RESOLUCION EJECUTIVA REGIONAL N° 627 - 2021-GRU-GR

Pucallpa, 31 DIC. 2021

VISTO; El INFORME N° 062-2021-GRU-SG-OTI, INFORME N° 014-2021-GRU-GRPP-SGDI/LPF, INFORME N° 217-2021-GRU-GRPP-SGDI, INFORME LEGAL N° 105-2021-GRU-GGR-ORAJ/TTC, y el texto de la Directiva, y;

CONSIDERANDO:

Que, de conformidad con el Artículo 191° de la Constitución Política del Perú, concordante con el Artículo 2° de la Ley N° 27867 – Ley Orgánica de Gobiernos Regionales, establece que los Gobiernos Regionales, son personas jurídicas de derecho público, con autonomía política, económica y administrativa en asuntos de su competencia;

Que, mediante el Decreto Legislativo N° 1412, se aprueba la Ley del Gobierno Digital, que 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;

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

Que, el numeral 5.2 de la antes citada Norma Técnica establece que la Alta Dirección debe establecer una política de seguridad de la información que sea apropiada para el propósito de la organización, que incluya objetivos de seguridad de la información o proporcione un marco de referencia para fijarlos, así como incluye compromisos para satisfacer los requisitos aplicables relacionados a la seguridad de la información y para la mejora continua del sistema de gestión de la seguridad de la información, debiendo dicha política estar disponible como información documentada, comunicarse dentro de la organización y estar disponible para las partes interesadas según corresponda;

Que, en ese propósito, mediante Resolución Ministerial N° 119-2018-PCM modificada por la Resolución Ministerial N° 087-2019-PCM, se establece que cada entidad de la Administración Pública debe constituir un Comité de Gobierno Digital con competencias, entre otras, en materia de seguridad de la información;

Que, mediante Decreto Supremo Nº 081-2013-PCM, se aprueba la Política Nacional de Gobierno Electrónico 2013 – 2017, que prevé determinados lineamientos estratégicos para el Gobierno Electrónico en el Perú, entre otros, el relacionado con la Seguridad de la Información (...);

Que, en el marco de las disposiciones contenidas en las normas precedentemente acotadas, la Oficina de Tecnologías de la información ha propuesto la

directiva denominada "políticas de seguridad de la información del Gobierno Regional de Ucayali";

Que, en uso de las facultades conferidas por la Ley N° 27867 – Ley Orgánica de Gobiernos Regionales y sus modificatorias, ACUERDO REGIONAL Nº 161-2021-GRU-CR de fecha 15 de diciembre de 2021; contando con las visaciones de la Gerencia General Regional, Gerencia Regional de Planeamiento y Presupuesto, Oficina Regional de Administración, Oficina Regional de Asesoría Jurídica, la Sub Gerencia de Desarrollo Institucional, Secretaria General, y la Oficina de Tecnologías de la Información y;

SE RESUELVE:

ARTÍCULO PRIMERO: APROBAR la **Directiva N° 028-2021-GRU-GR-GGR-GRPP-SGDI** "***DIRECTIVA DE POLITICAS DE SEGURIDAD DE LA INFORMACIÓN DEL GOBIERNO REGIONAL DE UCAYALI***", el cual forma parte de la presente Resolución.

ARTICULO SEGUNDO: DISPONER a la Oficina de Tecnologías de la Información el cumplimiento y la publicación de la presente resolución y la Directiva en el portal de transparencia del Gobierno Regional de Ucayali (*www.regionucayali.gob.pe*).

ARTÍCULO TERCERO: ENCARGAR a la Secretaria General la notificación del presente acto resolutivo a todas las Unidades Orgánicas de la Sede Central del Gobierno Regional de Ucayali, para su conocimiento, implementación y cumplimiento.

REGÍSTRESE, COMUNÍQUESE Y CÚMPLASE.

GOBIERNO REGIONAL DE UCAYALI

Med. Cir. Angel Luis Gutiérrez Rodríguez
GOBERNADOR REGIONAL (e)

DIRECTIVA Nº 028-2021-GRU-GR-GGR-GRPP-SGDI

DIRECTIVA DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN DEL GOBIERNO REGIONAL DE UCAYALI

I. OBJETIVO

Los Lineamientos de Seguridad de la Información tiene como objetivo salvaguardar los activos de información del GRU y los sistemas de información que soportan 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 mismo, la de garantizar la continuidad de los sistemas de información propios.

Del mismo modo, a través de la implementación los lineamientos materia del presente documento, se busca que la Seguridad de la Información forme parte de la cultura organizacional en la gobernanza de la institución, en todas las unidades orgánicas que pertenecen a la Sede Central, Sede ExInpe, Sede Apurímac, Sede Aldea Infantil San juan, Sede Gerencia Forestal y de Fauna Silvestre, Sede Defensa Nacional, Seguridad Ciudadana y Defensa Civil.

II. FINALIDAD

Con las políticas de seguridad de la información, el Gobierno Regional de Ucayali, tiene la finalidad de lograr garantizar la confidencialidad, integridad y disponibilidad de la información y minimizar los riesgos que le afectan

III. ALCANCE

La presente Directiva es de alcance para todos los funcionarios, empleados de confianza y servidores públicos nombrados o contratados, independientemente del régimen laboral al que pertenezcan, prestando servicios en las diferentes unidades orgánicas y órganos desconcentrados (especializados y territoriales).

En todos los casos se hará referencia al órgano, indistintamente de si pertenece al GRU.

De otro lado, ya que tanto el GRU como los órganos desconcentrados, órganos desconcentrados especializados y órganos desconcentrados territoriales cuentan con su propio personal de apoyo informático, y que corresponden a Unidades Ejecutoras distintas; en los casos que se haga mención a la OTI, se entenderá que se trata de la Oficina de Tecnologías de la Información del GRU, y en los casos que se haga mención a un Órgano Desconcentrado se entenderá que se trata del Especialista en Informática de dicho órgano desconcentrado.

Así mismo, en esta Directiva contiene disposiciones de aplicación a más de un órgano o programa, por lo que su alcance es de carácter General.

Se considera para el presente documento de manera específica las siguientes políticas de Seguridad de la información:

- Política de Organización de la Seguridad de la información.
- Política de Seguridad Relativa a los Recursos Humanos, de Formación y Concientización.
- 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 de Protección y Privacidad de Datos Personales.
- Política de Seguridad de la Información en la Gestión de Proyectos.

IV. BASE LEGAL

- Ley N° 30096, Ley de Delitos Informáticos.
- Ley N° 27269, Ley de Firmas y Certificados Digitales y su Reglamento, aprobado mediante Decreto Supremo N° 052-2008-PCM.
- Ley N° 27444, Ley del Procedimiento Administrativo General.
- Ley N° 27658, Ley Marco de Modernización de la Gestión del Estado.
- Ley N° 28612, Ley que norma el uso, adquisición y adecuación del software en la Administración Pública.
- Ley Nº 29733 Ley de Protección de Datos Personales
- Ley Nº 28716 - Ley de Control Interno de las Entidades del Estado.
- Decreto Legislativo N°822, Ley sobre el Derecho de Autor.
- Decreto Supremo N°043-2003-PCM, aprueba Texto Único Ordenado de la Ley Nº 27806, Ley de Transparencia y Acceso a la Información Pública.
- Decreto Supremo N°024-2006-PCM, Reglamento de la Ley N°28612; Ley que norma el uso, adquisición y adecuación del software en la administración pública.
- Resolución Ejecutiva Regional N° 256-2021-GRU-GR, que aprueba la Directiva N°0011-2021-GRU-GRPP-SGDI "Normas para La Formulación, Actualización, Modificación y Aprobación de Directivas Internas y Reglamentos en las Unidades Ejecutoras conformantes del Pliego 462: Gobierno Regional del Departamento de Ucayali"
- Ordenanza Regional N°010-2016-GRU-CR el cual deroga la Ordenanza Regional N° 007-2014-GRU/CR, que aprueba el Reglamento de Organización y Funciones del Gobierno Regional de Ucayali.

