"LINEAMIENTOS DE POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN DEL GOBIERNO REGIONAL AMAZONAS "

1. OBJETIVOS

Los Lineamientos de Seguridad de la Información tienen como objetivo proteger los recursos de la información del Gobierno Regional Amazonas - GRA. 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.

2. BASE LEGAL

- Ley Nº 27658, Ley Marco de Modernización de la Gestión del Estado.
- Ley Nº 27815, Ley del Código de Ética de la Función Pública.
- Ley Nº 29733, Ley de Protección de Datos Personales.
- Decreto Supremo Nº 109-2012-PCM, que aprueba la Estrategia para la Modernización de la Gestión Pública.
- Resolución Nº 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 Edición", en todas las entidades integrantes del Sistema Nacional de Informática.
- Resolución Ejecutiva Regional Nº 513-2019-GOBIERNO REGIONAL AMAZONAS/ GR, que conforma el Comité de Gobierno Digital del Gobierno Regional Amazonas.

3. ALCANCE

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

4. DEFINICIONES

Activos: Son los bienes que tienen valor para la organización y están constituidos por los siguientes tipos:

- **De Información:** Bases de datos, archivos, contratos, expedientes y acuerdos, documentación de sistema, información de investigación, manuales de usuario, procedimientos operacionales o de soporte, planes de continuidad de operaciones, registros de auditoría, e información de archivo.
- **De Software:** aplicaciones, de sistema, herramientas de desarrollo y utilidades.
- **Físicos:** equipos de cómputo, equipos de comunicaciones, medios removibles y otros.
- **Servicios:** Computacionales y de comunicación, utilidades generales, iluminación especial, energía y aire acondicionado.
- **Personas:** incluyendo sus calificaciones, competencias y experiencia.
- **Intangibles**: como reputación e imagen de la entidad.

Batch: Archivo magnético que tiene almacenado una secuencia de comandos que al ejecutarse reemplaza la operación de digitar los comandos en secuencia cada vez que se requiere efectuar una operación. Se utiliza para almacenar operaciones repetitivas.

Firewall: Dispositivo tecnológico que tiene como función proteger la red interna de una organización de accesos no autorizados del exterior vía Internet.

Red Privada Virtual – VPN: Metodología de conexión por Internet que permite a los usuarios conectarse a la red corporativa utilizando conexiones públicas, a través de canales seguros de comunicación.

Script: Es un archivo que contiene una secuencia de comandos que se utiliza para comunicarse en forma automática entre dos aplicaciones.

Evento de Seguridad de Información: Es una ocurrencia identificada de un sistema, servicio, o red el cual indica una posible brecha de la política de

seguridad de información o fallas de las salvaguardias o una situación desconocida que puede ser relevante para la seguridad.

Incidente de Seguridad de Información: Es indicado por una o varias series de eventos inesperados y no deseados que tienen una gran probabilidad de comprometer las operaciones de la entidad y de amenazar la seguridad de la información

Riesgo: Combinación de la probabilidad de un evento y sus consecuencias.

Tratamiento del Riesgo: Proceso de selección e implementación de medidas para modificar el riesgo.

Amenaza: Causa potencial de un incidente no deseado que puede resultar en daño al sistema u organización

Vulnerabilidad: Debilidad de un activo o grupo de activos que pueden ser explotados por una o más amenazas.

Oficial de Seguridad de la Información: Figura responsable por velar, mantener y administrar la seguridad de los activos de información de la entidad y que se expresa en el documento referido a Responsabilidades de la Gestión de la Seguridad.

5. DOMINIOS DE LA NORMA

Políticas de Seguridad: Constituye el presente documento y es donde se estipulan las políticas con respecto a la seguridad de la Información para el **Gobierno Regional Amazonas**.

Seguridad organizacional: Agrupa los temas de administración de la seguridad dentro de la entidad. (Roles, compromisos, autorizaciones, acuerdos, manejo con terceros)

Administración de Activos de Información: Habla del mantenimiento y protecciones apropiadas de todos los activos de información.

Seguridad del Recurso Humano: Temas para asegurar que todo el personal del GRA (funcionarios, servidores, CAS, locadores de servicios y otros) y demás personas (naturales, jurídicas, consultores, contratistas, u otros) entiendan sus responsabilidades y sean adecuados para los roles a desempeñar minimizando los riesgos relacionados con el recurso humano.

