, equipos de comunicación, bases de datos, equipos de cómputo y perfiles de acceso, a través de la implementación de acciones y procedimientos orientados a asegurar que todo cambio siga un proceso planificado que incluya responsabilidades y canales de comunicación, identificación de los recursos comprometidos, pruebas de comprobación y estrés, controles de seguridad, reversión en caso de fallas y análisis de impacto.

II. Todos los cambios deben ser solicitados a la Oficina Regional de Tecnologías de la Información y Telecomunicaciones del Gobierno Regional de Loreto, o la que haga sus veces en las Unidades Ejecutoras, por el propietario de la Información, y se llevará un registro sobre cada solicitud de cambio. En caso existiera algún problema con el cambio realizado, se revertirá al estado anterior al cambio.

c) Gestión de la Capacidad:

La Oficina Regional de Tecnologías de la Información y Telecomunicaciones del Gobierno Regional de Loreto, o la que haga sus veces en las Unidades Ejecutoras, debe garantizar la capacidad de los

recursos a fin de asegurar el desempeño requerido de los Sistemas de Información.

d) Separación de Entornos:

i. La Oficina Regional de Tecnologías de la Información y Telecomunicaciones del Gobierno Regional de Loreto, o la que haga sus veces en las Unidades Ejecutoras, debe separar entornos de desarrollo, pruebas y producción a fin de prevenir riesgos de acceso no autorizado o cambios al entorno operativo.

ii. La Oficina Regional de Tecnologías de la Información y Telecomunicaciones del Gobierno Regional de Loreto, o la que haga sus veces en las Unidades Ejecutoras, debe definir y documentar procedimientos para pases de desarrollo a producción, asimismo, el entorno de pruebas debe ser en lo posible, igual al ambiente de producción en lo referido a recursos de Tecnologías de información.

e) Protección contra Software Malicioso:

i. La Oficina Regional de Tecnologías de la Información y Telecomunicaciones del Gobierno Regional de Loreto, o la que haga sus veces en las Unidades Ejecutoras, debe adoptar las medidas necesarias para la prevención, detección y eliminación de código malicioso (malware) a nivel de servidores de red, computadoras portátiles, estaciones de trabajo, tabletas, Smartphone, etc.

ii. La Oficina Regional de Tecnologías de la Información y Telecomunicaciones del Gobierno Regional de Loreto, o la que haga sus veces en los Unidades Ejecutoras, debe asegurar que todas las estaciones de trabajo estén protegidas con el antivirus corporativo y que éste se encuentre actualizado. Asimismo, debe garantizar que el sistema operativo y los aplicativos de oficina cuenten con las últimas actualizaciones de seguridad (parches).

iii. La Oficina Regional de Tecnologías de la Información y Telecomunicaciones del Gobierno Regional de Loreto, o la que haga sus veces en las Unidades Ejecutoras, es responsable de la renovación de licencias de software, y debe definir su cronograma de renovación, para evitar que se produzca incumplimiento de uso ilegal de software.

iv. El Software utilizado por el Gobierno Regional de Loreto y en las Unidades Ejecutoras debe ser autorizado en forma expresa por la Oficina Regional de Tecnologías de la Información y Telecomunicaciones del Gobierno Regional de Loreto, o la que haga sus veces en las Unidades Ejecutoras, de corresponder.

v. El personal de soporte técnico de la Oficina Regional de Tecnologías de la Información y Telecomunicaciones del Gobierno Regional de Loreto, o la que haga sus veces en las Unidades Ejecutoras, como medida de prevención, si detecta que alguna estación de trabajo o computadora portátil se encuentra infectada con algún tipo de malware, debe de aislarla inmediatamente, desconectándola de la red corporativa.

f) Respaldo de Información:

i. La Oficina Regional de Tecnologías de la Información y Telecomunicaciones del Gobierno Regional de Loreto, o la que haga sus veces en las Unidades Ejecutoras, debe establecer procedimientos rutinarios para el respaldo de la información, de acuerdo con su criticidad, realizando copias de seguridad y pruebas de recuperación, conforme a un cronograma definido.

ii. La Oficina de Tecnologías de la Información del Gobierno Regional de Loreto, o la que haga sus veces en las Unidades Ejecutoras, debe resguardar las copias de seguridad en un ambiente distinto al de la Entidad (es decir, fuera de las instalaciones de la Entidad), que reúna las condiciones adecuadas de acondicionamiento, temperatura y humedad.

iii. La Oficina Regional de Tecnologías de la Información y Telecomunicaciones del Gobierno Regional de Loreto, o la que haga sus veces en las Unidades Ejecutoras, debe asegurar que los equipos y los medios de respaldo cuentan con un programa de mantenimiento preventivo y correctivo para asegurar su correcto funcionamiento.

iv. La Oficina Regional de Tecnologías de la Información y Telecomunicaciones del Gobierno Regional de Loreto, o la que haga sus veces en las Unidades Ejecutoras, debe estimar anticipadamente la cantidad necesaria de medios magnéticos u otros requeridos para realizar las copias de respaldo y, en caso de no contar con ello, solicitar su oportuna adquisición.

v. La Oficina Regional de Tecnologías de la Información y Telecomunicaciones del Gobierno Regional de Loreto, o la que haga sus veces en las Unidades Ejecutoras, debe mantener el registro actualizado de las operaciones de gestión de respaldo y recuperación, así como de las fallas que pudieran presentarse y las soluciones realizadas, a través del personal de soporte técnico.

vi. La Oficina Regional de Tecnologías de la Información y Telecomunicaciones del Gobierno Regional de Loreto, o la que haga sus veces en las Unidades Ejecutoras debe de realizar pruebas de restauración a las copias de seguridad a fin de asegurar que se pueda obtener correctamente la información almacenada al momento de ser necesaria.

vii. La Oficina Regional de Tecnologías de la Información y Telecomunicaciones del Gobierno Regional de Loreto, o la que haga sus veces en las Unidades Ejecutoras, debe revisar periódicamente la vigencia tecnológica de los equipos y software utilizados para el respaldo y recuperación de la información.

g) Registro y Monitoreo:

i. Todos los servicios informáticos se encuentran sujetos a monitoreo por parte de la Oficina Regional de Tecnologías de la Información y Telecomunicaciones del Gobierno Regional de Loreto, o la que haga sus veces en las Unidades Ejecutoras.

ii. La Oficina Regional de Tecnologías de la Información y Telecomunicaciones del Gobierno Regional de Loreto, la que haga sus veces en las Unidades Ejecutoras, debe generar registros de auditoría sobre el uso de los recursos de Tecnologías de información.

iii. Las actividades de los operadores y administradores de los sistemas de la Oficina Regional de Tecnologías de la Información y Telecomunicaciones del Gobierno Regional de Loreto, o la que haga sus veces en las Unidades Ejecutoras, debe ser monitoreadas, registradas, verificadas regular y periódicamente por la Oficina Regional de Tecnologías de la Información y Telecomunicaciones del Gobierno Regional de Loreto, o la que haga sus veces en las Unidades Ejecutoras.

iv. La Oficina Regional de Tecnologías de la Información y Telecomunicaciones del Gobierno Regional de Loreto, o la que haga sus veces en las Unidades Ejecutoras, debe contar con registro de fallas en los sistemas de información para seguimiento, registros de auditoría y monitoreo pertinente.

v. Cada servidor del Gobierno Regional de Loreto y sus Unidades Ejecutoras es responsable de las actividades realizadas a través de sus cuentas de acceso de red, correo electrónico, sistemas de información asociados y sistemas.

h) Sincronización de Reloj:

La Oficina Regional de Tecnologías de la Información y Telecomunicaciones del Gobierno Regional de Loreto, o la que haga sus veces en las Unidades Ejecutoras, debe mantener sincronizado los relojes en los Sistemas de Información con una fuente exacta que establece la "Hora Oficial de la República del Perú", a fin de garantizar la exactitud de los registros.

i) Control de Software Operacional:

La Oficina Regional de Tecnologías de la Información y Telecomunicaciones del Gobierno Regional de Loreto, o la que haga sus veces en las Unidades Ejecutoras, debe implementar mecanismos de restricción para la instalación de software en los equipos de cómputo por parte de los usuarios no autorizados.

j) Controles de Auditoria de los Sistemas de Información:

i. Todos los servicios informáticos se encuentran sujetos a monitoreo por parte de la Oficina Regional de Tecnologías de la Información y Comunicación, o la que haga sus veces en las Unidades Ejecutoras.

ii. La Oficina Regional de Tecnologías de la Información y Telecomunicaciones del Gobierno Regional de Loreto, o la que haga sus veces en las Unidades Ejecutoras, debe generar registros de auditoría sobre el uso de los recursos de Tecnologías de información.

5.12 Política de Seguridad de las Comunicaciones

5.12.1 Objetivo

a) Asegurar la protección de la información en las redes y sus instalaciones de procesamiento de la información de apoyo.

b) Proteger la información de las redes y la infraestructura que la soporta.

c) Monitorear las actividades de procesamiento de información no autorizadas.

5.12.2 Política

a) La Oficina Regional de Tecnologías de la Información y Telecomunicaciones del Gobierno Regional de Loreto, o quien haga sus veces en las Unidades Ejecutoras, debe implementar mecanismos de control y procedimientos necesarios para proveer la disponibilidad de las redes de datos y de los servicios que dependen de ellas; asimismo, vela por que se cuente con controles de seguridad que protejan la

integridad y la confidencialidad de la información que se transporta a través de dichas redes de datos.

b) La Oficina Regional de Tecnologías de la Información y Telecomunicaciones del Gobierno Regional de Loreto, o quien haga sus veces en las Unidades Ejecutoras debe realizar la segregación de redes, a fin de garantizar su debida protección.

c) Seguridad de Correo Electrónico

i. La Oficina Regional de Tecnologías de la Información y Telecomunicaciones del Gobierno Regional de Loreto, o quien haga sus veces en las Unidades Ejecutoras, puede efectuar la desactivación de la cuenta de correo electrónico institucional por algún uso indebido que transgreda lo establecido en el presente documento.

ii. Cada servidor o funcionario es responsable por la información que se transmita desde la cuenta de correo electrónico que le haya asignado la Entidad.

iii. En caso el servidor reciba mensajes con asuntos sospechosos y/o de origen desconocido, estos no deben ser abiertos y deben comunicar inmediatamente a la Oficina Regional de Tecnologías de la Información y Telecomunicaciones del Gobierno Regional de Loreto, o la que haga sus veces en las Unidades Ejecutoras, según corresponda, así como al Oficial de Seguridad de la Información para los fines correspondientes y luego deben ser eliminados

iv. El servidor debe usar firmas estandarizadas, de conformidad con el Manual de Entidad Corporativa del Gobierno Regional de Loreto.

v. El envío de mensajes masivos de correo electrónico dentro de la Entidad está permitido solo para el personal o dependencias autorizados por la Oficina Regional de Tecnologías de la Información y Telecomunicaciones del Gobierno Regional de Loreto, o quien haga sus veces en las Unidades Ejecutoras.

d) Acuerdo de Confidencialidad

La Oficina de Tecnologías de la Información y Telecomunicaciones del Gobierno Regional de Loreto, o la que haga sus veces en las Unidades Ejecutoras, asegura la protección de la información en el momento de ser transferida o intercambiada y establece los procedimientos y controles necesarios para el intercambio de información; asimismo, se establecen Acuerdos de Confidencialidad y/o de Intercambio de Información con terceras partes y/o con quienes corresponda.