- Resolución Ministerial N° 073-2004-PCM, que aprueba la Guía para la Administración Eficiente de Software Legal en la Administración Pública.
- Resolución Ministerial N°139-2004-PCM mediante la cual aprueban el documento "Guía técnica sobre evaluación de software para la Administración Pública".
- Resolución Ministerial N° 004-2016-PCM, aprueba el uso obligatorio de la Norma Técnica Peruana "NTP ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 2a. Edición".
- Resolución Ministerial Nº 087-2019-PCM que aprueba disposiciones sobre la conformación y funciones del Comité de Gobierno Digital.
- Resolución Contraloría General N°320-2006-CG, que aprueban las Normas de Control Interno para el Sector Público.
- Resolución Jefatural N°053-2003-INEI que aprueba la Directiva N°004-2003-INEI/ONTP "Norma Técnica para la implementación del Registro de Recursos Informáticos en las Instituciones de la Administración Pública".
- Resolución Jefatural N°347-2001-INEI, aprueban Directiva "Normas y Procedimientos Técnicos para garantizar la Seguridad de la Información publicadas por las entidades de la Administración Publica".
- Directiva N°010-2002-INEI/DTNP "Normas Técnicas para la Asignación de Nombres de Dominio de las entidades de la Administración Pública".
- Directiva N° 004-2016-OSCE/CD "Lineamientos para la contratación en la que se hace referencia a determinada marca o tipo particular", aprobada mediante resolución N° 011-2016-OSCE/PRE de fecha 09 de enero de 2016.
- Ordenanza Regional Nº 002-2018-GRU-CR – Aprueba el Reglamento de Organización y Funciones ROF, del Gobierno Regional de Ucayali.
- Ordenanza Regional N° 003-2019-GRU-CR, que aprueba la modificación estructural del Reglamento de Organización y Funciones - ROF del Gobierno Regional de Ucayali.

V. DISPOSICIONES GENERALES

6.1 Responsabilidades comunes

Los lineamientos de Seguridad de la Información son de obligatorio cumplimiento para todos los empleados o servidores bajo cualquier régimen laboral o modalidad contractual, considerando incluso a los proveedores de servicios, que tengan acceso o que desarrollen, adquieran o usen sistemas de información de la institución.

6.2 Sanciones por falta

El Gobierno Regional de Ucayali, en el marco de sus facultades para tomar medidas administrativas disciplinarias sobre los servidores (empleados) que devengan de una falta dispuesta en los Lineamientos de Seguridad de la Información conforme a los documentos normativos de la institución, sin perjuicio de las acciones civiles y/o penales que pudieran conllevar su aplicación.

VI. DISPOSICIONES ESPECÍFICAS

7.1 Política de Organización de la Seguridad de la Información.

7.1.1 Objetivo:

Establecer un marco de referencia de la gestión para iniciar y controlar la implementación y operación de la gestión de la seguridad de la información dentro de la entidad.

7.1.2 Política:

a) Roles y responsabilidades

El Gobierno Regional de Ucayali, deberá 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, entre otras actividades específicas de seguridad de la información. Los roles se definen en los perfiles de puestos, en los contratos, en documentos normativos y/o documentos administrativos internos.

b) Segregación de Funciones

- El Gobierno Regional de Ucayali, deberá segregar funciones para reducir oportunidades de modificación no autorizada o no intencional o mal uso de los activos de la organización. En el Reglamento de Organización y Funciones (ROF) el GRU consigna la segregación de funciones a partir de las unidades orgánicas.
- Por otro lado, la designación del Oficial de Seguridad de la Información (OSI) y las funciones del Comité de Gobierno Digital (CGD), que incluye al Oficial de Seguridad de la Información, otorga al GRU realizar con agentes internos de control transversal la participación directa de la alta dirección.

c) Contacto con autoridades y grupos de interés

- El Gobierno Regional de Ucayali, a través del Oficial de Seguridad de la Información, del Equipo de Respuestas ante Incidentes de Seguridad Digital y del Comité de Gobierno Digital, mantendrá contacto con la Secretaría de Gobierno Digital (SeGDi) de la Presidencia del Consejo de Ministros, con el Equipo de Respuesta ante Incidentes de Seguridad Digital Nacional (PeCERT) y el

Centro Nacional de Seguridad Digital, de acuerdo con los requerimientos en materia de seguridad sobre la materia. Esto incluye la obligación de notificar al Centro Nacional de Seguridad Digital todo incidente de seguridad digital, implementada a través del Procedimiento Gestión de atenciones TIC y Eventos e Incidentes de Seguridad de la Información.

- A raíz de la colaboración interinstitucional, el Oficial de Seguridad de la Información participará en los grupos de trabajo interinstitucionales Ad Hoc que se establezcan. Adicionalmente, el jefe de la Oficina de Tecnologías de la Información impulsará el contacto y mutua colaboración técnica con los proveedores especializados en servicios relacionados con la seguridad de la información.

d) Seguridad de la Información en la Gestión de Proyectos

- La Oficina de Tecnologías de la Información del GRU, en coordinación con la Oficina de Planeamiento y Presupuesto, deben gestionar que se integre la seguridad de la información en el proceso de gestión de proyectos de la institución, incluyendo a todos los tipos de proyectos, para garantizar que los riesgos de seguridad de la información sean identificados y tratados oportunamente.

- Los proyectos de inversión pública, en el marco del sistema nacional de programación multianual de inversiones, en la etapa de formulación de proyectos se debe incorporar una evaluación de riesgos de seguridad de la información para identificar los riesgos y determinar los controles necesarios. La evaluación de riesgos debe cubrir las etapas de formulación y evaluación, ejecución y funcionamiento del proyecto.

- Los proyectos de inversión pública en el marco del sistema nacional de programación multianual de inversiones, durante la elaboración del perfil del proyecto, así como el expediente técnico o documento equivalente, deberán incorporar entre sus objetivos, objetivos de seguridad de la información del proyecto, alineados con los objetivos generales del sistema de gestión.

- Los proyectos de carácter interno que no son parte del sistema nacional de programación multianual de

inversiones, en las etapas de diseño, implementación y operación se deberá incorporar la evaluación de riesgos de SI. En la etapa del diseño del proyecto, se deberá hacer referencia a los objetivos del sistema de gestión de seguridad de la información con los que contribuye.

e) Dispositivos Móviles

- El GRU utiliza dispositivos móviles institucionales y permite la utilización de dispositivos móviles de propiedad privada, bajo control y autorización. En cualquier caso, el GRU, a través de la Oficina de Tecnologías de la Información, realizará el monitoreo de la actividad en los dispositivos móviles, por ejemplo, los intentos fallidos de autenticación.

- La Oficina de Tecnologías de la Información del GRU es responsable de autorizar a los servidores y a los proveedores de servicio sobre el uso de dispositivos móviles en las instalaciones del GRU y sobre la instalación y uso de aplicaciones y servicios del GRU en dispositivos móviles de su propiedad, que sean necesarios para la prestación del servicio.

- Toda asignación de dispositivos móviles institucionales será justificada, requerida y aprobada por la jefatura de la unidad orgánica correspondiente, con el posterior VoBo de la Oficina de Tecnologías de la Información; la asignación será documentada en registros.

- Todo dispositivo móvil institucional o de propiedad de personas naturales que se apruebe para utilizarse con servicios o aplicaciones del GRU, deberá implementar algún método de autenticación para el acceso.

- Los servidores que no cuenten con un teléfono móvil institucional y requieran utilizar la cuenta de correo electrónico del GRU en sus teléfonos personales, deberán requerirlo a la Oficina de Tecnologías de la Información con el VoBo previo de la jefatura de la unidad orgánica a la que pertenecen.

- Para cualquier aplicación o servicio del GRU que se utilice en dispositivos móviles institucionales o de propiedad privada, los usuarios deberán firmar un acuerdo de usuario final en el que reconocen sus

obligaciones y aceptan que la institución puede ejercer monitoreo a las actividades realizadas.