Seguridad Física y Ambiental: Hace referencia a prevenir accesos físicos no autorizados (perímetro), daños o interferencias a las instalaciones de la entidad y a su información.

Administración de Comunicaciones y Operaciones: En este dominio se busca asegurar la correcta y segura operación de las áreas de procesamiento de información (actividades operativas y concernientes a la plataforma tecnológica)

Control y Acceso: Control físico o lógico de los accesos, áreas de procesamiento y procesos de la entidad.

Adquisición, Mantenimiento y Desarrollo de Sistemas de Información: Asegurar la inclusión de todos los controles de seguridad en los sistemas de información (infraestructura, aplicaciones, servicios, etc.)

Administración de Incidentes de Seguridad: Permitir que los eventos de seguridad de la información y las debilidades asociadas con los sistemas de información, sean comunicadas de tal manera que se tome una acción correctiva adecuada en el momento indicado.

Administración de la Continuidad de la Entidad: Enfocado en reaccionar en contra de interrupciones a las actividades de la entidad y en proteger procesos críticos de los efectos de fallas mayores en los sistemas de información o desastres, y asegurar que se resuelvan a tiempo.

Cumplimiento: Busca prevenir el incumplimiento total o parcial de cualquier ley, estatuto, regulación u obligación contractual de los requerimientos de seguridad.

6. ESTRUCTURA DE EVALUACIÓN

6.1. Evaluación de Riesgo de Seguridad

Se fundamenta en el principio de identificación de los procesos organizacionales críticos para el funcionamiento del Gobierno Regional Amazonas, y consiste en la separación e identificación de los activos de información que soportan dichos procesos sobre los cuales se determina un nivel de seguridad correspondiente a lo analizado en el momento de la evaluación.

Del resultado de ese análisis se ha creado y diseñado la presente Política de Seguridad de la Información.

6.2. Tratamientos de Riesgo de Salud

Es una tarea que debe realizarse constantemente actualizando los mapas o niveles de riesgo cada vez que se cumpla un ciclo del SGSI o al presentarse un cambio importante en los sistemas de información críticos.

El Oficial de Seguridad de la Información se encargará de coordinar todas las tareas necesarias para la gestión de riesgos.

7. 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.
- Disponibilidad de la información y los sistemas de información que soportan el GRA para garantizar que les Entidades o personas autorizadas tengan acceso a la información cuando lo quieran.
- Establecer, implementar, mantener y mejorar el sistema de gestión de seguridad de la información del GRA.

8. OBJETIVOS DE CONTROL

8.1. Protección de la Información

Los activos de información serán protegidos con el nivel necesario en proporción a su valor y el riesgo de pérdida para la entidad. La protección debe acentuar la confidencialidad, integridad y disponibilidad de los activos de información.

8.2. Protección de los Recursos Tecnológicos

Los recursos tecnológicos serán protegidos con el nivel necesario en proporción a su valor y el riesgo de pérdida para la entidad. Dichos recursos deben ser utilizados exclusivamente para desarrollar las actividades laborales establecidas para el personal del GRA (funcionarios, servidores, CAS, locadores de servicios y otros) y demás personas (naturales, jurídicas, consultores, contratistas, u otros) asegurando que su utilización se hará en forma adecuada, con el máximo de eficiencia y con ejemplar racionalidad.

8.3. Autorización de usuario

Todos los usuarios deben ser identificados independientemente con permisos de acceso, específicamente e individualmente autorizados por razones básicas de operaciones. Los métodos de acceso de usuarios deben exigir un proceso robusto de autenticación, autorización apropiada y auditoria confiable.

8.4. Responsabilidad

Los usuarios y custodios de los activos de información del **Gobierno Regional Amazonas** son responsables por el uso apropiado, protección y privacidad de estos activos. Los sistemas informáticos del **Gobierno Regional Amazonas** generarán y

mantendrán unas apropiadas pistas de auditoría para identificar usuarios, y documentar los eventos relacionados con eventos de seguridad.

8.5. Disponibilidad

Los activos de información deben estar disponibles para soportar los objetivos del **Gobierno Regional Amazonas.** Deben tomarse medidas adecuadas para asegurar el tiempo de recuperación de toda la información y el acceso por personas autorizadas.

8.6. Integridad

Los activos de información deben estar adecuadamente protegidos para asegurar su integridad y precisión. Las medidas de validación definidas permitirán detectar la modificación inapropiada, eliminación o adulteración de los activos de información.