La Oficina Regional de Tecnologías de la Información y Telecomunicaciones del Gobierno Regional de Loreto, o la que haga sus veces en las Unidades Ejecutoras, vela por el uso de Tecnologías informáticas y de telecomunicaciones para llevar a cabo el intercambio de información; de acuerdo a lo establecido en los acuerdos que contraiga.

5.13 Política de Adquisición, Desarrollo y Mantenimiento de Sistemas

5.13.1 Objetivos

a) Asegurar que los sistemas cumplan con los requisitos de seguridad de la Entidad.

b) Evitar pérdidas, modificaciones o mal uso de la información que se encuentra dentro de los sistemas.

c) Proteger la confidencialidad, autenticidad e integridad de los sistemas del sector.

5.13.2 Política

a) Metodología para la adquisición, desarrollo y mantenimiento de los sistemas:

i. La Oficina Regional de Tecnologías de la Información y Telecomunicaciones del Gobierno Regional de Loreto, o la que haga sus veces en las Unidades Ejecutoras, debe aprobar un procedimiento para la adquisición, desarrollo y mantenimiento de los sistemas.

ii. Todo desarrollo y/o mantenimiento de sistemas debe ser documentado, con la finalidad de que personas no familiarizadas con ellas en el Gobierno Regional de Loreto y en sus Unidades Ejecutoras, ejecuten las actividades con facilidad.

b) Requisitos de seguridad de los sistemas:

i. La Oficina Regional de Tecnologías de la Información y Telecomunicaciones del Gobierno Regional de Loreto, o la que haga sus veces, debe definir un procedimiento que incluya controles de seguridad durante las etapas de análisis y diseño de los sistemas.

ii. Todo sistema desarrollado por los servidores de la Oficina Regional de Tecnologías de la Información y Telecomunicaciones del Gobierno Regional de Loreto, o de la que haga sus veces, o por terceros, debe satisfacer los requisitos de seguridad definidos para el desarrollo y mantenimiento de los sistemas. En el caso de los terceros, el desarrollo de los sistemas debe constar en el respectivo contrato de prestación de servicios.

iii. El servidor debe cumplir los controles, estándares y metodologías referidas al desarrollo de los sistemas seguras que se hayan implementado.

iv. La Oficina Regional de Tecnologías de la Información y Telecomunicaciones del Gobierno Regional de Loreto, o la que haga sus veces en las Unidades Ejecutoras, debe verificar que los acuerdos sobre materia informática a suscribir con terceros, incluyan cláusulas relativas a la cesión de derechos y confidencialidad de la información, para el resguardo de la propiedad intelectual del Gobierno Regional de Loreto y de sus Unidades Ejecutoras.

iv. Los acuerdos que involucran el acceso, procesamiento, comunicación o manejo de terceros de las instalaciones de procesamiento de información, deben cubrir los requisitos de seguridad necesarios.

v. Todos los sistemas desarrollados por los servidores son de propiedad del Gobierno Regional de Loreto y de los órganos según corresponda.

c) Procesamiento correcto de los sistemas:

i. La Oficina de Tecnologías de la Información y Telecomunicaciones del Gobierno Regional de Loreto, o la que haga sus veces en las Unidades Ejecutoras, debe implementar controles de seguridad apropiados en los sistemas utilizadas por el Gobierno Regional de Loreto, o sus Unidades Ejecutoras para validar los datos de entrada, el procesamiento interno y los datos de salida.

ii. La Oficina de Tecnologías de la Información y Telecomunicaciones del Gobierno Regional de Loreto, o la que haga sus veces en las Unidades Ejecutoras, debe identificar los requerimientos para asegurar la autenticidad y la integridad de los mensajes en los sistemas, debiendo definirse e implementarse los controles apropiados.

d) Seguridad de los archivos de los sistemas:

La Oficina Regional de Tecnologías de la Información y Telecomunicaciones del Gobierno Regional de Loreto, o la que haga sus veces en las Unidades Ejecutoras, deben implementar controles sobre lo siguiente:

i. Control de los sistemas en Producción: Comprende la formulación y puesta en práctica de procedimientos orientados a controlar la instalación de los sistemas en producción.

ii. Protección de Datos de Prueba: Los datos de prueba de los sistemas deben ser cuidadosamente seleccionados, protegidos y controlados.

e) Control de acceso al Código Fuente de los sistemas:

La Oficina Regional de Tecnologías de la Información y Telecomunicaciones del Gobierno Regional de Loreto, o la que haga sus veces en las Unidades Ejecutoras, deben implementar los siguientes controles:

I. Restringir y controlar el acceso al código fuente de los sistemas o programas.

iii. Contar con un responsable del acceso al código fuente de los sistemas, quien debe implementar un registro de uso, si es que el código es requerido.

f) Uso de controles criptográficos:

La Oficina Regional de Tecnologías de la Información y Telecomunicaciones del Gobierno Regional de Loreto, o la que haga sus veces en las Unidades Ejecutoras, debe implementar el uso de controles para cifrar la información y proteger la confidencialidad, autenticidad e integridad de la misma, cuando sea requerido, y de acuerdo al nivel de exposición al riesgo.

g) Seguridad en los procesos de desarrollo y pase a producción:

i. Procedimiento para el desarrollo de los sistemas:
Todo el desarrollo y mantenimiento de los sistemas en el Gobierno Regional de Loreto y de sus Unidades Ejecutoras deben ser realizados conforme a los procedimientos establecidos, debiendo considerarse la NTP ISO/IEC 12207 y otros estándares pertinentes.

ii. Procedimiento para pase a producción:

- Los servidores encargados del desarrollo y mantenimiento de los sistemas, así como los terceros, no tendrá acceso a los datos de producción.

- Los ambientes de desarrollo y producción deben ser configurados en servidores diferentes, limitando el acceso solo al personal autorizado

- El pase a producción debe ser realizado exclusivamente por la persona autorizada por la Oficina Regional de Tecnologías de la Información y Telecomunicaciones del Gobierno Regional de Loreto, o la que haga sus veces en las Unidades Ejecutoras, quien lleva un control de los pases efectuados y/o actualizaciones de los sistemas en un registro o bitácora.

- Todo desarrollo, antes de su pase a producción, debe ser revisado por la Oficina Regional de Tecnologías de la Información y Telecomunicaciones del Gobierno Regional de Loreto, o la que haga sus veces en las Unidades Ejecutoras, para asegurar que se cumplan los estándares establecidos.

h) Control de cambios de los sistemas:

i. El control, registro y monitoreo de los cambios de los sistemas del Gobierno Regional de Loreto y de sus Unidades Ejecutoras debe ser supervisado y registrado por la Oficina de Tecnologías de la Información y Telecomunicaciones del Gobierno Regional de Loreto, o la que haga sus veces en las Unidades Ejecutoras.

ii. Todo acceso a la librería de los programas fuente debe ser controlado por la Oficina Regional de Tecnologías de la Información y Telecomunicaciones del Gobierno Regional de Loreto, o la que haga sus veces en las Unidades Ejecutoras, a fin de evitar accesos y/o cambios no autorizados.

i) Gestión de vulnerabilidades técnicas:

i. La Oficina Regional de Tecnologías de la Información y Telecomunicaciones del Gobierno Regional de Loreto, o la que haga sus veces en las Unidades Ejecutoras, debe programar la realización de pruebas de comprobación técnica a cargo de especialistas para verificar que se han implementado correctamente los controles de seguridad definidos para el hardware y software.

ii. Identificadas las vulnerabilidades técnicas, la Oficina Regional de Tecnologías de la Información y Telecomunicaciones del Gobierno

Regional de Loreto, o la que haga sus veces en las Unidades Ejecutoras, debe determinar los nesgas asociados e implementar los controles necesarios para mitigarlos. Los sistemas críticos y en alto riesgo deben ser tratadas primero.

iii. Para los sistemas que requieren una actualización de seguridad (parches), la Oficina Regional de Tecnologías de la Información y Telecomunicaciones del Gobierno Regional de Loreto, o la que haga sus veces en las Unidades Ejecutoras, debe probar y evaluar su efectividad en un ambiente de pruebas; asimismo, se deben considerar los riesgos asociados a su aplicación y, en todas las cosas, se deben cumplir los controles establecidos para la gestión de cambios.

5.14 Política de Relación con Proveedores

5.14.1 Objetivo

Garantizar la protección de los activos de información del Gobierno Regional de Loreto y de sus Unidades Ejecutoras, que son accesibles por los Proveedores.

5.14.2 Política

a) Todo proveedor que brinde servicios a Gobierno Regional de Loreto y a sus Unidades Ejecutoras, debe suscribir un acuerdo de confidencialidad, la misma que será parte del contrato de prestación de servicios como anexo.

b) Los proveedores sólo podrán desarrollar para Gobierno Regional de Loreto o sus Unidades Ejecutoras, aquellas actividades cubiertas bajo el correspondiente contrato u orden de prestación de servicios.

c) El proveedor debe proporcionar los datos completos de la persona de contacto, quien se encarga de recibir todo tipo de directivas de seguridad de la información.

d) El proveedor proporciona mensualmente, mientras dure la vigencia del contrato, la relación de personas, perfiles, funciones y responsabilidades asociadas al servicio provisto, e informa puntualmente de cualquier cambio (alta, baja, sustitución o cambio de funciones o responsabilidades) que se produzca en dicha relación.

e) Todo proveedor de servicios debe velar porque su personal que presta los servicios directamente a Gobierno Regional de Loreto y a sus Unidades Ejecutoras, cumpla con las políticas de seguridad de la

información recogidas en el presente documento. En caso de incumplimiento, Gobierno Regional de Loreto se reserva el derecho de solicitar al proveedor el cambio de personal, sin perjuicio del derecho de Gobierno Regional de Loreto o la que haga sus veces en las Unidades Ejecutoras, de resolver el contrato de prestación de servicios en los términos establecidos en el contrato.

f) Cualquier tipo de intercambio de información que se produzca entre el Gobierno Regional de Loreto, o la que haga sus veces en las Unidades Ejecutoras y el proveedor se debe entender que ha sido realizado dentro del marco establecido por el contrato u orden de prestación de servicios, de modo que dicha información tendrá el carácter de confidencial y no podrá ser utilizada en ningún caso fuera de dicho marco, ni para fines diferentes a los asociados al contrato.

g) Todo proveedor que tenga acceso a la información del Gobierno Regional de Loreto, o la que haga sus veces en las Unidades Ejecutoras, en ejecución de un contrato u orden de prestación de servicios, debe considerar que dicha información, es confidencial y sujeto a la Ley de Protección de Datos Personales.

h) Ningún proveedor puede utilizar la información del Gobierno Regional de Loreto y sus Unidades Ejecutoras para beneficio propio o de terceros. La información a la que tenga acceso el proveedor, únicamente puede ser utilizada para os fines específicamente indicados en el contrato u orden de prestación de servicios. Toda información proporcionada por el Gobierno Regional de Loreto u Unidades Ejecutoras, sigue siendo de propiedad de esta última.

i) El proveedor y su personal únicamente puede utilizar la información y activos tecnológicos autorizados por el Gobierno Regional de Loreto o de sus Unidades Ejecutoras para el desarrollo de los servicios contratados.

j) La distribución de la información ya sea en formato digital o papel, se realiza mediante los recursos determinados en el contrato de prestación de servicios y para la finalidad exclusiva de facilitar las funciones asociados a dicho contrato. El Gobierno Regional de Loreto y sus Unidades Ejecutoras, se reserva, en función del riesgo identificado, la implementación de medidas de control, registro y auditoría sobre los recursos de difusión.

k) Los recursos que el Gobierno Regional de Loreto o de las Unidades Ejecutoras que pone a disposición del proveedor, independientemente del tipo que sean, (informáticos, datos, software, redes, sistemas de comunicación, etc.) están exclusivamente destinados para cumplir con las obligaciones y propósito para los que fueron proporcionados.