- Las actividades de instalación y configuración de las aplicaciones de los dispositivos móviles, son realizadas por La Oficina de Tecnologías de la Información del GRU. Se debe verificar la configuración de seguridad de los aún Anexo N° 01 Checklist de configuración de seguridad de dispositivos móviles.

- El servidor del GRU debe proteger sus dispositivos móviles, no debiendo entregarlos a otra persona, en particular en aquellos dispositivos inteligentes que pueden acceder a información interna o confidencial de la entidad. En estos casos, incluso los mensajes recibidos de números o remitentes desconocidos deben ser denegados y borrados sin ser abiertos. Los servidores deben evitar utilizar redes inalámbricas públicas o desconocidas.

- El GRU no emplea los dispositivos móviles para almacenar información directamente, por lo que no serán sometidos a copias de respaldo.

- El GRU a través de La Oficina de Tecnologías de la Información debe mantener una administración centralizada de las características de los dispositivos móviles y las aplicaciones instaladas en ellos que procesan o almacenan información crítica.

- En caso de pérdida o robo de dispositivos móviles institucionales, se debe proceder de la siguiente manera:

  - ✓ El usuario debe reportar el hecho tan pronto sea posible a la Oficina de Gestión Patrimonial (en caso de dispositivos propiedad del GRU).

  - ✓ reportar la pérdida o robo de acuerdo a la DI-004-2020-IGP Directiva de Normas de austeridad y uso del servicio de telefonía móvil institucional.

- En caso de pérdida o robo de dispositivos móviles de propiedad privada que hayan sido autorizados para utilizar el correo institucional, se debe proceder de la siguiente manera:

- ✓ El usuario debe reportar el hecho tan pronto sea posible a la Oficina de Tecnologías de la Información.

- ✓ El personal de la Oficina de Tecnologías de la Información eliminará el contenido del correo electrónico institucional del equipo, a través de la consola central de control del correo electrónico.

f) Trabajo Remoto

- El Gobierno Regional de Ucayali, empleará el trabajo remoto para acceder y procesar información, más no ha previsto almacenar información en sitios de trabajo remoto para usuarios finales.

- El trabajo remoto podrá ser activado ante la aplicación de protocolos sanitarios que exijan el distanciamiento social o por necesidad de las unidades orgánicas, en cuyo caso, el jefe inmediato requerirá a la Oficina de Gestión de las Personas, la modificación del lugar de prestación de servicios, variando el centro de labores habitual de trabajo al domicilio. La comunicación que la Oficina de Gestión de las Personas emite al servidor debe ser notificada a la Oficina de Tecnologías de la Información del GRU, para la activación de los controles de seguridad de la información correspondientes.

- En el caso de utilizar dispositivos móviles, se aplicará la política específica de dispositivos móviles del presente documento.

- La Oficina de Tecnologías de la Información del GRU brindará asesoramiento a los servidores en cuanto a la configuración de redes domésticas y configuración de servicios de red inalámbricos de modo que se maximice el nivel de seguridad.

- El ancho de banda mínimo para viabilizar el trabajo remoto es en promedio 4Mbps.

7.2 Política de Seguridad Relativa a los Recursos Humanos de Formación y de Concientización

7.2.1 Objetivo

Asegurar una correcta gestión de los recursos humanos en el Gobierno Regional de Ucayali, siendo los servidores parte fundamental del resguardo de la Seguridad de la información.

7.2.2 Política

a) Antes del Empleo - Selección, Términos y Condiciones Laborales.

- La Oficina de Gestión de las Personas del Gobierno Regional de Ucayali, debe verificar y registrar los antecedentes laborales y las competencias requeridas para el puesto, según el procedimiento de selección y contratación de Personal y utilizando las herramientas de consulta, para ello se tiene disponible la Plataforma de Interoperabilidad del Estado (PIDE). Entre los que se tiene a los siguientes:
  - ✓ Registro de Grados y Títulos.
  - ✓ Registro Nacional de Sanciones de Destitución y Despidos (RNSDD).
  - ✓ Antecedentes policiales, penales y judiciales.
  - ✓ REDAM Registro Nacional de Deudores Alimentarios

- La Oficina de Gestión de las Personas del Gobierno Regional de Ucayali, aplicará los criterios de selección establecidos para detener el proceso de contratación o continuar con el mismo de acuerdo con la información de los registros consultados.

- Para el caso de los cargos de confianza donde no se aplica el proceso de selección, se recupera la documentación de los mismos registros que se consultan en un proceso de selección y contratación; de observarse antecedentes perniciosos, se comunican a la alta dirección, quedando a su discreción cualquier acción posterior.

- La Oficina de Gestión de las Personas del Gobierno Regional de Ucayali, deberá 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.

- La Oficina de Logística en el marco del procedimiento contrataciones de bienes y servicios por montos menores o iguales a ocho UIT, incluirá en las órdenes de compra (o/c) u órdenes de servicios (o/s) los compromisos de seguridad de la información necesarios, conservando la evidencia de la confirmación de la recepción.

- La Oficina de Tecnologías de la Información del Gobierno Regional de Ucayali, podrá generar declaraciones juradas de confidencialidad y compromiso con otras exigencias de seguridad de la información, por ejemplo, para personal de proveedores de servicios, si el caso amerita.

b) Durante el Empleo – Responsabilidad de la Alta Dirección, Concientización y Capacitación, Proceso Disciplinario.

- La alta dirección del Gobierno Regional de Ucayali se asegura que los servidores del GRU y los proveedores sean instruidos oportunamente sobre sus roles y responsabilidades de seguridad de la información a través de las funciones de las unidades orgánicas correspondientes (Oficina de Gestión de las Personas, Oficina de Logística y la Oficina de Tecnologías de la Información.

- La alta dirección del Gobierno Regional de Ucayali, demostrará apoyo a las políticas, los procedimientos, lineamientos y controles de seguridad de la información al suscribir los documentos normativos correspondientes. Adicionalmente, comunicará directamente a los servidores la importancia del cumplimiento de los requisitos a través de los canales institucionales.

- La Oficina de Gestión de las Personas del Gobierno Regional de Ucayali, debe comunicar a los servidores del GRU, 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.

- La Oficina de Gestión de las Personas del Gobierno Regional de Ucayali, en coordinación con la Oficina de Tecnologías de la Información deberá establecer programas de inducción para los nuevos servidores, así como, actualizaciones regulares sobre políticas, procedimientos y otros documentos normativos.

- La Oficina de Gestión de las Personas del Gobierno Regional de Ucayali, debe comunicar a la Oficina de Tecnologías de la Información del GRU, cuando corresponda, el inicio, rotación del vínculo laboral de los servidores para el otorgamiento de acceso a los Sistemas de información.

- La Oficina de Tecnologías de la Información, en coordinación con la Oficina de Tecnologías de la Información, programará actividades de formación y capacitación en el marco del sistema de gestión de la seguridad de la información para asegurar que los colaboradores conozcan sus roles y responsabilidades, adquieran las competencias necesarias y se logre una cultura de prevención en seguridad de la información fortalecida. Esto será realizado en el marco del Procedimiento de Capacitación o a través de un Cronograma de Capacitación y Concientización propio de la Oficina de Tecnologías de la Información.

- La Oficina de Logística, en coordinación con la Oficina de Tecnologías de la Información, deberá incluir en los Términos de Referencia de bienes y servicios relacionados con la seguridad de la información, como son: servicios de internet, firewall, servicios web, etc. Los requisitos relacionados con actividades de formación técnica para los administradores de servicios, usuarios y dueños de activos de información del Gobierno Regional de Ucayali.

- La Oficina de Tecnologías de la Información, en coordinación con el Oficial de Seguridad de la Información, incluirán actividades internas de formación y de concientización.

- La Oficina de Tecnologías de la Información en coordinación con la Oficina de Imagen Institucional, complementarán las actividades de formación y concientización, con campañas audiovisuales de temas específicos, que utilicen un lenguaje sencillo, ejemplos y casos para atraer la atención de los usuarios.