8.7. Confidencialidad

Los activos de información deben mantenerse protegidos para asegurar su confidencialidad entre los usuarios autorizados para acceder a los mismos. En todo momento deben mantenerse los esquemas de seguridad que prevengan la divulgación no autorizada de información.

8.8. Confianza

Todo el personal del GRA (funcionarios, servidores, CAS, locadores de servicios y otros) y demás personas (naturales, jurídicas, consultores, contratistas, u otros) deben demostrar capacidad para acceder los requerimientos de seguridad del Gobierno Regional Amazonas y justificar la confianza en sus capacidades para asegurar los activos de información de la entidad. La confianza empieza a ser incrementalmente importante cuando los activos son compartidos con otras personas.

8.9. Esfuerzo de Equipo

Para que logre ser efectiva, la seguridad de la información debe ser un esfuerzo de equipo donde deben participar en forma activa todo el personal del GRA. (funcionarios, servidores, CAS, locadores de servicios y otros) y demás personas (naturales, jurídicas, consultores, contratistas u otros) que tengan interacción con la información o los sistemas de información de la entidad. Todos deben cumplir

con las políticas de seguridad de información y más que eso, desempeñar un papel proactivo para su protección y divulgación de estas políticas.

8.10. Soporte Primario para la Seguridad de la Información

El Oficial de Seguridad de la Información debe facilitar la administración y desarrollo de iniciativas sobre seguridad de información. El Oficial de Seguridad de la Información deberá proveer dirección y experiencia técnica para asegurar que la información del Gobierno Regional Amazonas se encuentre protegida apropiadamente. Esto incluye considerar la confidencialidad, la integridad y la disponibilidad de la información y de los recursos informáticos que la soportan.

Los usuarios son responsables de familiarizarse y cumplir con las políticas de seguridad de la información; las dudas que puedan surgir alrededor de éstas deben ser consultadas al Oficial de Seguridad de la Información de la entidad.

8.11. Revisión de Seguridad en Sistemas de información

En forma periódica el Gobierno Regional Amazonas debe efectuar las pruebas necesarias para evaluar el cumplimiento de las diferentes políticas de seguridad, lo mismo que para verificar el cumplimiento de los estándares de configuración en las diferentes plataformas técnicas e instalaciones de tecnología de información. Esta tarea será realizada por el Oficial de Seguridad de la Información y el responsable de la Unidad de Tecnología de la Información.

La información que es soportada por la infraestructura de tecnología informática del Gobierno Regional Amazonas 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.

La información propiedad del Gobierno Regional Amazonas y sobre la cual tiene sus derechos, podrá ser suministrada a los entes de control pertinentes, cuando estos lo requieran, con previa autorización expresa por los jefes inmediatos.

Para efectos de control del flujo de la información de los procesos de la entidad, se asignarán responsables de la información, quienes deben asegurar y otorgar acceso a la información que genere su área, con el fin de lograr un adecuado ambiente de control y un buen nivel de segregación de funciones.

En caso de divulgación no autorizada de la información de propiedad del Gobierno Regional Amazonas, se realizarán las investigaciones pertinentes para establecer

sanciones, las cuales serán evaluadas con el jefe inmediato del usuario involucrado y el Comité de Seguridad para lo cual utilizarán el concepto emitido por el Oficial de Seguridad de la Información sobre el hecho y su impacto en la entidad.

9. POLÍTICAS

Estas Políticas cuentan con el apoyo de un Sistema de Gestión de Seguridad de la Información (SGSI), integrado entre otros, por normas, procedimientos y formatos los cuales están en constante revisión y actualización por cada ciclo del SGSI.

9.1. Políticas de seguridad

La Política de Seguridad de la Información (expresada en este documento) especifica las pautas que deben ser cumplidas por parte de todo el personal del GRA (funcionarios, servidores, CAS, locadores de servicios y otros) y demás personas (naturales, jurídicas, consultores, contratistas, temporales o terceras partes u otros), con el fin de asegurar un adecuado nivel de confidencialidad, integridad y disponibilidad en su información.

9.2. Aspectos Organizacionales de la Seguridad

9.2.1. Oficial de Seguridad de la Información

El Gobierno Regional Amazonas mantendrá dentro de su organización un Oficial de Seguridad de la Información, cuyas funciones estarán caracterizadas y definidas según la necesidad de nuestra institución.