Gobierno Regional de Loreto y sus Unidades Ejecutoras se reservan el derecho de implementar mecanismos de control y auditoría que verifiquen el uso apropiado de estos recursos.

l) El proveedor debe notificar a la Oficina Regional de Tecnologías de la Información y Telecomunicaciones del Gobierno Regional de Loreto, o la que haga sus veces en las Unidades Ejecutoras, cualquier incidencia que se detecte y que afecte o pueda afectar a la seguridad de la Información de la Entidad.

5.15 Política de Gestión de Incidentes de Seguridad de la Información

5.15.1 Objetivo

Asegurar que los incidentes de seguridad de la información del Gobierno Regional de Loreto y los de sus Unidades Ejecutoras sean comunicados oportunamente a las instancias correspondientes, con la finalidad de adoptar acciones preventivas y correctivas que correspondan.

5.15.2 Política

a) Los incidentes relativos a la seguridad de la información deben ser comunicados a la Oficina Regional de Tecnologías de la Información y Telecomunicaciones del Gobierno Regional de Loreto, o la que haga sus veces en las Unidades Ejecutoras y al Oficial de Seguridad de la Información, conforme al procedimiento que se establezca para tal efecto.

b) El servidor del Gobierno Regional de Loreto y de sus Unidades Ejecutoras deben conocer el procedimiento de gestión de incidentes de seguridad de la información, e informar de su ocurrencia tan pronto tome conocimiento de ellos.

c) Cualquier servidor del Gobierno Regional de Loreto y de sus Unidades Ejecutoras debe comunicar al Oficial de Seguridad de la Información del Gobierno Regional de Loreto, o la que haga sus veces en las Unidades Ejecutoras las sugerencias, debilidades, vulnerabilidades y/o situaciones de riesgo que puede tener relación con la seguridad de la información y las directrices contempladas en las presentes políticas de las que tenga conocimiento.

d) El servidor del Gobierno Regional de Loreto y sus Unidades Ejecutoras deben conocer su responsabilidad respecto a la comunicación de los incidentes de seguridad que tome conocimiento, debiendo ser notificados de los resultados una vez que el incidente haya sido resuelto.

e) Reportados los incidentes de seguridad de la información a la Oficina Regional de Tecnologías de la Información y Telecomunicaciones del Gobierno Regional de Loreto, o la que haga sus veces en los Unidades Ejecutoras, y al Oficial de Seguridad de la Información, debe proceder a su exhaustivo análisis por parte del servidor que designe la referida oficina o dependencia del programa, a efectos de adoptar las acciones que correspondan.

f) Los incidentes de seguridad serán evaluados por el Oficial de Seguridad del Gobierno Regional de Loreto y de sus Unidades Ejecutoras, a efectos de proponer las acciones preventivas que correspondan, para lo sucesivo.

g) Periódicamente, la Oficina Regional de Tecnologías de la Información y Telecomunicaciones del Gobierno Regional de Loreto o la que hagas sus veces en las Unidades Ejecutoras, debe analizar las actividades realizadas y estudiar posibles mejoras cambios que puedan proponerse al Comité de Gestión de Seguridad de la Información para prevenir la ocurrencia de futuros incidentes de Seguridad de la Información.

5.16 Política de Continuidad de la Seguridad de la Información

5.16.1 Objetivo

a) Preservar la seguridad de la información durante las fases de activación, de desarrollo de procesos, procedimientos y planes para la continuidad de la operatividad y de vuelta a la normalidad.

b) Garantizar la disponibilidad de los recursos de tratamiento de la información.

5.16.2 Política

a) La Oficina Regional de Tecnologías de la Información y Telecomunicaciones del Gobierno Regional de Loreto, o quien haga sus veces en las Unidades Ejecutoras, debe incluir la continuidad de la seguridad de la información dentro del proceso de gestión de continuidad operativa.

b) La Oficina Regional de Tecnologías de la Información y Telecomunicaciones del Gobierno Regional de Loreto, o quien haga sus veces en las Unidades Ejecutoras, debe verificar los controles de continuidad de seguridad de la información que se han implementados regulares para asegurar que sean válidos y efectivos.

c) La Oficina Regional de Tecnologías de la Información y Telecomunicaciones del Gobierno Regional de Loreto, o quien haga sus veces en las Unidades Ejecutoras, debe asegurar la existencia de recursos redundantes para el tratamiento de la información a fin de cumplir con los requisitos de disponibilidad.

d) La Oficina Regional de Tecnologías de la Información y Telecomunicaciones del Gobierno Regional de Loreto, o quien haga sus veces en las Unidades Ejecutoras, debe realizar las pruebas de la funcionalidad de los procesos, procedimientos y controles de continuidad de la seguridad de la información para garantizar que se encuentran conforme a los objetivos de continuidad de la seguridad de la información, estas pruebas deben quedar documentadas.

5.17 Política de Cumplimiento

5.17.1 Objetivo

a) Prevenir incumplimientos de las obligaciones legales, estatutarias, reglamentarias o contractuales relativas a la seguridad de la información o de los requisitos de seguridad.

b) Garantizar que la seguridad de la información se implementa y opera de acuerdo con la política y procedimientos de la Entidad.

5.17.2 Política

a) Todos los órganos y unidades orgánicas del Gobierno Regional de Loreto y sus Unidades Ejecutoras deben cumplir con todos los requisitos legislativos, regulaciones y requerimientos contractuales relativas a seguridad de la información, asimismo, deben ser identificadas y documentadas.

b) Todos los órganos y unidades orgánicas del Gobierno Regional de Loreto y sus Unidades Ejecutoras deben asegurar el cumplimiento a los derechos de propiedad intelectual, para lo cual todo el software que utiliza en la Entidad debe contar con la respectiva licencia de uso.

e) Los servidores del Gobierno Regional de Loreto y sus Unidades Ejecutoras no deben destruir o eliminar registros o información importante, sin la aprobación respectiva de los propietarios de información.

c) El Gobierno Regional de Loreto y sus Unidades Ejecutoras a través del Órgano o Unidad Orgánica responsable de acuerdo a su competencia, debe de garantizar la protección y la privacidad de los datos personales conforme a la legislación aplicable.

d) El Gobierno Regional de Loreto y sus Unidades Ejecutoras a través del Órgano o Unidad Orgánica responsable de acuerdo a su competencia, debe establecer los términos, condiciones y finalidades para datos personales en cumplimiento con la Ley existente y su Reglamento.

e) La Oficina Regional de Tecnologías de la Información y Telecomunicaciones del Gobierno Regional de Loreto, o la que haga sus veces en las Unidades Ejecutoras, debe asegurar que la seguridad de la información este implementada y operada, a través de revisiones independientes de la seguridad de la información mediante auditorías para asegurar que se mantenga de forma eficaz, eficiente y efectiva.

5. Anexo: Definiciones

Para los fines del presente Lineamiento, se establecen las siguientes definiciones

- **Activo de Información:** Información que tiene valor para la Entidad, pudiendo además ser aquel recurso (humano, tecnológico, etc.) que efectúa el tratamiento directo o indirecto de la información que soporta uno o más procesos de la Entidad.
- **Antecedentes Laborales:** Información que permite identificar los antecedentes (Policiales, Penales, Judiciales) del servidor.
- **Clasificación de Información:** Conjunto de actividades que permiten identificar y clasificar los activos de información en términos de la sensibilidad e importancia para el GOBIERNO REGIONAL DE LORETO y sus Unidades Ejecutoras.
- **Confidencialidad:** Característica/propiedad por la cual la información no está disponible o revelada a individuos, entidades, o procesos no autorizados.
- **Comité de Gobierno Digital:** Grupo de funcionarios encargados de la Gestión del Gobierno Digital en la Entidad, conformados mediante Resolución N" 100-2020-GRL-GR
- **Disponibilidad:** Característica/propiedad por la cual la información permanece accesible y disponible para su uso cuando lo requiera una entidad autorizada.
- **Dispositivos Móviles:** Aparatos electrónicos como computadoras portátiles, tablet, celulares o smartphone que permiten el tratamiento de la

información durante su desplazamiento y uso en ambientes no controlados por la Entidad.

- **Evento:** Un suceso o serie de sucesos que pueden ser interno o externo al GOBIERNO REGIONAL DE LORETO o sus Unidades Ejecutoras, originados por una misma causa, que ocurren durante el mismo periodo de tiempo.
- **Incidente de Seguridad de la Información:** Evento no deseado que tiene una probabilidad significativa de comprometer las operaciones de la Entidad y que genera amenazas a la seguridad de la información.
- **Información:** Cualquier forma de registro electrónico, óptico, magnético o en otros medios similares, susceptible de ser procesada, distribuida y almacenada.
- **Integridad:** Característica/propiedad por la cual la información conserva su exactitud y se encuentra completa.
- **Medios Removibles:** Son aquellos dispositivos que se insertan en los conectores externos de los equipos informáticos para almacenar información, tales como memoria USB, disco duro externo o tarjetas de memoria.
- **Oficial de Seguridad de la Información:** Servidor responsable de la Seguridad de la Información, designado mediante Resolución Ejecutiva Regional N° 136-2020-GRL-GR
- **Propietario de Activo de Información:** Una persona, cargo, proceso o grupo de trabajo designado por la organización, quien tiene la responsabilidad de definir los controles y/o lineamientos para el cuidado de los activos de información, bajo su responsabilidad. Es el responsable de la información y de los procesos que la manipulan, sean estos manuales, mecánicos o electrónicos.
- **Riesgo:** Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Combinación de la probabilidad de un evento y sus consecuencias.
- **Seguridad de la Información:** Son todas las actividades orientadas a preservar la integridad, confidencialidad y disponibilidad de la información y los activos asociados a su tratamiento, independientemente de la forma en que éste se presente.
- **Sistema de Información:** Conjunto independiente de recursos de información organizados para la recopilación, procesamiento, mantenimiento, transmisión y difusión de la información según determinados procedimientos, tanto automatizado como manuales.

- **Sistema de Gestión de la Seguridad de la Información (SGSI):** La parte de un sistema global de gestión que, basado en el análisis de riesgos, establece, implementa, opera, monitoriza, revisa, mantiene y mejora la Seguridad de la Información. (El Sistema de Gestión incluye una estructura de organización, políticas, planificación de actividades, responsabilidades, procedimientos, procesos y recursos).