- La Oficina de Gestión de las Personas del Gobierno Regional de Ucayali, puede iniciar procesos disciplinarios y/o acciones legales pertinentes a los servidores que incumplan las políticas de seguridad de la información y disposiciones en los documentos normativos de seguridad de la información establecidos. En este caso, el inicio del proceso debe ser requerido por la Oficina de Tecnologías de la Información, tras verificar las evidencias de incumplimiento. Las referencias de estas evidencias deberán igualmente ser proporcionadas por la Oficina de Tecnologías de la

Información. Las acciones a tomarse en los procesos disciplinarios deben utilizar las escalas indicadas en el Reglamento Interno de Servidores Civiles o documento análogo aplicable y deberán aplicarse los documentos normativos adicionales que se aprueben.

c) Después del Empleo.
- Las responsabilidades y deberes que permanecen válidos luego de la desvinculación se encuentran en los contratos.
- La Oficina de Gestión de las Personas del Gobierno Regional de Ucayali, deberá comunicar a la Oficina de Tecnologías de la Información del GRU, 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 el proceso de bloqueo de los accesos a los sistemas de información y demás recursos institucionales.

7.3 Política de Gestión de Seguridad de Activos de Información

7.3.1 Objetivo

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

7.3.2 Política

a) Inventario de Activos de Información La Oficina de Tecnologías de la Información del Gobierno Regional de Ucayali, deberá mantener un inventario de activos de información actualizada y revisada periódicamente, asimismo, dicho inventario debe contar con un propietario de activo de información. Esto será realizado a través del procedimiento Metodología de Gestión de Riesgos de Seguridad de la Información.

b) Los propietarios de activos de información son responsables de la gestión del activo de información durante todo su ciclo de vida, y deberán:
1. Asegurarse que los activos son inventariados.
2. Asegurarse que los activos son clasificados y protegidos adecuadamente.
3. Definir y revisar periódicamente las restricciones de acceso y las clasificaciones de activos importantes, teniendo en cuenta las políticas aplicables de control de acceso.
4. Garantizar el manejo adecuado cuando el activo es eliminado o destruido.

c) Uso de Activos de información

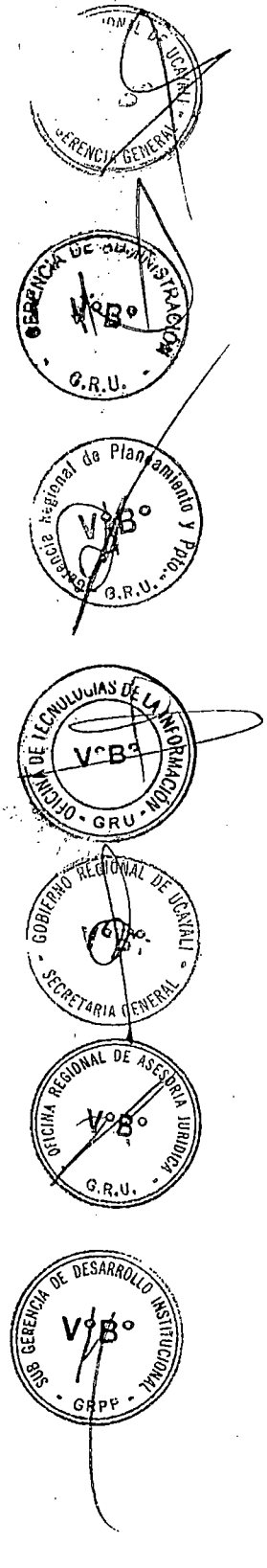
- Los empleados deberán usar los activos de información para los fines y objetivos del GRU, de acuerdo con los documentos normativos, la política, y procedimientos que se definan, y considerando los criterios de buen uso consignados en el Anexo N° 02 Uso Aceptable de Activos de información.
- Se deberá cumplir con los documentos normativos específicos, que cubren las prácticas requeridas para bienes y locales del Gobierno Regional de Ucayali:
- En el marco de las relaciones que el GRU deberá 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.

d) Devolución de Activos de información
- El Gobierno Regional de Ucayali, ha establecido el procedimiento para el retorno de los activos de información de la Entidad de los servidores que dejan de laborar en la institución. a través de la Directiva N° 0007-2020-GRU-GRPP-SGDI, procedimientos para la suscripción del Acta de Entrega-Recepción de cargo en las Unidades Ejecutoras conformantes del Pliego 462: Gobierno Regional de Ucayali", aprobado con Resolución Ejecutiva Regional 122-2020-GRU-GR.

e) Clasificación y manejo de la información
- 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.
- Los propietarios de los activos de información deberán etiquetar la información según la clasificación realizada. La información pública (pública e interna) no necesita una etiqueta. La información confidencial será etiquetada inicialmente en el documento que se utilice para realizar el inventario de activos de información y se aplicarán etiquetas en los metadatos asociados a la información. Esto se realiza en el marco del procedimiento Gestión de Activos de Información.

DENOMINACIÓN	DESCRIPCIÓN	CATEGORÍA EN EL GRU
Información Confidencial	Aquella información que es	Incluyendo a los datos de

	considerada como confidencial de acuerdo a lo establecido en el Texto Único Ordenado de la Ley 27806, Ley de Transparencia y Acceso a la Información Pública.	carácter personal y sensible de servidores, clientes y demás personas naturales sobre las cuales el GRU, efectuará algún tratamiento de información para un fin determinado declarado como banco de datos personales. Usuarios y contraseñas a los sistemas; valores de contratación. Este tipo de información debe estar protegido del acceso no 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 de Transparencia y Acceso a la Información Pública. El GRU cataloga esta información en: Información Pública e Información de Uso Interno.	<u>Información Pública</u> Aquella que de acuerdo a la normativa nacional vigente se encuentra publicada en el Portal de Transparencia estándar. Se debe manejar de modo que tenga altos niveles de disponibilidad.



		Información de Uso Interno Aquella información que se encuentra en la Intranet de la Institución. Esta información se manejará según las competencias de las unidades orgánicas, estableciendo permisos de lectura / escritura para evitar modificaciones no intencionales.

f) Gestión de Medios Removibles:

- El Gobierno Regional de Ucayali, no autorizará la utilización de medios removibles personales, para tal efecto pone a disposición los servicios de productividad suficientes.
- El Gobierno Regional de Ucayali, solamente autorizará los medios removibles portátiles aprobados por la Oficina de Tecnologías de la Información.
- Para el caso de los discos duros removibles y similares utilizados en computadoras de usuarios y servidores, la Oficina de Tecnologías de la Información del Gobierno Regional de Ucayali, brinda la asistencia técnica que se requiera.
- Para la eliminación de medios, se procede según el Anexo III Eliminación de Medios Removibles en caso corresponda. y se mantendrán los registros de las comunicaciones de las actividades realizadas.
- El servidor en el Gobierno Regional de Ucayali, para proteger los medios que contienen información durante su transporte se debe seguir los siguientes criterios:
  1. Documentar una hoja de ruta
  2. Realizar el lacrado del medio removible o el equipo en el que se encuentra instalado.

3. De utilizarse proveedores, deben ser aprobados, incluyendo la revisión de antecedentes del personal asignado
4. Personas autorizadas.
5. Utilizar vehículos y material de embalaje suficiente y de acuerdo con especificaciones de los fabricantes de hardware.
6. No trasladar medios con soportes magnéticos (discos duros) en contacto con otros equipos que incluyen imanes potentes, como parlantes para eventos.
7. Elaborar un informe de transferencia de medios que contenga información, incluyendo la hoja de ruta utilizada y las horas de inicio, llegada y cualquier parada planificada o no planificada.

7.4 Política de Control de Accesos

7.4.1 Objetivos

- 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.
- Controlar los accesos a la información.
- Prevenir accesos no autorizados a los sistemas de información y a los servicios de red.
- Restringir el acceso a las instalaciones de procesamiento de información.