9.2.2. Comité de seguridad

Se establece el Comité de Seguridad, como ente de la entidad para atender los temas en materia de Seguridad de la Información que requieran de una definición o aprobación. Además, este Comité debe conocer y aprobar los planes de Seguridad de la Información. Cuando el Comité de Seguridad se reúna con el propósito de revisar temas de seguridad de la información se incluirá la participación de la Unidad de Tecnología de la Información.

9.2.3. Coordinación de Seguridad

El Gobierno Regional Amazonas deberá contar con un Oficial de Seguridad de la Información que asuma las tareas y responsabilidades que conlleva este rol, y que se expresan en el documento referido a Responsabilidades de la Gestión de la Seguridad.

9.2.4. Seguridad con Terceros

a) Todas las conexiones a la red interna del Gobierno Regional Amazonas, de las personas que trabajan en el GRA, cual quieras sea su condición laboral deben ser autorizadas, revisadas y monitoreadas por la Unidad de Tecnología de la Información, según sus requerimientos

b) Además, los contratos para los cuales se transfiere la responsabilidad por la seguridad de la información a un tercero deben dejar en forma explícita el compromiso por parte de este, de la aplicación de los controles de seguridad necesarios en la medida en que el Gobierno Regional Amazonas le haya transferido dicha responsabilidad

9.2.5. Acuerdos de Seguridad

Todo el personal del GRA. (funcionarios, servidores, CAS, locadores de servicios y otros) y personas (naturales, jurídicas, consultores, contratistas, u otros) que deban realizar labores dentro de la entidad, cuya labor involucre el manejo de información de la entidad ya sea por medios lógicos o físicos; deben conocer, entender, firmar y aceptar el correspondiente acuerdo de confidencialidad que para su caso aplique y que se expresa en los documentos: Acuerdo de Confidencialidad y usos de TI (para personal del GRA) y el Acuerdo de Confidencialidad - Terceros (para las otras personas).

Todas estas personas están obligadas a continuar protegiendo la información del Gobierno Regional Amazonas cumpliendo las políticas de seguridad después de terminar su relación con la entidad.

9.2.6. Responsabilidad por la Información

a) Cada conjunto de datos tendrá un usuario dueño y responsable de los datos que están en producción. Donde se entiende por dueño de la información al usuario que trabaja con la información y como responsable de la información al director del área donde ésta se genera

b) Es responsabilidad de la Unidad de Tecnología de la Información, mantener segura la información sistematizada de la entidad

9.2.7. Segregación de Funciones

El Gobierno Regional Amazonas debe asegurar que los procesos se desarrollen a través de una correcta segregación de funciones que permita garantizar que la ejecución, la revisión, la autorización y el seguimiento se den a diferentes niveles

9.3. Clasificación y control de activos

9.3.1. Inventarios de Activos

a) El Gobierno Regional Amazonas mantendrá todos sus activos de información referenciados e inventariados y constantemente actualizará

b) Toda adquisición de cualquier naturaleza que haga la entidad en materia de hardware, software y servicios en temas informáticos e información, debe tener un control a través de la Unidad de Tecnología de la Información.

c) Se debe realizar un control de todo hardware y software que sea recibido, así como de su ubicación y protección, desde que se adquieren o arriendan, hasta su retiro de uso.

9.3.2. Clasificación de Información

a) Cada activo de información propiedad del Gobierno Regional Amazonas, debe estar asignado a un personal de la entidad (funcionarios, servidores, CAS, locadores de servicios y otros) quien se responsabilizará por el mismo.

b) Toda la información utilizada por el Gobierno Regional Amazonas y su personal (funcionarios, servidores, CAS, locadores de servicios y otros), debe ser clasificada y administrada de acuerdo a los niveles establecidos por la entidad y que se expresan en el documento referido a la Clasificación de la Información.

9.4. Seguridad en Recursos Humanos

9.4.1. Responsabilidad de los usuarios

a) Todo personal nuevo del GRA. (funcionarios, servidores, CAS, locadores de servicios y otros), que hayan aprobado los procesos de selección, deberán conocer, entender y asumir sus responsabilidades con respecto a la seguridad de la información, según el rol a desempeñar. Igualmente es responsabilidad de todo personal vinculado a la entidad con anterioridad a la elaboración de este documento, conocer, entender y asumir sus responsabilidades con respecto a la seguridad de la información, según el rol a desempeñar

b) El incumplimiento de esta Política de Seguridad de la Información así como las normas, procedimientos y formatos que regulan el SGSI que

conlleve a un incidente de seguridad, implicará un proceso disciplinario y/o las acciones legales correspondientes, dentro del marco legal vigente, por parte de la entidad para establecer la responsabilidad del usuario involucrado. El término del contrato de trabajo con el Gobierno Regional Amazonas, implica el cumplimiento de los procesos de entrega de activos de información y remoción de privilegios sobre la plataforma tecnológica de la entidad.