GOBIERNO REGIONAL DE LORETO

Comité de Gestión de Seguridad de la Información

DIRECTIVA GENERAL N° 001-2021-GRL-GGR-ORTIT

"SEGURIDAD DE LA INFORMACIÓN DEL GOBIERNO REGIONAL DE LORETO"

(Resolución Gerencial Regional N°344-2021-GRL-GGR)

Oficina Regional de Tecnologías de la Información y Telecomunicación

BELÉN, JUNIO DEL 2021

I. OBJETO

Establecer el marco general de la Seguridad de la Información en el Gobierno Regional de Loreto y sus áreas descentralizadas, mediante medidas tecnológicas físicas y legales necesarias para proteger la información institucional contra el acceso no autorizado, divulgación, aprovechamiento, intromisión de sistemas o mala uso que se puede producir en forma intencional o accidental.

II. FINALIDAD

Proteger los activos de la información en el Gobierno Regional de Loreto, mitigando las amenazas y el riesgo de exposición de información sensible, asegurando la confidencialidad, integridad, disponibilidad y confiabilidad de la información fortaleciendo la cultura de seguridad en la entidad.

III. BASE LEGAL

III.1. Constitución Política del Perú y su modificatoria.
III.2. Ley Nº 27867, Ley Orgánica de los Gobiernos Regionales.
III.3. Ley 27783, Ley de Bases de la Descentralización y normas modificatorias.
III.4. Ley 27444, Ley del Procedimiento Administrativo General.
III.5. Ley 27815, Ley del Código de Ética de la Función Pública.
III.6. Ley 27658, Ley Marco de Modernización de la Gestión del Estado.
III.7. Ley N° 29733, Ley de Protección de Datos Personales.
I.1. Ley N°30096, Ley de Delitos Informáticos y sus Modificatorias.
I.2. Ley N° 27309, Ley que incorpora los delitos informáticos al Código Penal.
III.8. Ley N°28612, Ley que Norma el Uso, Adquisición, y Adecuación del Software en la Administración Pública.
III.9. Ley N°31170, Ley de Implementación de Mesa de Parte Digitales y Notificaciones Electrónicas.
III.10. Ley N°30225, Ley de Contrataciones del Estado.
III.11. Decreto Supremo N°344-2018-EF, Reglamento de la Ley N°30225.
III.12. Decreto Legislativo N°1412-2018-PCM, Ley del Gobierno Digital.
III.13. Decreto Supremo Nº 029-2021-2021-PCM, Reglamento de la Ley N°1412 del Gobierno Digital.
III.14. Decreto de Supremo Nº 051-2018-PCM, Portal de Software Público Peruano y establece disposiciones adicionales sobre el Software Público Peruano, (fecha: 14/05/2018).

III.15. Decreto Supremo N° 083-2011-PCM, que crea la Plataforma de interoperabilidad del Estado - PIDE.

III.16. 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.

III.17. Decreto Supremo Nº 053-2006-PCM, Reglamento del Registro Nacional de Derecho de Autor y Derechos Conexos, contemplado en el Decreto Legislativo N° 822, Ley sobre el Derecho de Autor.

III.18. Resolución N°0791-2015/CDA-INDECOPI, Lineamientos complementarios de la Comisión de Derecho de Autor sobre el Uso Legal de los Programas de Ordenador (Software).

III.19. Decreto Supremo N° 043-2003-PCM, que aprueba el Texto Único Ordenado de la Ley N° 27806, Ley de Transparencia y Acceso a la Información Pública.

III.20. Decreto Supremo N° 024-2006-PCM, que aprueba el Reglamento de la Ley N° 28612.

III.21. Decreto Supremo N° 050-2018-PCM, que aprueba la Definición de Seguridad Digital en el Ámbito Nacional.

III.22. Decreto de Urgencia N°006-2020, Decreto de Urgencia que crea el Sistema Nacional de Transformación Digital.

III.23. Decreto de Urgencia N°007-2020, Decreto de Urgencia que aprueba el Marco de Confianza Digital y dispone medidas para su fortalecimiento.

III.24. Resolución Ministerial N° 004-2016-PCM, que aprueba el Uso obligatorio de la Norma Técnica Peruana "NTP ISO/IEC 27001:2014 Tecnología de la Información, Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 2da. Edición", en todas las entidades integrantes del Sistema Nacional de Informática.

III.25. Norma Técnica N°001-2018-PCM-SGP, Condiciones Mínimas y plazos para la Implementación y Uso Progresivos del Sistema Único de Trámites – SUT.

III.26. Resolución Ministerial N° 041-2017-PCM, que aprueba el uso obligatorio de la Norma Técnica Peruana "NTP-ISO/IEC 12207:2016-Ingeniería Software y Sistemas. Procesos del ciclo de vida del software. 3era. Edición", en todas las entidades integrantes del Sistema Nacional de Informática.

III.27. 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.

III.28. Resolución Ejecutiva Regional N°163-2017-GRL-GR, Directiva General N°011-2017-GRL- OEDII, que contiene las "Normas para la Formulación, Tramite, aprobación y Actualización de Directivas"

III.29. Resolución Ejecutiva Regional N°100-2021-GRL-GR, de fecha 27/04/2020; Constitución del Comité de Gobierno Digital, Funciones y Designación del Líder Digital – GOREL.

III.30. Resolución Ejecutiva Regional N°141-2021-GRL-GR, de fecha 03/05/2021; Designación del Funcionario Responsable del Software del GOREL

III.31. Resolución Ejecutiva Regional N°151-2021-GRL-GR, de fecha 03/05/2021; Conformación del Comité de Gestión de la Seguridad de la Información y Designación del Oficial de Seguridad de la Información del GOREL.

III.32. Resolución Ejecutiva Regional N°168-2021-GRL-GR, de fecha 31/05/2021; conformación del Equipo de Respuestas ante Seguridad Digital del GOREL.

III.33. Reglamento Interno de Trabajo / RIT - GOREL.

IV. ALCANCE

Las disposiciones contenidas en la presente Directiva General son de aplicación y cumplimiento obligatorio en todo el Gobierno Regional de Loreto, para:

IV.1. El Personal que interactúan de una manera habitual u ocasional con los activos de información, independientemente de su vínculo laboral o contractual.

IV.2. Las Personas naturales o jurídicas que brindan servicios a la entidad y que tengan acceso a la información o sus activos informáticos.

V. NORMAS GENERALES

V.1. **Principios de seguridad Informática en el Gobierno Regional de Loreto:**
El Gobierno Regional de Loreto se rige por los siguientes principios y servicios de Seguridad informática

- **Eficacia:**
  Garantizar que toda la información utilizada es necesaria y útil para el desarrollo de las actividades del Gobierno Regional de Loreto.

- **Eficiencia:**
  Asegurar que el procesamiento de la información se realice mediante una óptima utilización de los recursos humanos y materiales.

- **Confiabilidad:**
  Garantizar que los sistemas informáticos brinden información correcta para ser utilizada en la operación de cada uno de los procesos.

- **Integridad:**
  Asegurar que la información y sus métodos de procesamiento son completos que permitan la marcha de las actividades en cada uno de los sistemas informáticos.

- **Exactitud:**
  Asegurar que toda la información se encuentre libre de errores y/o irregularidades de cualquier tipo.

- **Disponibilidad:**
  Garantizar que la información y la capacidad de su procesamiento manual y automático sean resguardados y recuperadas eventualmente cuando sea necesario, de manera tal que no se interrumpa significativamente la marcha de las actividades de la institución.

- **Legalidad:**
  Asegurar que toda la información y los medios físicos que la contienen, procesen y transporten cumplan con las regulaciones legales vigente en cada ámbito.

- **Confidencialidad:**
  Garantizar que toda la información esté protegida del uso no autorizado, revelaciones accidentales, espionaje informático, violación de la privacidad y otras acciones similares de acceso de terceros no permitidos.

- **Autorización:**
  Garantizar que todos los accesos a datos cumplan con niveles de autorización correspondientes para su utilización y divulgación.

- **Protección Física:**
  Garantizar que todos los medios de procesamiento y/o conservación de información cuentan con medidas de protección física que eviten el acceso y/o utilización indebida por personal no autorizado.

- **Propiedad:**

Asegurar que todos los derechos de propiedad sobre la información utilizada por todo el personal en el desarrollo de sus tareas, estén adecuadamente establecidos a favor de la institución.

V.2. **Uso obligatorio en todas las entidades integrantes del Sistema Nacional de Informática de la Norma Técnica Peruana "NTP-ISO/IEC 27001:2014 "Tecnología de la Información"** Resolución Ministerial Nº 004-2016-PCM, mediante la cual se establece que las entidades de la Administración Pública deben establecer, mantener y documentar un Sistema de Gestión de la Seguridad de la Información (SGSI).

V.3. **La Seguridad de la Información**. El Marco de Seguridad Digital del Estado Peruano se articula y sustenta en las normas, procesos, roles, responsabilidades y mecanismos regulados e implementados a nivel nacional en materia de Seguridad de la Información.

V.4. **El Sistema de Gestión de Seguridad de la Información (SGSI)** comprende el conjunto de políticas, lineamientos, procedimientos, recursos y actividades asociadas, que gestiona una entidad con el propósito de proteger sus activos de información, de manera independiente del soporte en que estos se encuentren. Asimismo, contempla la gestión de riesgos e incidentes de Seguridad de la Información y seguridad digital, la implementación efectiva de medidas de ciberseguridad, y acciones de colaboración y cooperación.

VI. MECÁNICA OPERATIVA

A. Sobre los Recursos Informáticos

VI.1. De la solicitud de los recursos informáticos.

VI.1.1. Toda necesidad de equipos informáticos debe ser dirigida como requerimiento de compra a la Oficina Regional de Tecnologías de la Información y Comunicación, quien elabora las especificaciones técnicas, y lo remite al área usuaria para la firma del Jefe de la Unidad.

VI.1.2. El área usuaria remite el requerimiento a la Oficina Regional de Administración para realizar la adquisición mediante la Oficina Ejecutiva de Logística. Una vez finalizado el proceso de adquisición, los equipos informáticos serán puestos en almacén para luego emitir el informe técnico y la conformidad por parte de la Oficina Regional de Tecnologías de la Información y Comunicación.

VI.2. De la asignación de los recursos informáticos.

VI.2.1. De la asignación de hardware y otros medios físicos

a. La asignación de recursos informáticos sólo puede ser solicitada por el Gerente, Sub Gerente, Jefe o nomenclatura similar, mediante documento dirigido al Jefe de la Oficina Regional de Tecnologías de la Información y Comunicación, precisando los servicios informáticos que requiere que sean implementados en la respectiva computadora (nivel de acceso a sistemas o aplicaciones e instalación de software no estándar).

b. El Gerente, Sub Gerente, Jefe o nomenclatura similar puede solicitar al Jefe de la Oficina Regional de Tecnologías de la Información y Comunicación que se le asigne algún recurso informático adicional para la prestación de servicios, entre ellos de locación de servicios, siempre que se encuentre vinculado a las funciones de la unidad o sub unidad orgánica.

c. Al personal que se le asigne el recurso informático es responsable por el buen funcionamiento y por la integridad de sus componentes.

d. Todo traslado y/o reasignación de equipos informáticos será informado a la Oficina Regional de Tecnologías de la Información y Comunicación y a la Sub Unidad de logística, y contar con la supervisión de estas Sub Unidades para la desconexión y traslado de los equipos informáticos.

e. Ante cualquier proceso interno de asignación y/o rotación de equipos de cómputo, la Oficina Regional de Tecnologías de la Información y Comunicación elabora una lista de chequeo para su operatividad, lista dentro de la cual se encuentra debidamente registrado la instalación y/o validación de las herramientas administrativas y antivirus.