7.4.2 Política

a) Requerimientos para el control de accesos:
La Oficina de Tecnologías de la Información del GRU, establece que todos los accesos a los recursos de información deberán basarse en la necesidad y rol del usuario, tomando en cuenta los siguientes aspectos:

- Los requerimientos de seguridad de cada una de las aplicaciones.
- Identificación de toda la información relacionada a las aplicaciones y los riesgos a la que está expuesta.
- Uso de perfiles de usuarios estandarizados definidos según roles.
- Revisión periódica de los controles de acceso. Los propietarios de los activos revisan los derechos de acceso de los usuarios y deben notificar a la Oficina de Tecnologías de la Información sobre cualquier modificación necesaria.
- Revocación de los derechos de acceso.

b) Gestión de acceso del personal:

- Con el propósito de impedir accesos no autorizados a los recursos de información, La Oficina de Tecnologías de la Información del Gobierno Regional de Ucayali, en coordinación con la Oficina de Logística, han establecido el control a través de la distribución de llaves, de acuerdo con listas visadas por las jefaturas de ambas unidades.
- 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 y a las instalaciones de procesamiento de información, comunicando directamente a la Oficina de Tecnologías de la Información del Gobierno Regional de Ucayali y a la Oficina de Logística, respectivamente.
- La Oficina de Tecnologías de la Información del Gobierno Regional de Ucayali, deberá 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.
- La Oficina de Tecnologías de la Información del Gobierno Regional de Ucayali, configura la red de manera que no se compartan identificadores entre diferentes usuarios ni pueda permitirse la duplicidad de sesiones de usuarios.
- La Oficina de Tecnologías de la Información del Gobierno Regional de Ucayali, gestiona la asignación y habilitación o revocación de usuarios del Servicio de Directorio.
- Para los servicios no vinculados al Servicio de Directorio, se registran y cancelan usuarios a través de los paneles de control específicos de administración.
- Es posible asignar accesos a terceros, en este caso se asignan cuentas de usuario genéricas y a solicitud del responsable de la unidad orgánica solicitante.
- Para usuarios privilegiados (administradores), se gestionan cartas de asignación de derechos de acceso, firmado por el director de la Oficina de Tecnologías de la Información.

c) Gestión de usuarios y contraseñas

- La gestión de usuarios y contraseñas harán que el servicio de directorio se proporcione por primera vez al usuario según el siguiente criterio:
  1. En el caso de servidores, la Oficina de Gestión de las Personas remite la lista oficial para el alta de usuarios, tras lo cual la Oficina de Tecnologías de la Información se contacta con los nuevos usuarios a

través de cualquier medio disponible, a fin de proporcionar sus credenciales.

2. En el caso de terceros, el área responsable del servicio debe solicitar a la Oficina de Tecnologías de la Información la creación de las cuentas genéricas necesarias para la prestación, tras lo cual OTI envía las credenciales al área responsable por correo electrónico, las cuales serán reenviadas al tercero.

- Las cuentas de usuarios y contraseñas de sistemas y servicios no vinculados al servicio de directorio deben ser solicitados a la Oficina de Tecnologías de la Información. En este caso las credenciales se entregan al solicitante a través del correo electrónico institucional.
- Las cuentas de usuarios y contraseñas para los repositorios de desarrollo de soluciones informáticas son gestionadas de manera centralizada por un personal asignado de la OTI, quien genera cuentas vinculadas a usuarios institucionales a través de nombres de usuario coincidentes con correos electrónicos asignados y a través de un repositorio local. Las credenciales se entregan a los usuarios autorizados a través del correo electrónico.
- Para el caso de las cuentas gestionadas por el servicio de directorio, los usuarios están obligados a cambiar sus contraseñas de acceso inicial en un plazo no mayor a un mes, para esto se dispone de un servicio web con certificados digitales, desde donde los usuarios pueden cambiar sus contraseñas.
- Las contraseñas almacenadas en bases de datos deben ser cifradas con un patrón criptográfico de mínimo 256 bits.
- 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 personales e intransferibles y el servidor es responsable de mantener su confidencialidad.
- Para el caso de servicios o equipos con administración compartida, el proveedor entregará las credenciales a través de informes de instalación dirigidos a la Oficina de Tecnologías de Información.
- Las reglas de conformación de contraseñas deben estar automatizadas en todos los sistemas donde esto es viable, de modo que los sistemas rechacen contraseñas

débiles. El estándar de conformación de contraseñas se encuentra en el Anexo N° 04 Patron de Contraseñas

d) Control de acceso a las redes informáticas:
- El acceso a los recursos de red, internos y externos debe ser controlado por La Oficina de Tecnologías de la Información del GRU, de manera que el servidor no comprometa la seguridad de los activos de información.
- Para la seguridad en las redes informáticas, se deben tener en cuenta los siguientes aspectos:
  1. Lineamientos de uso de la red.
  2. Para el caso de Segmentación de redes. Se utilizará la segmentación de redes, gestionada por el firewall y del Switch CORE alojado en el Data Center institucional. Cada usuario ingresa al segmento que le ha sido asignado. De necesitar ingresar a un segmento distinto, debe solicitarlo a la Oficina de Tecnologías de la Información, previo VoBo de su jefe inmediato. La justificación de la necesidad debe incluirse en el requerimiento. La Oficina de Tecnologías de la Información del GRU puede denegar el requerimiento si la justificación no guarda relación con el acceso solicitado.
  3. Control de conexiones a redes en base a la política.
  4. Control de enrutamiento de redes.

e) Control de acceso a los sistemas operativos:
- El acceso a los sistemas operativos de las estaciones de trabajo (equipos de cómputo) del Gobierno Regional de Ucayali, debe ser debidamente controlado por la Oficina de Tecnologías de la Información, a fin de evitar accesos no autorizados a recursos o información.
- Dentro de los aspectos que deben ser tomados en consideración para definir los controles, se incluyen:
  1. Identificación automática de estación de trabajo
  2. Inicio de sesión seguro.
  3. Identificación y autenticación de usuarios.
  4. Sistema de gestión de contraseñas.
  5. Restricción del uso de herramientas utilitarias del sistema operativo con capacidades de eludir y/o sobrescribir los controles de seguridad.

f) Control de acceso a las aplicaciones:
- La Oficina de Tecnologías de la Información del Gobierno Regional de Ucayali, controla los accesos a la información y a las aplicaciones del servicio de productividad, restringiendo para uso exclusivo del

personal debidamente autorizado; asimismo, así como de revisar periódicamente los accesos asignados, revocando los derechos cuya vigencia de autorización haya caducado.

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

g) Conexiones externas

Sea cual fuere el caso, para el acceso remoto (todo acceso a la información de la institución fuera del centro de trabajo se deberá utilizar la tecnología y acceso seguro (SSL-VPN) y su uso debe ser autorizado solo en caso de ser necesario por el jefe del órgano o unidad orgánica y la Oficina de Tecnologías de la Información, con el conocimiento del Oficial de Seguridad de la información.

7.5 Política de Seguridad Física y del Entorno

7.5.1 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 respectivamente.

7.5.2 Política

a) Los perímetros de seguridad física deberán ser establecidos en planos de arquitectura. Se ha determinado perímetros externos con paredes de material noble. Asimismo, se han marcado las áreas internas sensibles:
   - Centro de Datos.
   - Nodos de conexión vía Radioenlace.

b) El servidor del Gobierno Regional de Ucayali que atienda a personas externas a la institución (incluyendo suministradores) debe asegurar que los datos de todas las visitas de personas externas a la institución quedarán anotados en el registro de visitas.

c) La Oficina de Tecnologías de la Información del Gobierno Regional de Ucayali, supervisará el uso estricto de las llaves de acceso al Centro de Datos y otras áreas sensibles para su debida protección, a través de una asignación formal de las llaves con listados con firmas de autorización. Adicionalmente se deberá controlar con cámaras de videovigilancia en puntos clave que incluyen las áreas sensibles.

d) La Oficina de Tecnologías de la Información del Gobierno Regional de Ucayali, clasifica a las áreas según su nivel de seguridad y criticidad, estos se describen a continuación:

ÁREA	DESCRIPCIÓN
Común	Son zonas de uso común para el empleado del GRU.
Pública	Son zonas que son de utilización pública y de recepción de personas externas a la entidad.
Restringida o Critico	Son zonas seguras donde la información que se genera transmite, trata o almacena es crítica para la entidad. Los accesos a estos despachos son controlados.