c) Todos los usuarios deben conocer y dar cumplimiento de la normatividad de uso de la tecnología (uso del correo, uso de las impresoras, navegación en Internet, etc.) establecido por la Unidad de Tecnología de la Información del GRA.

9.4.2. Entrenamiento

Todo el personal del GRA. (funcionarios, servidores, CAS, locadores de servicios y otros) será entrenado en los temas de seguridad necesarios para asegurar que se cumpla el esquema de seguridad, evitando su incumplimiento debido a falta de capacitación o desconocimiento del SGSI.

9.5. Seguridad física del Entorno

9.5.1. Controles de Acceso Perimetral

a) Todo el personal del GRA. (funcionarios, servidores, CAS, locadores de serv1c1os y otros) deberán portar constantemente y en un lado visible su fotocheck que lo identifica como personal de la entidad.

b) Todas las demás personas (naturales, jurídicas, consultores, contratistas, temporales o terceras partes u otros) que hagan su ingreso a las instalaciones de la entidad deberán estar adecuadamente identificadas y anunciar su llegada a través del personal de vigilancia de las instalaciones. Cualquier elemento que entre o salga de las diferentes unidades orgánicas debe ser anunciado al personal de vigilancia para que este proceda a hacer el registro correspondiente.

c) Las puertas de acceso a las áreas de manipulación o administración de información confidencial o privada, deberán permanecer cerradas en todo momento.

d) Para el ingreso o salida de cualquier elemento deberá diligenciarse el formato de autorización que tiene establecida la entidad con el registro completo de la información que allí se solicita.

e) Todas las personas que ingresen a las áreas restringidas de la entidad, deberán cumplir los controles establecidos para el acceso específico a dichas áreas

9.5.2. Controles Ambientales

El Gobierno Regional Amazonas, proporcionará el ambiente adecuado para la conservación de medios magnéticos y equipos.

a) El Gobierno Regional Amazonas, grabará en video las actividades en áreas públicas, puertas de acceso a áreas restringidas y zonas de manipulación de información confidencial o privada, con el fin de mantener un control de seguridad.

b) Gobierno Regional Amazonas, mantendrá en condiciones óptimas de limpieza, seguridad, mantenimiento y funcionalidad de cada uno de los elementos que forman parte del centro de cómputo y para el resguardo de los backups de la información, de acuerdo con las recomendaciones que sobre cada uno provea el fabricante.

c) Todo el personal del GRA. (funcionarios, servidores, CAS, locadores de servicios y otros) que utilice estaciones de trabajo para la realización de su labor, deberán acoger como práctica permanente el bloqueo de la pantalla al ausentarse de su puesto, así como mantener en orden sus papeles de trabajo, siempre pensando en la confidencialidad de la información.

d) Las estaciones de trabajo de los usuarios finales serán desactivadas automáticamente si superan un tiempo de inactividad determinada en cada caso, según el nivel de riesgo que corresponda, siendo necesario digitar nuevamente la clave de acceso en el momento que requiera continuar con la conexión.

9.5.3. Mantenimiento

Gobierno Regional Amazonas, establecerá esquemas de mantenimiento para toda su plataforma tecnológica que deberá ser cumplido dentro de las fechas programadas.

Cuando un medio magnético, propiedad del Gobierno Regional Amazonas, termine su ciclo de vida, deberá ser destruido de acuerdo a las exigencias de la Unidad de Tecnología de la Información.

Al disponer de un disco duro utilizado, ya sea para su entrega o reutilización, deberá pasar por un proceso adecuado de borrado determinado por la Unidad de Tecnología de la Información.

9.5.4. Cintoteca

La entidad contará con una cintoteca adecuada y segura para la custodia de la información.

La Cintoteca deberá cumplir con la normatividad relacionada a seguridad de áreas de procesamiento de datos (áreas restringidas)

9.5.5. Centro de Computo

La Unidad de Tecnología de la Información debe establecer los mecanismos de seguridad necesarios para la correcta protección del Centro de Datos (o centro de cómputo), de manera que se mantenga la confidencialidad y seguridad de la información que se procesa, así como la integridad de los equipos.