VI.2.2. De la asignación de software.

a. El usuario tendrá acceso autorizado únicamente a aquellos datos y recursos que necesite para el desarrollo de sus funciones, conforme a lo solicitado por la unidad orgánica a la cual pertenece.

b. El equipo de cómputo que es entregado al usuario, contiene un software instalado de acuerdo al perfil solicitado por su unidad orgánica. Cualquier necesidad adicional de software, es solicitada mediante documento escrito o correo electrónico a la Oficina Regional de Tecnologías de la Información y Comunicación.

c. El equipo de cómputo que se entrega al usuario está completamente operativo y contiene el software base necesaria para desarrollar sus funciones, según lo solicitado por la unidad orgánica respectiva y lo permitido por la Oficina Regional de Tecnologías de la Información y Comunicación. Cualquier necesidad de software y/o utilitario adicional debe ser solicitada a la Oficina Regional de Tecnologías de la Información y Comunicación, vía documento escrito o correo electrónico.

VI.3. De la recepción de los recursos Informáticos.

*VI.3.1. **Del uso y conservación de hardware y otros medios físicos.***

a. La instalación de los equipos informáticos está a cargo del personal de la Oficina Regional de Tecnologías de la Información y Comunicación. Se ceñirán estrictamente a los requerimientos de los equipos, cuidando las especificaciones del cableado y de los circuitos de protección necesarios. En ningún caso se permitirán instalaciones improvisadas o sobrecargadas.

b. Las computadoras personales (laptops) se entregan completamente operativas, incluyendo únicamente el software y hardware permitido por la Oficina Regional de Tecnologías de la Información y Comunicación.

c. Del uso de memorias externas

Discos Externos: El uso de discos duros externos es autorizado por la Oficina Regional de Tecnologías de la Información y Comunicación, previa solicitud mediante correo electrónico de la unidad orgánica correspondiente.

Memoria Removible (USB): Los puertos de conexión para memorias removibles se encuentran desactivados de forma

permanente. Solo se activan a solicitud de los Gerente, Sub Gerente, Jefe o nomenclatura similar, especificando que tipo de información será almacenada y cuál será su finalidad.

VI.3.2. De las prohibiciones en el uso del hardware y otros medios físicos.

Todo el personal usuario de dichos recursos informáticos debe saber que no tiene el derecho de confidencialidad en su uso.

Queda prohibido:

a. El uso de estos recursos informáticos para actividades no relacionados con el propósito de la institución, o bien con la extralimitación en su uso.

b. Dejar encendido la computadora personal que se le ha asignado al finalizar la jornada de trabajo o al retirarse del centro de trabajo, salvo excepciones previamente coordinadas con la Oficina Regional de Tecnologías de la Información y Comunicación.

c. Utilizar el acceso autorizado de otro usuario, aunque dispongan de la autorización del propietario.

d. Contener archivos en el escritorio de la Computadora y/o computadora portátil, solamente debe contener aplicaciones o herramientas del sistema.

e. Almacenar datos de carácter personal en las unidades locales de disco de computadores de trabajo.

f. Conectar cualquier artefacto eléctrico ajeno a los equipos de cómputo en el estabilizador de voltaje, el cual ha sido instalado exclusivamente para protegerlos.

g. Conectar impresoras en el mismo estabilizador de voltaje de una computadora de escritorio porque podría en algunos casos, rebasar la capacidad eléctrica del estabilizador y causar daños a los equipos informáticos.

h. Abrir los dispositivos o equipos informáticos. Queda exceptuado de esta prohibición el personal encargado de brindar soporte técnico.

i. Pegar calcomanías o cualquier tipo de adornos en la computadora personal; salvo etiquetas de inventario o de identificación para efectos del control patrimonial.

j. Fumar, ingerir alimentos o bebidas, cuando se encuentren frente al teclado o cerca a orificios o rejillas de ventilación de los equipos. Cualquier desperfecto por las causas señaladas, dará lugar a que el usuario asuma el costo de reparación correspondiente, sin perjuicio de la respectiva sanción administrativa, conforme a la normatividad vigente.

k. Permitir que un tercero utilice la computadora que se le ha asignado, para fines ajenos al servicio.

VI.3.3. De las prohibiciones en el uso del software.

a. Está prohibido las actividades, equipos o aplicaciones que no estén directamente especificados como parte del Software o de los estándares de los recursos informáticos propios del Gobierno Regional De Loreto.

b. Que el usuario instale de manera arbitraria software en su equipo de cómputo, siendo responsable de las consecuencias que ello produjera.

VI.4. De la seguridad de la computadora.

VI.4.1. La Oficina Regional de Tecnologías de la Información y Comunicación es la encargada de suministrar medidas de seguridad adecuadas contra la intrusión o daños a la información almacenada en los sistemas, así como la instalación de cualquier herramienta, dispositivo o software que refuerce la seguridad en la computadora.

VI.4.2. En caso se requiera acceder a la computadora del usuario ausente, el Gerente, Sub Gerente, Jefe o nomenclatura similar interesada debe solicitarlo por escrito o vía correo electrónico a la Oficina Regional de Tecnologías de la Información y Comunicación. De ser necesario, esta última eliminará las claves de acceso a red, asignando nuevas claves, las que serán de conocimiento exclusivo del Gerente, Sub Gerente, Jefe o nomenclatura similar o del responsable que este designe. Quien posea las claves asumirá en

forma personal la responsabilidad por la confidencialidad de las mismas, así como de las consecuencias derivadas de su uso.

VI.4.3. La Oficina Regional de Tecnologías de la Información y Comunicación es la única autorizada para monitorear constantemente el tráfico de paquetes sobre la red, con el fin de detectar y solucionar anomalías, registrar usos indebidos o cualquier falla que provoque problemas en los servicios de la red.

VI.4.4. La Oficina Regional de Tecnologías de la Información y Comunicación debe mantener informados de sucesos de intrusos o daños a las computadoras y/o información a los/las usuarios/as y poner a disposición de los/las mismos/as el software que refuerce la seguridad de los sistemas de cómputo.

VI.4.5. **Del antivirus.**

VI.4.5.1. **Antivirus de red.**

- Todos los equipos de cómputo deben tener instalado un software antivirus.
- Periódicamente se hará el rastreo en los equipos de cómputo, así como, la actualización de las firmas de antivirus, proporcionadas por el fabricante del software antivirus, en los equipos conectados a la Red.
- La desinstalación del antivirus se encuentra restringida a la validación de clave de desinstalación, la cual se encuentra a disposición únicamente del equipo de soporte técnico.
- Es responsabilidad de los usuarios informar oportunamente a la Oficina Regional de Tecnologías de la Información y Comunicación, acerca de una sospecha de infección por virus informático.

VI.4.5.2. **Uso del antivirus**

- El usuario no debe desinstalar la solución de su computadora pues ocasiona un riesgo de seguridad ante el peligro de virus.

- Si el usuario hace uso de medios de almacenamiento personales, estos son rastreados por el software antivirus en la computadora del usuario o por el equipo portátil designado para tal efecto.

- El usuario debe comunicarse con el personal de soporte técnico en caso de problemas de virus, para buscar la solución.

- El usuario es notificado por personal de soporte técnico cuando sea desconectado de la red con el fin de evitar la propagación del virus a otros usuarios, así como cuando sus archivos resulten con daños irreparables por causa de virus o cuando viole las políticas de antivirus.

VI.4.6. La Oficina Regional de Tecnologías de la Información y Comunicación posee una clave de administrador para poder acceder y/o cambiar cualquier contraseña, ante necesidad justificada o ausencia del responsable del equipo, previa solicitud y autorización del Gerente, Sub Gerente, Jefe o nomenclatura similar, en concordancia con el numeral 6.6.5 de la presente Directiva.

VI.4.7. De la Política de Seguridad Lógica de los Recursos Informáticos.

Son orientadas a proteger la información almacenada en los equipos informáticos del Gobierno Regional De Loreto.

- **Longitud de Contraseña:**
  La longitud de las contraseñas tiene un mínimo de ocho (8) caracteres y una longitud máxima de doscientos cincuenta y cinco (255) caracteres.

- **Contraseñas difíciles de descifrar:**
  Establecer o crear contraseñas difíciles de descifrar. En general no se deben de utilizar palabras de un diccionario, derivados del usuario, series de caracteres comunes como 12345678. Asimismo, no deben emplear detalles personales a menos que se estén acompañadas por caracteres adicionales que no tengan ninguna relación.

- **Contraseñas con caracteres alfabéticos y no alfabéticos:**

Las contraseñas deben tener al menos un carácter alfabético y uno no alfabético. Se consideran caracteres no alfabéticos los números y los signos de puntación, de igual manera se pueden utilizar caracteres no impresos.

- **Contraseñas con letras mayúsculas y minúsculas:**
  Todas las contraseñas escogidas por el usuario del Gobierno Regional De Loreto deben tener por lo menos un carácter alfabético en minúscula y otro en mayúscula. Esto ayudará para que las contraseñas sean más difíciles de descifrar por personas no autorizadas.

- **Contraseñas generadas por el sistema:**
  Las contraseñas generadas por el sistema son generadas teniendo como base el tiempo del reloj u alguna otra parte del sistema de procedencia impredecible que cambie frecuentemente.

- **Protección de los algoritmos que se utilizan en la generación de las contraseñas:**
  Todo programa y archivo que contenga fórmula, algoritmo u otras especificaciones que se utilicen para la generación de las contraseñas por medio del sistema de computación debe estar controlado con las más altas medidas de seguridad que éste proporcione.

- **Cambio periódico obligatorio de la contraseña:**
  El sistema operativo debe obligar automáticamente a que todos los usuarios cambien sus contraseñas al menos una vez cada noventa (90) días.

- **Cambio obligatorio de la contraseña al acceder por primera vez al sistema:**
  Las contraseñas inicialmente emitidas por un administrador de sistema deben ser validas solamente para la primera conexión del usuario, momento en el cual el usuario debe cambiar la contraseña antes de realizar cualquier otro trabajo.

- **Límite de intentos consecutivos infructuosos para ingresar la contraseña:**
  Después de cinco (5) intentos consecutivos e infructuosos de ingreso de la contraseña, el sistema debe al usuario:

a. Incapacitarlo temporalmente por no menos de tres minutos.

b. Suspender el acceso del usuario hasta que el administrador del sistema lo ponga a funcionar nuevamente

- **Proceso de identificación personal ante el sistema:** En el momento en que el usuario va a ingresar a la red y/o al sistema del computador, se debe solicitar una combinación de la identificación de usuario y de una contraseña.

VI.4.8. Los usuarios deben adoptar las medidas necesarias para evitar que alguna otra persona pueda ver su clave al momento de digitarla, incluyendo el personal de la Oficina Regional de Tecnologías de la Información y Comunicación. Si ello ocurriese, es recomendable cambiar la clave.

VI.4.9. Si un usuario tiene sospechas de que su acceso autorizado (identificador de usuario y contraseña) está siendo utilizado por otra persona, debe proceder al cambio de su contraseña e informar a su jefe inmediato y éste reportar a el Jefe de la Oficina Regional de Tecnologías de la Información y Comunicación.