e) Toda persona externa al GRU 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.

f) Cualquier empleado del GRU deberá portar en todo momento su fotocheck para su debida identificación y desplazamiento dentro de la institución.

g) Los visitantes que ingresan a las instalaciones del GRU deberán portar en todo momento su pase de visita.

h) Personal del GRU, deberá cumplir con lo establecido en la Directiva N°0008-2017-GRU-GRPP-SGDI "Uso, Control, Desplazamiento Interno y Externo de Bienes Patrimoniales en las Unidades Ejecutoras y dependencias integrantes del Pliego 462: Gobierno Regional del Departamento de Ucayali" establecido en la institución para el desplazamiento de activos como equipos de cómputo, impresoras y cualquier otro bien que pertenece al parque informático institucional.

i) Todos los equipos de cómputo que ingresan al GRU deberán ser previamente registrados por el personal de vigilancia y seguridad institucional.

j) El GRU a través de los Órganos y Unidades Orgánicas de acuerdo a su responsabilidad deberán de implementar medidas de protección contra amenazas externas y

ambientales, dichas medidas de protección, deberá incluir los siguientes:

- Controles de acceso y seguridad física.
- Detectores de humo.
- Sistemas de puesta tierra.
- Grupo Electrógeno.

k) La Oficina de Tecnologías de la Información del GRU, debe proteger los equipos de Tecnologías de la información de fallas por falta de suministro de energía y otras anomalías eléctricas.

l) La Oficina de Tecnologías de la Información del GRU, debe proteger el cableado de la red de comunicaciones y suministro de energía para evitar intercepción o daño.

m) 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.

n) La Oficina de Tecnologías de la Información del GRU, debe mantener programas de mantenimiento de los equipos de Tecnologías de información.

o) La Oficina de Tecnologías de la Información, deberá mantener programas de mantenimiento de los sistemas de Climatización, Sistemas de Energía Ininterrumpida (UPS), Protección de Fases y demás sistemas y/o servicios disponibles y en ejecución, a fin de garantizar la continuidad de los servicios y de la gestión administrativa diaria.

p) La Oficina de Tecnologías de la Información del GRU, debe implementar una Política de Escritorio Limpio y Pantalla Limpia en cada Equipo de Cómputo instruyendo para ello a cada usuario (empleado) bajo su responsabilidad, a fin de evitar el acceso no autorizado y el uso indebido de la información.

7.6 Política de Seguridad de las Operaciones

7.6.1 Objetivo

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

7.6.2 Política

a) Procedimientos Operativos Documentados:
La Oficina de Tecnologías de la Información y del GRU, deberá documentar procedimientos 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:
- La Oficina de Tecnologías de la Información del GRU, 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.
- Todos los cambios deben ser solicitados a La Oficina de Tecnologías de la Información del GRU, 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 de Tecnologías de la Información del GRU, debe garantizar la capacidad de los recursos a fin de asegurar el desempeño requerido de los Sistemas de información.

d) Separación de Entornos:
- La Oficina de Tecnologías de la Información del GRU, debe separar entornos de desarrollo, pruebas y producción con el fin de prevenir riesgos de acceso no autorizado o cambios al entorno operativo.
- La Oficina de Tecnologías de la Información del GRU, debe venir 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
- La Oficina de Tecnologías de la Información del GRU, 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, teléfonos inteligentes, etc.

- La Oficina de Tecnologías de Información del GRU, debe asegurar que todas las estaciones de trabajo estén protegidas con el antivirus corporativo y que este se encuentre actualizado. Asimismo, debe garantizar que el sistema operativo y los aplicativos de oficina cuenten con las últimas actualizaciones de seguridad (parches).
- La Oficina de Tecnologías de la Información del GRU, 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.
- El Software utilizado por el GRU debe ser autorizado en forma expresa por La Oficina de Tecnologías de la Información.
- El personal de soporte técnico de la Oficina de Tecnologías de la Información del GRU, como medida de prevención, si detecta que alguna estación de trabajo o computadora portátil se encuentra infectada con algún tipo de malware, debe aislarla inmediatamente, desconectándola de la red corporativa.

f) Respaldo de la Información

- La Oficina de Tecnologías de la Información del GRU, 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.
- La Oficina de Tecnologías de la Información del GRU, debe resguardar las copias de seguridad en un ambiente distinto al del origen de la información (es decir, en un local distinto), que reúna las condiciones adecuadas de acondicionamiento, temperatura y humedad.
- La Oficina de Tecnologías de la Información del GRU, debe asegurar que los equipos y los medios de respaldo cuentan con un programa de mantenimiento preventivo y correctivo para asegurar su correcto funcionamiento.
- La Oficina de Tecnologías de la Información del GRU, 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.
- La Oficina de Tecnologías de la Información del GRU, debe de realizar pruebas de restauración a las copias de seguridad con el fin de asegurar que se pueda obtener

correctamente la información almacenada al momento de ser necesaria.

- La Oficina de Tecnologías de la Información del GRU, debe revisar periódicamente la vigencia tecnológica de los equipos y software utilizados para el respaldo y recuperación de la información.
- La Oficina de Tecnologías de la Información del GRU, 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.
- La Oficina de Tecnologías de la Información del GRU, debe de realizar pruebas de restauración a las copias de seguridad con el fin de asegurar que se pueda obtener correctamente la información almacenada al momento de ser necesaria.
- La Oficina de Tecnologías de la Información del GRU, debe revisar periódicamente la vigencia tecnológica de los equipos y software utilizados para el respaldo y recuperación de la información.

g) Registro y Monitoreo

- Todos los servicios informáticos se encuentran sujetos a monitoreo por parte de La Oficina de Tecnologías de la Información del GRU.
- La Oficina de Tecnologías de la Información del GRU, debe generar registros de auditoría sobre el uso de los recursos de Tecnologías de información.
- Las actividades de los operadores y administradores de los sistemas de la Oficina de Tecnologías de la Información del GRU, deben ser monitoreadas, registradas, verificadas regularmente y periódicamente por la Oficina de Tecnologías de la Información.
- La Oficina de Tecnologías de la Información del GRU, debe contar con registro de fallas en los sistemas de información para seguimiento, registros de auditoría y monitoreo pertinente.
- Cada empleado del GRU, será responsable de todas 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 de Tecnologías de la Información del GRU, deberá 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 de Tecnologías de la Información del GRU, deberá implementar mecanismos de restricción para la instalación de software en los equipos de cómputo por parte de los usuarios no autorizados.

j) Controles de Auditoría de los Sistemas de Información
- Todos los servicios informáticos se encuentran sujetos a monitoreo por parte de La Oficina de Tecnologías de la Información.
- La Oficina de Tecnologías de la Información del GRU, debe generar registros de auditoría sobre el uso de los recursos de Tecnologías de información.

7.7 Política de Seguridad de las Comunicaciones

7.7.1 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.

7.7.2 Política

a) La Oficina de Tecnologías de la Información del GRU, 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 de Tecnologías de la Información del GRU, debe realizar la segregación de redes, a fin de garantizar su debida protección.

c) Seguridad de Correo Electrónico
- La Oficina de Tecnologías de la Información del GRU, podrá efectuar el bloqueo de la cuenta de correo electrónico institucional por algún uso indebido que transgrede lo establecido en el presente documento.
- Cada empleado es responsable por la información que se transmita desde la cuenta de correo electrónico que le haya asignado la institución.

- En caso el servidor reciba mensajes con asuntos sospechosos y/o de origen desconocido, estos no deberán ser abiertos y deben comunicarse inmediatamente a la Oficina de Tecnologías de información del GRU, según corresponda, así como al Oficial de Seguridad de la información para los fines correspondientes y luego deben ser eliminados.
- El envío de mensajes masivos de correo electrónico dentro de la institución está permitido solo para el personal o dependencias autorizados por la Alta Dirección del GRU.

d) Acuerdo de Confidencialidad

La Oficina de Tecnologías de la Información del GRU, 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; del mismo modo, se establecen Acuerdos de Confidencialidad y/o de intercambio de información con terceras partes y/o con quienes corresponda.