Gobierno Regional Amazonas, mantendrá las condiciones físicas y ambientales óptimas recomendadas para centros de cómputo, así como controles automáticos para incendio y temperatura {humedad, monitoreo por el CCTV, etc)

9.5.6. Área Restringida

Gobierno Regional Amazonas, clasificará sitios (áreas) que por su actividad, activos, manejo transaccional, etc., se deban manejar en forma restringida teniendo controles de acceso y registro de visitantes. Se consideran dentro de éstas, por ejemplo: El centro de cómputo y el gabinete de comunicaciones.

9.6. Gestión de Comunicaciones y Operaciones

9.6.1. Documentación Operativa

a) Todos los procedimientos operativos del Gobierno Regional Amazonas, estarán adecuadamente documentados, mantenidos y a disposición de los usuarios a quienes compete.
b) Es responsabilidad de la Unidad de Tecnología de la Información, mantener debidamente actualizada toda la documentación referente a la plataforma tecnológica de la entidad.

9.6.2. Control de Cambios

Cualquier cambio a la plataforma tecnológica del Gobierno Regional Amazonas, (a excepción de las estaciones de trabajo) deberá ser completamente documentado y controlado por la Unidad de Tecnología de la Información.

Cualquier cambio en la plataforma de las estaciones de trabajo deberá ser autorizado por la Unidad de Tecnología de la Información.

Cualquier cambio realizado a las aplicaciones desarrolladas para la operación normal del Gobierno Regional Amazonas, deberá ser completamente documentado y sus versiones controladas según los requerimientos establecidos por la Unidad de Tecnología de la Información.

Todos los cambios en el ambiente de producción deberán ceñirse a las regulaciones establecidas para la adecuada puesta en producción, por la Unidad de Tecnología de la Información.

9.6.3. Uso de la Tecnología

a) La Unidad de Tecnología de la Información definirá los criterios de utilización de los servicios de tecnología y los estándares adecuados para la óptima administración de los recursos.
b) Los recursos informáticos del Gobierno Regional Amazonas deben ser utilizados únicamente para propósitos propios de la entidad.

9.6.4. Acceso Remoto

La entidad proporcionará tecnologías de acceso remoto al personal del GRA (funcionarios, servidores, CAS, locadores de servicios y otros), previa evaluación y autorización del área correspondiente. La Unidad de Tecnología de la Información garantizará un adecuado esquema de seguridad para los mismos.

9.6.5. Separación de Ambientes

Gobierno Regional Amazonas, mantendrá identificados, controlados y aislados sus ambientes de desarrollo, calidad y producción, aplicando para cada uno los procedimientos específicamente estipulados por la entidad, para su operación o administración.

9.6.6. Capacidad de desempeño

La plataforma tecnológica del Gobierno Regional Amazonas, será continuamente monitoreada con el fin de establecer niveles de capacidad y

desempeño, empleando las herramientas adecuadas y manteniendo actualizada la debida documentación.

9.6.7. Servicio de Red

a) El Gobierno Regional Amazonas, mantendrá un constante monitoreo sobre la red interna, implementando las herramientas que le permitan detectar, prevenir y recuperarse del código malicioso encontrado en su plataforma tecnológica.

b) El Gobierno Regional Amazonas, se reserva el derecho de examinar toda la información almacenada o transmitida por sus sistemas de cómputo y de comunicación y debe informar a todo el personal del GRA. (funcionarios, servidores, CAS, locadores de servicios y ot ros) y demás personas (naturales, jurídicas, consultores, contratistas, u otros) que no deben esperar privacidad asociada con la información que ellos almacenan o envían a través de estos sistemas.

c) La entidad mantendrá actualizada y con la debida aprobación de la Unidad de Tecnología de la Información, una lista de las categorías de acceso NO permitido para la navegación en Internet. En todas las ocasiones los intereses, el buen nombre y la seguridad de la entidad deben ser protegidos por todo el personal del GRA (funcionarios, servidores, CAS, locadores de servicios y otros) y demás personas (naturales, jurídicas, consultores, contratistas, u otros) que presentan servicios a la entidad.

9.6.8. Servicios Web

La entidad vigilará el cumplimiento de los compromisos de seguridad de la página www.regionamazonas.gob.pe, a través de la revisión periódica de los informes de vulnerabilidad entregados a la entidad.