VI.4.10. Utilizar el menor número de archivos que contenga datos de carácter personal y mantener los mismos en un lugar seguro y fuera del alcance de terceros.

VI.4.11. Los usuarios sólo pueden crear carpetas que contengan datos de carácter personal para un uso temporal y siempre que sea necesario para el desempeño de su trabajo. Estos ficheros temporales nunca serán ubicados en la Unidad C:\ del disco local del equipo de trabajo y deben ser eliminados cuando hayan dejado de ser útiles para la finalidad que se crearon.

VI.4.12. Los usuarios tienen cuidado con los dispositivos de almacenamiento, especialmente aquellos que hayan utilizado para guardar copias de sus archivos digitales y que forman parte de su acervo documentario.

VI.5. De las computadoras denominados servidores.

VI.5.1. **De la configuración e instalación.**

a. La Oficina Regional de Tecnologías de la Información y Comunicación tiene la responsabilidad de verificar la instalación, configuración e implementación de seguridad, en los servidores conectados a la Red.

b. Durante la configuración de los servidores, la Oficina Regional de Tecnologías de la Información y Comunicación debe regular el uso de los recursos del sistema y de la red, principalmente la restricción de directorios, permisos y programas a ser ejecutados por los usuarios.

c. Los servidores que proporcionen servicios a través de la red e internet deberán:

- Funcionar las veinticuatro (24) horas del día los trescientos sesenta y cinco (365) días del año.
- Recibir mantenimiento preventivo semestral que incluya depuración de archivos logs.

d. La información de los servidores deberá ser respaldada de acuerdo con los siguientes criterios, como mínimo:

- Diariamente, información crítica.
- Semanalmente, los documentos web.
- Mensualmente, configuración del servidor y logs.

VI.6. De la supervisión y control de los recursos informáticos.

VI.6.1. La Oficina Regional de Tecnologías de la Información y Comunicación debe llevar un control total y sistematizado de los recursos de cómputo y licenciamiento.

VI.6.2. La Oficina Regional de Tecnologías de la Información y Comunicación organizará al personal responsable del mantenimiento preventivo y correctivo de los equipos de cómputo.

VI.6.3. **De los técnicos en soporte.**

Los Técnicos en soporte tendrán las siguientes atribuciones y/o responsabilidades:

a. Ingresar de forma presencial y remota a computadoras única y exclusivamente para la solución de problemas y bajo solicitud explícita del usuario.

b. Utilizar los analizadores previa autorización del usuario y bajo la supervisión de éste, informando de los propósitos y los resultados obtenidos.

c. Realizar respaldos periódicos de la información de los recursos de cómputo que tenga a su cargo, siempre y cuando se cuente con dispositivos de respaldo.

d. Registrar cada máquina en el inventario de control de equipos de cómputo y red del Gobierno Regional De Loreto.

e. Realizar la instalación o adaptación de los sistemas de cómputo de acuerdo con los requerimientos en materia de seguridad.

f. Implementar un Software Antivirus en las computadoras del Gobierno Regional De Loreto.

g. Solucionar contingencias presentadas ante el seguimiento de virus que la solución no haya detectado automáticamente.

h. Configurar el analizador de red para la detección de virus.

i. Son los únicos autorizados de asistir de forma presencial y remota a los usuarios de los servicios del Gobierno Regional De Loreto previa solicitud a la Oficina Regional de Tecnologías de la Información y Comunicación.

j. En el caso de los servicios del Gobierno Regional De Loreto en zonas distantes, se contactará vía remota para el diagnóstico y de no ser posible esta conexión se tomará contacto con técnicos/as de la zona para el diagnóstico correspondiente.

VI.6.4. El resguardo de los equipos de cómputo queda bajo responsabilidad de la Oficina Regional de Tecnologías de la Información y Comunicación contando con un control de los

equipos que permita conocer siempre la ubicación física de los mismos.

VI.6.5. **Usuario ausente**

a. La Sub Unidad de Recursos Humanos comunica a la Oficina Regional de Tecnologías de la Información y Comunicación, con la debida anticipación el cese o cualquier otra circunstancia que determina la ausencia de un usuario, a fin de que se desactive el respectivo acceso a red y demás servicios informáticos. Dicha comunicación será puesta en conocimiento del Gerente, Sub Gerente, Jefe o nomenclatura similar.

b. En caso que el usuario ausente retorne al centro de labores por necesidad de servicio, o luego de una licencia, vacaciones, comisión u otros casos, y requiera el uso de su computadora como el correo electrónico institucional u otros servicios informáticos, bastará la comunicación escrita o por correo electrónico institucional del Gerente, Sub Gerente, Jefe o nomenclatura similar o a la Oficina Regional de Tecnologías de la Información y Comunicación, retomando el usuario su responsabilidad respecto de la información almacenada y procesada en ella, por lo que deberá modificar la clave de acceso de red y demás servicios informativos, de ser el caso.

VI.6.6. **Usuario Tercero**.

Está prohibido permitir a personas ajenas al Gobierno Regional De Loreto el acceso a la información contenida en las computadoras, salvo lo dispuesto en el ítem (b) del numeral 6.2.1 de la presente Directiva.

VI.7. De la renovación de recursos informáticos.

VI.7.1. Los Equipos de cómputo tienen una vida útil de cuatro (4) años. Antes del término de la vida útil de los equipos de cómputo, la Oficina Regional de Tecnologías de la Información y Comunicación realizará las acciones necesarias que aseguren la renovación de estos.

VI.7.2. Cuando las unidades orgánicas requieran renovar un equipo de cómputo para el desempeño de sus actividades, éstas deberán

solicitar a la Oficina Regional de Tecnologías de la Información y Comunicación a fin de que se seleccione el equipo adecuado. Sin el visto bueno de la Oficina Regional de Tecnologías de la Información y Comunicación no podrá iniciarse ningún proceso de compra.

B. De los servicios informáticos.

VI.8. De la solicitud a los servicios de tecnología de la información

VI.8.1. Las unidades orgánicas definirán los servicios de internet a ofrecer a su personal y se coordinará con la Oficina Regional de Tecnologías de la Información y Comunicación para su otorgamiento y configuración.

VI.8.2. En caso de que el usuario necesite un software y/o utilitario adicional, el Gerente, Sub Gerente, Jefe o nomenclatura similar formaliza el pedido mediante documento escrito o por correo electrónico ante el Director de la Oficina Regional de Tecnologías de la Información y Comunicación.

VI.9. De la asignación a los servicios de tecnologías de información.

VI.9.1. Las cuentas de ingreso a los sistemas y los recursos de cómputo son propiedad del Gobierno Regional De Loreto y se usarán exclusivamente para actividades relacionadas con la labor asignada.

VI.9.2. Todas las cuentas de acceso a los sistemas y recursos informáticos son personales e intransferibles, sólo deberá ser utilizada por el usuario del equipo, quien será el único responsable de su confidencialidad. Se permite su uso única y exclusivamente mientras mantengan una relación contractual con el Gobierno Regional De Loreto.

VI.9.3. Cuenta de acceso al dominio del Programa, La Oficina Regional de Tecnologías de la Información y Comunicación proporciona el acceso a la red de dominio únicamente al personal que indique el Gerente, Sub Gerente, Jefe o nomenclatura similar correspondiente, asignándoles un "nombre de usuario/a" el mismo que se forma con la primera letra de su nombre seguida de su apellido paterno. El procedimiento inicia con la solicitud de creación de perfil del Gerente, Sub Gerente, Jefe o nomenclatura similar a la Oficina Regional de Tecnologías de la Información y

Comunicación, quien recibe y valida los datos, generando una cuenta de dominio mediante un nombre de cuenta y contraseña, el cual se remite mediante correo electrónico a el Gerente, Sub Gerente, Jefe o nomenclatura similar, para finalmente recibir el apoyo técnico para el acceso a la plataforma.

VI.9.4. Cuenta de acceso al correo electrónico institucional.

a. La Oficina Regional de Tecnologías de la Información y Comunicación se encargará de asignar las cuentas a los usuarios para el uso de correo electrónico institucional.

b. Para efecto de asignarle una cuenta de correo electrónico al usuario, el Gerente, Sub Gerente, Jefe o nomenclatura similar solicitante, comunicara formalmente a la Oficina Regional de Tecnologías de la Información y Comunicación mediante documento escrito o correo electrónico.

c. La Oficina Regional de Tecnologías de la Información y Comunicación, atiende la solicitud recibida, verifica, valida y registra los datos del servidor o funcionario para la creación de la cuenta de usuario de correo electrónico.

d. El nombre de la cuenta de correo electrónico institucional para cada usuario estará formado por la letra inicial del nombre seguido inmediatamente del apellido paterno, ligado con el símbolo @ al nombre de dominio "regionloreto.gob.pe". Para casos de similitudes de cuentas, la Oficina Regional de Tecnologías de la Información y Comunicación coordinará con las personas involucradas el nombre de la cuenta, tratando de seguir la regla antes mencionada. Las excepciones a lo dispuesto en el presente literal las autoriza la Unidad de Administración.

e. La Oficina Regional de Tecnologías de la Información y Comunicación crea una contraseña genérica para los usuarios nuevos, por lo que la cuenta es activada en el momento en que el usuario ingrese por primera vez a su correo electrónico siendo obligatorio que el usuario defina su nueva contraseña, asumiendo la responsabilidad de la confidencialidad de las mismas.

f. Los usuarios a quienes se ha asignado una cuenta de correo electrónico son responsables de todas las actividades que se realizan con dichas cuentas.

g. Los usuarios deben mantener activo permanentemente el correo electrónico y conectarse como mínimo, una vez al día, para ver los mensajes, comunicados o cualquier tipo de notificación institucional.

h. El correo electrónico sólo debe ser utilizado como una herramienta de comunicación e intercambio de información oficial. Los usuarios deben evitar que los archivos adjuntos superen los 6 Mb, por motivos de mantener un adecuado desempeño de la red.

i. La capacidad de almacenamiento para cada casilla de correo electrónico está definida en 300 Mb para evitar la saturación. el usuario tiene la responsabilidad de bajar a carpetas locales los mensajes de correos (revisados en la bandeja de entrada, enviado y en la papelera), mediante el uso Zimbra Cliente Desktop (correo electrónico multiplataforma), previamente configurado por la Oficina Regional de Tecnologías de la Información y Comunicación.

j. Todos los mensajes de correo electrónico serán registrados y almacenados en el servidor de correo electrónico, para una mejor distribución de los mismos, el usuario clasifica en forma permanente sus correos recibidos (bandeja de entrada y enviados) en carpetas locales.

k. Los usuarios deben evitar responder correos electrónicos, adjuntando en el contenido los mensajes previos, puesto que este contenido puede poseer información reservada y privada salvo que el envío y el asunto en mención así lo amerite.

l. El uso del correo electrónico es sólo para fines laborales, está totalmente prohibido su utilización para envío de cadenas de correo, spams, archivos de entretenimiento, mp3, videos mpg, imágenes jpg, entre otros, salvo que las necesidades y naturaleza del servicio justifique su uso, lo cual deberá ser autorizado por la Oficina Regional de Tecnologías de la Información y Comunicación a petición del Gerente, Sub Gerente, Jefe o nomenclatura similar interesada.

m. El número máximo de destinatarios por cada correo enviado es de treinta (30) cuentas por vez, un número superior al indicado generaría un alto congestionamiento de la red y podría ser considerado en muchas organizaciones como correo SPAM, bloqueando el mismo. Ante la necesidad oficial de envío de mensajes masivos que superen el número de destinatarios indicados, la Oficina Regional de Tecnologías de la Información y Comunicación, en coordinación con las unidades orgánicas involucradas, determinará la mejor técnica posible que no perjudique el correcto desempeño de la red de datos.

n. La auto firma (nombre, cargo, teléfonos) en el correo electrónico debe ser breve e informativa, no debiendo ocupar más de tres líneas. No deberá incluirse la dirección de correo electrónico en la autofirma.

o. Constituye infracción administrativa funcional, pasible de sanción administrativa, las siguientes acciones en el uso del correo electrónico oficial:

   - Facilitar o ingresar la cuenta de correo electrónico en páginas de publicidades ajenas al sector público.
   - Suscribirse por internet a listas globales ajenas a la función institucional.
   - Utilizar el correo electrónico institucional para cualquier propósito ajeno al Gobierno Regional De Loreto.
   - El envío de mensajes que comprometan la información del Gobierno Regional De Loreto o que violen las normas sobre protección de datos personales, sin perjuicio de la responsabilidad penal, civil o administrativa a que hubiese lugar.
   - Finalmente, se responde formalmente a través de documento escrito o correo electrónico al Gerente, Sub Gerente, Jefe o nomenclatura similar solicitante sobre la creación de la cuenta de usuario y así como el apoyo técnico en el acceso a la plataforma.