La Oficina de Tecnologías de la Información del GRU, 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 se determinen.

7.8 Política de Adquisición, Desarrollo y Mantenimiento de Sistemas

7.8.1 Objetivo

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

7.8.2 Política

a) Metodología para la adquisición, desarrollo y mantenimiento de los sistemas:
   - La Oficina de Tecnologías de la Información del GRU, debe aprobar un procedimiento para la adquisición, desarrollo y mantenimiento de los sistemas.
   - Todo desarrollo y/o mantenimiento de sistemas debe ser documentado, con la finalidad de que personas no rutinarias con ellas en el GRU, ejecuten las actividades con facilidad.

b) Requisitos de seguridad de los sistemas

- La Oficina de Tecnologías de la Información del GRU, debe definir un procedimiento que incluya controles de seguridad durante las etapas de análisis y diseño de los sistemas.
- Todo sistema desarrollado por los servidores de la Oficina de Tecnologías de la Información del GRU o por terceros, deberá 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 deberá constar con el respectivo contrato de prestación de servicios.
- El empleado debe cumplir los controles, estándares y metodologías referidas al desarrollo de los sistemas seguros que se hayan implementado.
- La Oficina de Tecnologías de la Información del GRU, 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 GRU.
- Los acuerdos que involucran el acceso, procesamiento, comunicación o manejo de terceros de las instalaciones de procesamiento de información, deberán cubrir los requisitos de seguridad necesarios.
- Todos los sistemas desarrollados por los servidores o empleados de ser el caso, son propiedad del GRU.

c) Procesamiento correcto de los sistemas
- La Oficina de Tecnologías de la Información del GRU, debe implementar controles de seguridad apropiados en los sistemas utilizadas por la institución, para validar los datos de entrada, el procesamiento interno y los datos de salida.
- La Oficina de Tecnologías de la Información del GRU, 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 de Tecnologías de la Información del GRU, deberán implementar los siguientes controles:
- Control de los sistemas en Producción: Comprende la formulación y puesta en marcha de procedimientos orientados a controlar la instalación de los sistemas en producción.

- 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 de Tecnologías de la Información del GRU, controla el acceso al código fuente de las aplicaciones que desarrolla la institución, a través de la asignación de cuentas institucionales para los repositorios utilizados. Estos conservan trazabilidad y registro de los cambios y salidas de código fuente.

f) Uso de controles criptográficos:
La Oficina de Tecnologías de la Información del GRU, debe implementar el uso de controles para cifrar la información y proteger la confidencialidad, autenticidad e integridad de la misma. Se utilizarán certificados digitales de 2048 bits. Las claves criptográficas se gestionarán a través del registro de fechas de activación, renovación y desactivación.

g) Seguridad en los procesos de desarrollo y pase a producción:
- Para el desarrollo de los sistemas: Todo el desarrollo y mantenimiento de los sistemas en el GRU deberán ser realizados conforme a los procedimientos establecidos, debiendo considerarse la NTP ISO/IEC 12207 y otros estándares pertinentes.
- Procedimiento para pase a producción:
  1. Los servidores encargados del desarrollo y mantenimiento de los sistemas, así como los terceros, no tendrán acceso a los datos de producción.
  2. Los ambientes de desarrollo y producción deben ser configurados en servidores diferentes, limitando el acceso solo al personal autorizado.
  3. El pase a producción debe ser realizado exclusivamente por personal autorizado de la Oficina de Tecnologías de la Información del GRU, quien lleva un control de los pases efectuados y/o actualizaciones de los sistemas en un registro o bitácora.
  4. Todo desarrollo, antes de su pase a producción, debe ser revisado por la Oficina de Tecnologías de la Información del GRU, para asegurar que se cumplan los estándares establecidos.

h) Control de cambios de los sistemas

- El control, registro y monitoreo de los cambios de los sistemas del GRU deberá ser supervisado y registrado por la Oficina de Tecnologías de la Información.
- Todo acceso a la librería de los programas fuente debe ser controlado por la Oficina de Tecnologías de la Información del GRU, a fin de evitar accesos y/o cambios no autorizados.

i) Gestión de vulnerabilidades técnicas:
- La Oficina de Tecnologías de la Información del GRU, deberá 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.
- Identificadas las vulnerabilidades técnicas, la Oficina de Tecnologías de la Información del GRU, deberá determinar los riesgos asociados e implementar los controles necesarios para mitigarlos. Los sistemas críticos y en alto riesgo deben ser tratados primero.
- Para los sistemas que requieren una actualización de seguridad (parches), la Oficina de Tecnologías de la Información del GRU, deberá 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.

7.9 Política de Relación con Proveedores

7.9.1 Objetivo

Garantizar la protección de los activos de información del GRU, que son de acceso para los Proveedores.

7.9.2 Política

a) Todo proveedor que brinde servicios al GRU, deberá 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 el GRU, aquellas actividades cubiertas bajo el correspondiente contrato u orden de servicios.

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

d) El proveedor entregará mensualmente, mientras dure la vigencia del contrato, la relación de personas, perfiles,

funciones y responsabilidades asociadas al servicio materia del contrato, e informará 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 al GRU, deberá cumplir con las políticas de seguridad de la información recogidas en el presente documento. En caso de incumplimiento, el GRU se reservará el derecho de solicitar al proveedor el cambio de personal, sin perjuicio del derecho de IGP, 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 GRU y el proveedor se deberá 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 GRU, en ejecución de un contrato u orden de servicios, deberá considerar que dicha información, es confidencial y sujeto a la Ley de Protección de Datos Personales.

h) Ningún proveedor puede utilizar la información del GRU para beneficio propio o de terceros. La información a la que tenga acceso el proveedor únicamente podrá ser utilizada para los fines específicamente indicados en el contrato u orden de servicios, Toda información proporcionada por el GRU, sigue siendo de propiedad de esta última.

i) El proveedor y su personal únicamente puede utilizar la información y activos tecnológicos autorizados por el GRU 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 servicios y para la finalidad exclusiva de facilitar las funciones asociados a dicho contrato. El GRU, se reservará, en función del riesgo identificado, la implementación de medidas de control, registro y auditoría sobre los recursos de difusión.

k) Los recursos que el GRU 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. El GRU se reserva 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 de Tecnologías de la Información del GRU, cualquier incidencia que se detecte y que afecte o pueda afectar a la seguridad de la información de la institución.

7.10 Política de Gestión de Incidentes de Seguridad de la información

7.10.1 Objetivo

Asegurar que los incidentes de seguridad de la información sean comunicados oportunamente a las instancias correspondientes, con la finalidad de adoptar acciones preventivas y correctivas que correspondan.

7.10.2 Política

a) Los incidentes relativos a la seguridad de la información deben ser comunicados a la Oficina de Tecnologías de la Información y al Oficial de Seguridad de la Información, conforme al procedimiento que se establezca para tal efecto.

b) El empleado del GRU deberá 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 empleado del GRU, deberá comunicar al Oficial de Seguridad de la información de la institución, 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 empleado del GRU, deberá 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 de Tecnologías de la Información del GRU, 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 GRU, a efectos que proponga las acciones preventivas que correspondan, en lo sucesivo.

g) Periódicamente, la Oficina de Tecnologías del GRU, deberá analizar las actividades realizadas y estudiar posibles mejoras o cambios que puedan proponerse ante la ocurrencia de futuros incidentes de Seguridad de la información.

7.11 Política de Continuidad de la Seguridad de la información

7.11.1 Objetivo

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

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

7.11.2 Política

a) La Oficina de Tecnologías de la Información del GRU, deberá incluir la continuidad de la seguridad de la información dentro del proceso de gestión de continuidad operativa.

b) La Oficina de Tecnologías de la Información del GRU, deberá verificar los controles de continuidad de seguridad de la información que se han implementado regularmente para asegurar que sean válidos y efectivos.

c) La Oficina de Tecnologías de la Información del GRU, 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 de Tecnologías de la Información del GRU, 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.

7.12 Política de Cumplimiento, Protección y Privacidad de Datos Personales

7.12.1 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 implemente y sea operada de acuerdo con la políticas y procedimientos de la institución.