9.6.9. Software

La entidad efectuará constantes revisiones al cumplimiento de las normas en materia de propiedad intelectual. Todo el personal del GRA. (funcionarios, servidores, CAS, locadores de servicios y otros) y demás personas (naturales, jurídicas, consultores, contratistas u otros) tienen PROHIBIDO instalar o utilizar software o productos sin licencias autorizadas por la entidad. Se exceptúan de esta política los productos de software con licencia de libre utilización o que sean soportados con certificado de propiedad de licencia de

terceros. En todo caso, cualquier instalación de software debe ser solicitada y obtenida a través de la Unidad de Tecnología de la Información.

9.6.10. Computación Móvil

a) Los equipos de cómputo (sin importar su propietario) utilizados fuera del Gobierno Regional Amazonas y en funciones propias de la entidad, deben ser exclusivamente utilizados para brindar apoyo a las actividades de la entidad y deben ser sujetos a un grado equivalente de protección igual al de los equipos que se encuentran dentro de las instalaciones del Gobierno Regional Amazonas. Se deben aplicar las siguientes pautas:

   El uso de equipos portátiles asignados al personal del GRA. (funcionarios, servidores, CAS, locadores de servicios y otros) deben atenerse a todas las recomendaciones de seguridad y, adicionalmente, deberán seguir las instrucciones emitidas por la Unidad de Tecnología de la Información.

   Las computadoras personales, para conectarse a la red del GRA., previamente deben pasar por una verificación y autorización por parte de la Unidad de Tecnología de la Información.

   Durante los viajes, los equipos y medios magnéticos no deben dejarse desatendidos en lugares públicos. Las computadoras portátiles se deben llevar como equipaje de mano.

   Los equipos portátiles son vulnerables al robo, pérdida o acceso no autorizado durante los viajes. Se les deben proporcionar una forma apropiada de protección al acceso (Ej. Contraseñas de encendido, encriptación, etc.) con el fin de prevenir el acceso no autorizado.

   Las instrucciones del fabricante concernientes a la protección del equipo se deben seguir en todo momento (Ej.: para protegerse contra la exposición de campos electromagnéticos muy fuertes).

b) La utilización de elementos removibles de almacenamiento (DVD's, memorias USB, CD's reescribibles, discos duros portátiles, etc.) por parte de los usuarios, deberá cumplir estrictamente los lineamientos establecidos por la Unidad de Tecnología de la Información mediante pautas recomendadas por parte del Oficial de Seguridad de la Información. La administración (custodia, reutilización y destrucción) adecuada de estos elementos, tanto para su conservación como la

destrucción, cuando fuera necesario, estará determinada por los procedimientos establecidos en la Unidad de Tecnología de la Información.

c) El ingreso y/o salida de los equipos de cómputo y elementos removibles de almacenamiento (DVD's, memorias USB, CD's reescribibles, discos duros portátiles, etc.), que SI pertenecen al GRA., deberá ser previamente autorizado por la Unidad de Tecnología de la Información y registrado por la Unidad de Logística y el Personal de Seguridad.

d) El ingreso y/o salida de los equipos de cómputo y elementos removibles de almacenamiento (DVD's, memorias USB, CD's reescribibles, discos duros portátiles, etc.) que NO pertenecen al GRA, deberá ser previamente autorizado por la Unidad de Tecnología de la Información y registrado por el Personal de Seguridad.

9.6.11. Backups

a) Toda la información del Gobierno Regional Amazonas, debe ser respaldada por medio de copias de seguridad siguiendo el procedimiento adecuado según el componente. Esto incluye la información de las estaciones de trabajo que cada responsable de área considere necesario, previa coordinación con el responsable de la Unidad de Tecnología de la Información para incluirlos en el procedimiento de backup.

b) Es responsabilidad de cada personal del GRA (funcionarios, servidores, CAS, locadores de servicios y otros) ubicar en una unidad de red la información referida únicamente al Gobierno Regional Amazonas que requiera ser respaldada por la Unidad de Tecnología de la Información.

c) Es responsabilidad de la Unidad de Tecnología de la Información, mantener en buen funcionamiento los sistemas que le permitan prevenir, detectar y corregir ingresos o intentos de ingresos no autorizados.