VI.9.5. **Permiso de navegación en Internet.**

a. El Gerente, Sub Gerente, Jefe o nomenclatura similar, puede solicitar a la Oficina Regional de Tecnologías de la Información y Comunicación el acceso a las páginas de internet que se encuentren bloqueadas, cuando para el desarrollo de funciones y/o del servicio se requiera.

b. **Conectividad a internet.**

- El servicio de Internet debe estar utilizado únicamente para tareas y actividades que contribuyan al desarrollo institucional.
- La autorización de acceso a internet se concede exclusivamente para actividades de trabajo. Todo el personal del Gobierno Regional De Loreto tiene las mismas responsabilidades en cuanto al uso de internet.
- El acceso a internet se restringe exclusivamente a través de la Red establecida, es decir, por medio del sistema de seguridad con Firewall Proxy incorporado en la misma.
- No está permitido acceder a internet llamando directamente a un proveedor de servicio de acceso y usando un navegador, o con otras herramientas de internet conectándose con un modem.
- Sólo puede haber transferencia de datos desde o hacia internet en conexión con actividades propias del trabajo desempeñado.

c. **Internet Inalámbrico (WiFi)**

- La red inalámbrica es un servicio que permite conectarse a internet sin la necesidad de algún tipo de cableado. la Red inalámbrica le permitirá utilizar los servicios de Red, en zonas de cobertura del Gobierno Regional De Loreto, donde además de hacer uso del servicio de acceso a los sistemas, se puede acceder al servicio de internet de manera controlada.

- La Oficina Regional de Tecnologías de la Información y Comunicación es la encargada de la administración, habilitación y/o bajas de usuarios en la red inalámbrica de la institución.

d. **Excepciones.**

- En caso de eventos, cursos, talleres, conferencias, etc. Se podrán habilitar equipos con acceso a la red inalámbrica de manera temporal por el tiempo necesario, previa solicitud de los interesados con una anticipación de por lo menos un día hábil en relación al evento a desarrollar.

- En el caso de estos eventos las restricciones para acceder podrán ser "anuladas" temporalmente por la Oficina Regional de Tecnologías de la Información y Comunicación y en concordancia con el literal a) del numeral 6.9.5 de la presente directiva.

VI.9.6. **Acceso a la red.**

a. Para el acceso a la red y sistemas administrativo (tales como SIGA, SIAF, Correo institucional, Sistema de Tramite Documentario, Sistema de Caja Única, entre otros) el Gerente, Sub Gerente, Jefe o nomenclatura similar, solicita a la Oficina Regional de Tecnologías de la Información y Comunicación mediante documento escrito o correo institucional. La Oficina Regional de Tecnologías de la Información y Comunicación recibe y valida la factibilidad para realizar el cableado y habitación de IP del equipo de cómputo, y posteriormente generar permisos y restricciones.

b. El acceso a la red y demás servicios informáticos (tales como SIGA, SIAF, Correo Institucional, Correo Electrónico, etc.) podrán ser eliminados a petición del Gerente, Sub Gerente, Jefe o nomenclatura similar respectiva o del Jefe de la Sub Unidad de Recursos Humanos cuando comunique el cese laboral.

c. Ningún usuario recibirá un identificador de acceso a la red, recursos informáticos o aplicaciones hasta que no acepte formalmente el Formulario de Solicitud de Creación de Cuentas de Red. (Anexo 1)

d. Los usuarios pueden utilizar la infraestructura de la Red para proveer servicios a los usuarios terceros y/o visitas, previa autorización de la Oficina Regional de Tecnologías de la Información y Comunicación.

e. Cuando exista más de diez (10) minutos de inactividad del usuario en el computador, se activará una pantalla protectora para evitar el acceso a la red no autorizado.

VI.10. De la recepción de los servicios de tecnología de información.

VI.10.1. **Del uso adecuado del dominio del Programa.**

La Oficina Regional de Tecnologías de la Información y Comunicación poseerá una clave administradora para poder acceder y/o cambiar configuraciones de los equipos, ante necesidad justificada, previa solicitud y autorización del responsable de la unidad orgánica involucrada

VI.10.2. **Del uso adecuado de los correos gratuitos.**

El uso de correos gratuitos como el Hotmail, Gmail, Yahoo, Latín Mail, Mix Mail, Ec-Red, Terra, entre otros está limitado para el uso personal del servidor; y deben utilizarse con moderación y no deberá enviarse correos por fines de trabajo utilizando estas cuentas.

VI.10.3. De las prohibiciones en el uso de los servicios de tecnología de la información (correo, internet, red, etc.)

a. No se permite el uso de los servicios de la red cuando su uso no contribuye con los objetivos institucionales del Gobierno Regional De Loreto.

b. **Prohibiciones de Acceso a Internet**

- El acceso a ciertas categorías de sitios web, cualquier tipo de contenido explícito de pornografía, citas románticas, juegos, apuestas, chat y glamour y otros que establezca la Unidad de Administración a propuesta de la Oficina Regional de Tecnologías de la Información y Comunicación. La eventual disponibilidad de conectarse con un sitio web de estas categorías no implica que los usuarios estén autorizados a visitarlo.

- La descarga de archivos de música, videos, juegos y otros de tipo de entretenimiento debido a que el canal de comunicación de internet es sólo para fines laborales, salvo

excepciones debidamente justificadas y autorizadas a visitarlo.

- Uso de Juegos "On Line" en la red.
- Debido a la saturación que ocasiona el ejecutar los programas de radios por internet, tanto musicales como noticiosos, el uso de estas funcionalidades se encuentra restringido, salvo excepciones debidamente justificadas y autorizadas por la Unidad de Administración.

c. El uso desmesurado del correo, internet, red, que generen tráfico elevados, se cancelará la cuenta o se desconectará temporal o permanentemente al usuario o red involucrada.

d. Introducir en los Sistemas de Información o en la Red institucional contenidos obscenos, amenazadores, inmorales u ofensivos.

e. Introducir voluntariamente programas, virus, macros, applets, controles Active-X o cualquier otro dispositivo lógico o secuencia de caracteres que causen o sean susceptibles de causar cualquier tipo de alteración o daño en los Recursos informáticos.

C. Sobre la Información

VI.11. De la información y sus respaldos.

VI.11.1. La información generada por todas las unidades orgánicas es de propiedad del Gobierno Regional De Loreto y no de quien la elabora.

VI.11.2. La información adopta diversas formas que puede estar impresa o escrita en papel, asimismo puede ser almacenada a través de aplicaciones (sistemas usados para procesar y mantener información), transmitida por correo o medios electrónicos, mostrada en video o hablada en conversación. Debe protegerse adecuadamente cualquiera que sea la forma que tome o los medios por los que se comparta o almacene.

VI.11.3. Los activos de información deben ser utilizados de acuerdo a lo establecido por los responsables de la información.

VI.11.4. El usuario es responsable de organizar y mantener en orden la información contenida en el equipo de cómputo que le ha sido asignado.

VI.11.5. Los usuarios tienen especial cuidado con los dispositivos de almacenamiento, especialmente aquellos que hayan utilizado para guardar copias de sus archivos digitales y que forman parte de su acervo documentario.

VI.11.6. **Respaldo de la Información**

- Las Bases de Datos del Gobierno Regional de Loreto son respaldadas periódicamente/en forma automática y manual, según los procedimientos establecidos en la presente directiva.
- Las Bases de Datos tendrán una réplica en uno o más equipos remotos alojados en un lugar seguro que permita tener contingencia y continuidad del servicio.
- Los demás respaldos (una copia completa) deberán ser almacenados en un lugar seguro y distante del sitio de trabajo.
- Los/as usuarios/as que tengan asignada una computadora son responsables de realizar el respaldo de la información local. almacenada en el disco duro de su equipo, a fin de que pueda contar con su información de manera oportuna, para ello pueden usar USB o Disco Externo previa coordinación con la Oficina Regional de Tecnologías de la Información y Comunicación o en todo caso registrar una casilla en la nube.

VI.12. De la Administración de la Base de Datos

VI.12.1. El Administrador de la Base de Datos es el encargado de asignar las cuentas a los usuarios para el uso de servicios informáticos.

VI.12.2. El Administrador de la Base de Datos no debe eliminar ninguna información del sistema, a menos que la información esté dañada o ponga en peligro el buen funcionamiento del sistema.

VI.12.3. Las contraseñas serán asignadas por el Administrador de la Base de Datos en el momento en que el usuario desee activar su cuenta, previa solicitud del Gerente, Sub Gerente, Jefe o nomenclatura similar correspondiente.

VI.12.4. En caso de olvido de contraseña de un usuario, será necesario que se presente con el Administrador de la Base de Datos para reasignarle su contraseña.

VI.13. Del Plan de Contingencias.

La Oficina Regional de Tecnologías de la Información y Comunicación gestionará la aprobación y/o actualización del Plan de Contingencias, preferentemente, cada semestre, para que contenga las medidas técnicas, humanas y organizativas necesarias actualizadas para garantizar la continuidad de las labores en el Gobierno Regional de Loreto.

VI.14. De la Seguridad Perimetral.

La seguridad perimetral es uno de los métodos posibles de protección de la Red, basado en el establecimiento de recursos de seguridad en el perímetro externo de la red y en diferentes niveles. Esto permite definir niveles de confianza, permitiendo el acceso de determinados usuarios internos o externos a determinados servicios, y denegando cualquier tipo de acceso a otros. La Oficina Regional de Tecnologías de la Información y Comunicación implementa soluciones lógicas y físicas que impidan el acceso no autorizado a los equipos de la institución como, por ejemplo:

- Rechazar conexiones a servicios comprometidos.
- Permitir sólo ciertos tipos de tráfico (p.ej. correo electrónico, http, https).
- Proporcionar un único punto de interconexión con el exterior.