7.12.2 Política

a) Todos los órganos y unidades orgánicas de GRU, deberán 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 de GRU, deberán 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.

c) Los servidores del GRU, no deberán destruir o eliminar registros o información importante, sin la aprobación respectiva de los propietarios de información.

d) El GRU a través del Gerente de la Oficina Regional de Asesoría Jurídica como oficial de Datos Personales designado de acuerdo a su competencia, deberá garantizar la protección y la privacidad de los datos personales conforme a la legislación aplicable.

VII. DISCPOSICIONES TRANSITORIAS COMPLEMENTARIAS FINALES

- Primero. - El incumplimiento de las disposiciones previstas en la presente Directiva, en la medida que constituyan acciones sancionables conforme al Decreto Legislativo N° 728 - Ley de Productividad y Competitividad Laboral, Decreto Legislativo Nº 1057, que regula el Régimen Especial de Contratación Administrativa de Servicios, Ley Nº 27815 - Ley del Código de Ética y Ley N°30057 - Ley del Servicio Civil, será sancionado conforme lo establecido en dichas normas y sus respectivos reglamentos.

- Segundo. - La Oficina de Tecnologías de la Información, se encargará de velar por el cumplimiento de represente directiva.

- Tercero. -Todo aquello que no se encuentre contemplado en la presente Directiva, será incluido por la OTI en futuras actualizaciones.

VIII. ANEXOS

ANEXO N° 01: Checklist de Configuración de Seguridad de Dispositivos Móviles.

ANEXO N° 02: Uso Aceptable de Activos de Información.

ANEXO N° 03: Eliminación de Medios Removibles.

ANEXO N° 04: Estándar de Contraseñas.

ANEXO N° 01 CHECKLIST DE CONFIGURACIÓN DE SEGURIDAD DE DISPOSITIVOS MÓVILES

N°	DISPOSITIVO MÓVIL	Satisfactorio	No Satisfactorio
1	Autenticación de acceso configurada (contraseña mayor a 4 dígitos y/o biométrica)		
2	Último escaneo de antivirus o aplicación de seguridad del SO no indica acciones pendientes ante amenazas.		
3	No tiene actualizaciones de seguridad pendientes.		
	COMPUTADORAS PORTÁTILES		
4	Antivirus actualizado, licenciado y activado.		
5	Libre de software prohibido por la institución.		
	Teléfono Móviles y Tablets		
6	Contar con la última versión disponible del SO.		
7	Aplicación de seguridad del sistema operativo activada, por ejemplo, Google Play Protect		
8	No se tienen aplicaciones sospechosas, con permisos excesivos.		
	Otros requisitos Ad Hoc		
Acciones tomadas ante requisitos No Satisfechos			
Resultado Final	Aprobado		No Aprobado

ANEXO N° 02 USO ACEPTABLE DE ACTIVOS DE INFORMACIÓN

USO ACEPTABLE
Utilizar los dispositivos institucionales para labores y actividades relacionadas directamente con las funciones del puesto y los objetivos institucionales.
Salvaguardar la información interna y la información confidencial (usuarios y contraseñas, URLs, datos personales, documentos internos, etc.).
Respetar las configuraciones establecidas por los administradores de los sistemas.
Cumplir con las políticas para contraseñas, trabajo remoto, de acceso y otras que emita la institución.
Cuidar la infraestructura física (instalaciones, hardware, elementos de las redes de comunicaciones) de modo que se evite su fallo prematuro.
Notificar a OTIDG ante cualquier dificultad a nivel lógico o físico y seguir las instrucciones que se proporcionan.
USO INACEPTABLE
Realizar copias no autorizadas de información.
Permitir que queden documentos físicos expuestos en el escritorio.
Está prohibido proporcionar datos de usuario/contraseña o facilitar el acceso a los sistemas de la institución a terceros, ya sea deliberadamente o por error; esto incluye anotar las contraseñas en papel, en archivos digitales u otros soportes no autorizados.
Revelar o publicar datos personales de servidores de la institución.
Acceder o intentar acceder a datos, servidores, cuentas para las que no se tiene autorización y/o permiso.
Introducción de códigos maliciosos malware (virus, gusanos, adware, y demás variantes).
Instalar o intentar instalar software no autorizado.
Usar los equipos de cómputo para realizar tareas ajenas a las encargadas por la institución.
Realizar pruebas de seguridad a los sistemas de la institución sin estar autorizado.
El ingreso y utilización NO autorizada de dispositivos de almacenamiento masivo, tales como memorias USB, discos duros portátiles, tarjetas de memoria y similares.
El acceso o intento de acceso a sitios web de mala reputación, sospechosos o potencialmente peligrosos.
Publicar en redes sociales opiniones personales que pueden parecer o confundirse con la posición de la institución.
Envío de SMS, mensajes o correos electrónicos ajenos a las funciones organizacionales de la institución.
Acceder físicamente a zonas o ambientes para los que no se está autorizado.
Acceder a las instalaciones fuera del horario laboral sin tramitar los permisos de autorización respectivo.

No llevar consigo el fotocheck dentro de las instalaciones de la institución
Intentar resolver un problema propio de la competencia de los administradores de los sistemas, esto incluye tratar de acceder a configuraciones de nivel administrador o abrir y manipular elementos de hardware.

ANEXO N° 03 ELIMINACIÓN DE MEDIOS REMOVIBLES

N°	PROCEDIMIENTOS OBLIGATORIOS
01	El personal que realiza la gestión patrimonial entrega el medio a la Oficina de Tecnologías de la Información del GRU.
02	El personal de la Oficina de Tecnologías de la Información del GRU, realiza una revisión y diagnóstico; de concluir que el medio no está operativo, ejecuta lo siguiente:
03	- De ser posible, sobre escribir manualmente el íntegro de la capacidad disponible del medio intervenido. - De ser posible lo anterior, realizar formateo de bajo nivel. - Para discos duros, de no ser viables las iniciativas anteriores por algún daño electrónico o físico interno del disco duro, aplicar la destrucción física, perforando dos agujeros con un taladro directamente sobre los platos del disco (Se recomienda, usar lentes de seguridad para este procedimiento).
04	- Se entrega y se comunica la baja al personal que realiza el control patrimonial de la Oficina de Gestión Patrimonial de la institución.
05	- El personal que realiza el control patrimonial almacena el medio.
06	- El personal que realiza el control patrimonial realiza los trámites para su disposición final.

ANEXO N° 04 PATRÓN DE CONTRASEÑAS

Para asegurar un patrón de contraseñas al momento de crearlos o actualizarlos, se requiere cumplir los siguientes criterios:

1. Longitud mínima:

GRUPO DE USUARIOS	LONGITUD MINIMA DESEADA
Administradores de sistemas y servicios de dominio organizativo.	10 caracteres
Usuarios generales.	8 caracteres

2. Requisitos de complejidad:
   - Restricciones:
     a) No utilizar contraseñas ya utilizadas en cuentas personales.
     b) No utilizar una sola palabra, por ejemplo "campeondelmundo" o una frase conocida como "amigosxsiempre".
     c) No deben ser iguales al nombre de la cuenta del propio usuario.
     d) No deben ser iguales a el/los nombre(s) o apellido(s) del usuario.
     e) No se permitirá el uso de contraseñas clasificadas como contraseñas débiles y fáciles de determinar, como por ejemplo: 12345678, password, contraseña, admin123, yavemos y otras muy conocidas que no garantizar la seguridad de la información.

   - La contraseña debe cumplir con los siguientes criterios de uso de caracteres:

Criterio	Administradores de Sistemas y Servicios de dominio organizativo	Usuarios Generales
AL menos una letra mayúscula.	X	X
Al menos una letra minúscula.	X	X
Dígitos numéricos de base 10 (0-9).	X	X
Caracteres No Alfanuméricos y especiales.	X	

3. El historial de contraseñas se establecerá en 12 para prevenir la reutilización de contraseñas.
4. La vigencia mínima de las contraseñas será de 90 días.
5. La vigencia máxima de las contraseñas será de 360 días.