- Redirigir el tráfico entrante a los sistemas adecuados dentro de la intranet (Red interna).

- Ocultar sistemas o servicios vulnerables que no son fáciles de proteger desde internet.

- Auditar el tráfico entre el exterior y el interior.

- Ocultar información: nombres de sistemas, topología de la red, tipos de dispositivos de red, cuentas de usuarios/as internos.

VI.15. De las restricciones

VI.15.1. Nadie puede observar, copiar, alterar o destruir la información que reside en los equipos sin el consentimiento explícito del Gerente, Sub Gerente, Jefe o nomenclatura similar respectiva.

VI.15.2. Los usuarios no deben distribuir información referida a las vulnerabilidades del sistema y deben reportar rápidamente todas las alertas del sistema de seguridad de información. Los riesgos o fallas sospechosas y otras anomalías deben ser notificados en forma inmediata a la Oficina Regional de Tecnologías de la Información y Comunicación.

D. Sobre los Ambientes Tecnológicos del Centro de Comunicaciones

VI.16. De los Ambientes Tecnológicos.

VI.16.1. De las características mínimas.

a. La Oficina Regional de Tecnologías de la Información y Comunicación cuenta con ambientes tecnológicos como centro de cómputo (sala de datos) donde se ubican los sistemas de telecomunicaciones y servidores.

b. Todos los sistemas de comunicaciones están debidamente protegidos con la infraestructura apropiada de manera que el usuario no tenga acceso físico directo.

c. La Oficina Regional de Tecnologías de la Información y Comunicación debe señalizar las zonas de circulación y zonas restringidas de los centros de cómputo o áreas críticas (sala de datos).

d. La Sub Unidad de Logística en coordinación con la Oficina Regional de Tecnologías de la Información y Comunicación considerará los estándares vigentes de cableado estructurado durante el diseño de nuevas áreas de trabajo o la implementación de la mejora tecnológica de comunicaciones en el crecimiento de las áreas existentes.

e. El Centro de Computo debe contar con la siguiente infraestructura para su protección:

- Tener una puerta de acceso de vidrio templado transparente, para favorecer el control del uso de los recursos de cómputo.
- Ser un área restringida
- Tener un sistema de control de acceso que garantice la entrada sólo al personal autorizado por la Oficina Regional de Tecnologías de la Información y Comunicación.
- Recibir limpieza al menos una vez por semana que permita mantener el ambiente libre sin polvo.
- Estar libre de contactos e instalaciones eléctricas en mal estado.
- Aire acondicionado. Mantener a 21 grados centígrados.
- Seguir los estándares de protección eléctrica vigente para minimizar el riesgo de daños físicos de los equipos de telecomunicaciones y servidores.
- Contar con algún esquema que asegure la continuidad del servicio.
- Prevención y/o detección de incendios.
- Contar con extintores de incendio cercano a la data center.

VI.16.2. **Del acceso.**

a. El acceso de terceras personas a los ambientes tecnológicos es plenamente controlado y vigilado. Durante el acceso se debe portar una identificación que les será asignado por el área de seguridad.

b. Las visitas internas o externas a las instalaciones físicas de los ambientes tecnológicos se harán en el horario de 9:00 a.m. a 2:00 p.m., acompañados por una responsable de la Oficina Regional de Tecnologías de la Información y Comunicación.

VI.17. De los archivos compartidos

La Oficina Regional de Tecnologías de la Información y Comunicación proporciona acceso a las carpetas compartidas en el servidor únicamente al personal que indique el Gerente, Sub Gerente, Jefe o nomenclatura similar, quien podrá acceder usando sus credenciales de acceso.

VII. DISPOSICIONES COMPLEMENTARIAS.

Mediante la presente Directiva difundimos los objetivos de Seguridad de la Información que se esperan alcanzar, los cuales conseguiremos mediante la aplicación de controles de seguridad que permitan gestionar un nivel de riesgo aceptable, determinar y minimizar vulnerabilidades, garantizar la continuidad de los servicios, asegurar el cumplimiento de las obligaciones establecidas en las normas legales vigentes y los requisitos de seguridad destinados a impedir infracciones y violaciones que afecten la Seguridad de la Información en nuestra Institución.

VII.1. Propiedad de la Información

Toda la información generada y almacenada en los dispositivos de almacenamiento masivo y de respaldo del Gobierno Regional de Loreto - GOREL, pertenece a la entidad y no puede ser utilizada y/o aprovechada en beneficio personal o de terceros.

La información que es soportada por la infraestructura de tecnología informática del GOREL, pertenece a la entidad a menos que en una relación contractual se establezca lo contrario. Sin embargo, **la facultad de otorgar acceso a la información es del responsable del área que genera esa información**. Para el control de la información se asignarán responsables en cada unidad orgánica, quienes deben asegurar proporcionar el acceso a la

información que genere su área, con la finalidad de promover un adecuado ambiente de control y separación de funciones.

VII.2. Liderazgo y Compromiso

La Oficina Regional de Tecnologías de la Información y Telecomunicación adoptará las medidas necesarias para que la Directiva de Seguridad de la Información sea conocido únicamente por el personal de cualquier modalidad contractual en el Gobierno Regional de Loreto, y de esta forma:

VII.2.1. Verificar que la política de Seguridad de la Información y los objetivos de Seguridad de la Información estén alineados y sean compatibles con la dirección estratégica de la organización.

VII.2.2. Asegurar que el sistema de gestión de Seguridad de la Información este incluido en el Mapa de procesos de la organización.

VII.2.3. Asignar los recursos económicos necesarios para el adecuado funcionamiento del sistema de gestión de Seguridad de la Información.

VII.2.4. Resaltar la importancia de la Seguridad de la Información para el GOREL.

VII.3. Los casos no previstos que pudieran presentarse en la Directiva serán resueltos por la Oficina Regional de Tecnologías de la Información y Telecomunicación, el Comité de Gestión de Seguridad de la Información, el Oficial de la Seguridad de la Información y el Equipo de Respuestas ante Incidentes de Seguridad Digital.

VIII. RESPONSABILIDAD

Son responsables directos del cumplimiento de la presente Directiva General, todos los servidores civiles del Gobierno Regional de Loreto. (Los servidores civiles de las entidades públicas se clasifican en los siguientes grupos:

a) Funcionario público.
b) Directivo público.
c) Servidor Civil de Carrera.
d) Servidor de actividades complementarias. BASE LEGAL: Ley del Servicio Civil Ley Nº 30057 (Artículo 2); Cualquiera que mantiene un vínculo laboral o contractual con la entidad.

La Oficina Regional de Tecnologías de la Información y Comunicación es responsable de gestionar el uso adecuado de los recursos informáticos (físicos y lógicos), así como la protección frente a las amenazas propias del internet. es la unidad orgánica responsable de brindar los servicios informáticos, de aprobar la incorporación de tecnologías de información vinculadas con el desarrollo y operación de los sistemas de información y el mantenimiento de los equipos de cómputo asignados a los usuarios. Del buen funcionamiento de los equipos informáticos y servicios, brindando el soporte adecuado para el normal desempeño de las labores de los usuarios de manera eficaz y eficiente.

El usuario que recibe los servicios informáticos solicitados o necesarios para su desempeño, es responsable del cumplimiento de la presente Directiva, del uso adecuado de los equipos de cómputo, del software utilizado y de los datos administrados. Los usuarios son responsables del cuidado físico y lógico de los equipos de cómputo, así como, del uso de sus credenciales (usuario/contraseña). El usuario que ceda su acceso a otra persona, sigue siendo responsable de las actividades que este tercero realice.

La Oficina de Control Institucional, en merito a sus funciones de control Previo, Control Concurrente y Control Posterior es la responsable de velar, apoyar y reportar oportunamente por el cumplimiento de la presente directiva.

IX. ANEXOS

IX.1. DEFINICIONES

IX.2. Formatos para Inducción, Capacitación y Actas de Mantenimiento Preventivo y Correctivos al Parque Informático

ANEXO 1

DEFINICIONES

Para efectos de la Aplicación y cumplimiento de la presente Directiva, téngase en cuenta las siguientes definiciones:

- **Base de Datos:**
  Es el conjunto de datos pertenecientes a un mismo contexto, organizados y almacenados sistemáticamente para su posterior uso.
  La administración de la Base de Datos recae en el personal de la Oficina Regional de Tecnologías de la Información y Comunicación.

- **Contraseña:**
  Conjunto de caracteres que permite el acceso de un/a usuario/a un recurso informático (password).

- **Data Center:**
  Se denomina centro de procesamiento de datos a aquella ubicación donde se concentran los recursos de tecnología de información necesarios para el procesamiento de información.

- **Hardware:**
  Constituye todas las partes físicas y tangibles de una computadora

- **Información:**
  Es el conjunto organizado de datos procesados que constituyen un conocimiento y como tal merece darle una protección adecuada.

- **Medios Físicos:**
  Conjunto de elementos físicos que componen un ordenador, tales como el Disco Duro, CD ROM, disquetera, Memoria USB; en dicho conjunto incluyen los dispositivos electrónicos y periféricos.

- **Protección de la Información:**
  Consiste en proteger la información de un amplio rango de amenazas (terremotos, incendios, virus informáticos, etc.) para asegurar la continuidad de los procesos, minimizar los daños a la entidad y maximizar la prestación de los servicios del Gobierno Regional de Loreto.

- **Recursos Informáticos:**
  Se entiende por recurso informático a la generalidad de equipos informáticos (hardware) y programas de ordenador (software y sistemas de información),

cuyo uso y aplicación adecuados es normado por la Oficina Regional de Tecnologías de la Información y Comunicación.

- **Red:**
  Se refiere a la red de datos, consiste en la interconexión de las computadoras con que cuenta el GOBIERNO REGIONAL DE LORETO. La red de datos incluye el hardware como el software necesario para la interconexión de los distintos dispositivos.

- **Seguridad de Recursos Informáticos:**
  La seguridad de los recursos informáticos se enfoca en la protección de la infraestructura computacional y todo lo relacionado con esta con la finalidad de minimizar los posibles riesgos a la infraestructura.

- **Servicios de las Tecnologías de Información:**
  Se refiere a los servicios informáticos (usuario en el dominio, correo electrónico, sistemas administrativos, internet entre otros servicios informáticos), que se brinda en la entidad.

- **Sistema de Comunicación:**
  Se refiere al equipo activo y los medios de comunicación.

- **Software:**
  Constituye la parte intangible y lógica de una computadora (aplicaciones y programas)

- **Soporte Técnico Informático:**
  Es el servicio de asesoría, mantenimiento preventivo y correctivo que brinda la Oficina Regional de Tecnologías de la Información y Comunicación a los/las usuarios/as del GOBIERNO REGIONAL DE LORETO, en forma presencial o remota, mediante comunicaciones telefónicas, por correo electrónico institucional o por cualquier otro medio de comunicación interna.

- **Terceros:**
  Proveedores/as de servicios o visitas externas.

- **Usuario/a:**
  Persona que hace uso de los servicios de las tecnologías de información proporcionada por la Oficina Regional de Tecnologías de la Información y Comunicación, tales como equipos de cómputo o sistemas informático.