9.6.12. Revisión y Monitoreo de Logs

El Gobierno Regional Amazonas, realizará un monitoreo permanente de la red a través de los diferentes logs establecidos y configurados a conveniencia de la entidad. Estos logs serán revisados y analizados de acuerdo a las tareas programadas dentro de la Unidad de Tecnología de la Información.

9.6.13. Responsabilidad Operativa

a) Dentro del personal de la Unidad de Tecnología de la Información debe existir un responsable de la seguridad de los backups.

b) Gobierno Regional Amazonas, a través de la Unidad de Tecnología de la Información se responsabilizará de la seguridad de la información en los equipos centrales de cómputo, quien adoptará las mejores prácticas en materia de control de acceso a la información de acuerdo a la tecnología usada.

c) Gobierno Regional Amazonas, a través de la Unidad de Tecnología de la Información, asegurará la mejor selección (técnica) de los proveedores de servicios, para los elementos y equipos que forman parte del centro de cómputo.

d) Es responsabilidad de la Unidad de Tecnología de la Información brindar la información al ente regulador de la entidad sobre las actividades de desarrollo y mantenimiento de los aplicativos, y es potestativo del ente de control su participación en los grupos de trabajo.

9.6.14. Telefonía

La entidad contará con el servicio telefónico local, nacional y de celulares según la autorización dada a través de la Ley de Presupuesto, para los demás se utilizar el uso de manera particular a todo el personal del GRA.

9.6.15. Administración de Usuarios

a) Las cuentas que no hayan sido utilizadas en los últimos noventa días deben ser eliminadas o inhabilitadas dependiendo del caso.

b) Está prohibido intentar ingresar a los servicios de cómputo y comunicaciones con la cuenta de otro personal del GRA (funcionarios, servidores, CAS, locadores de servicios u otros.

c) La Unidad de Tecnología de la Información del Gobierno Regional Amazonas, definirá el esquema de usuarios para la administración y uso de cada plataforma tecnológica, utilizando los criterios de mínimo riesgo e impacto para la entidad.

d) El nivel de acceso debe ser definido por funciones específicas dentro de cada aplicación y para cada usuario.

e) Cada personal del GRA. tendrá un código único de identificación ante el sistema y será responsable de todo registro a su nombre.

f) La creación, eliminación y revisión de privilegios de los usuarios de la red y las aplicaciones del Gobierno Regional Amazonas, deberán ser regularmente revisados según las actividades programadas de la Unidad de Tecnología de la Información.

g) El Gobierno Regional Amazonas clasificará las cuentas de usuario de acuerdo a los niveles de acceso autorizados y requeridos para la operación o administración de los sistemas de la entidad.

h) Las unidades correspondientes deberán enviar mensualmente a la Unidad de Tecnología de la Información, la lista actualizada de altas, bajas, vacaciones, incapacidades, licencias, consultorías, servicios, etc. de todo el personal del GRA. a fin de llevar un control de las cuentas de usuario correspondientes según sea el caso.

9.6.16. Contraseñas

a) Cada personal del GRA. (funcionarios, servidores, CAS, locadores de servicios y otros) debe tener asociada una contraseña que cumpla con las características de contraseñas seguras referida en el documento de Administración de Contraseñas de Usuarios, documentos que debe ser administrado por la Unidad de Tecnología de Información

b) El Gobierno Regional Amazonas, mantendrá definido para todos sus sistemas de información un esquema de construcción de contraseñas fuertes que debe ser cumplida por todo el personal del GRA.

c) Las contraseñas deberán permanecer enmascaradas en todos los medios tecnológicos en los cuales son digitadas.

d) Es responsabilidad directa del personal del GRA. (funcionarios, servidores, CAS, locadores de servicios y otros), velar por la confidencialidad y buen uso de su contraseña.

e) No se deben almacenar contraseñas en formato legible en archivos tipo "batch", scripts de logon automáticos, macros de software, teclas de función de terminales, computadores sin control de acceso, archivos de texto o en sitios donde personas no autorizadas puedan descubrirlos y utilizarlos.

9.6.17. Controles de Acceso de Red

a) Ninguna persona que labore en la Unidad de Tecnología de la Información tendrá acceso a los datos en producción, en modalidad diferente a la de consulta, a excepción del Administrador de la Base de

Datos o cuando se realice por expresa solicitud y autorización del responsable de la Unidad de Tecnología de la Información.

b) El personal del GRA. (funcionarios, servidores, CAS, locadores de servicios y otros) no tendrán acceso de escritura a los datos de producción por fuera de los sistemas de información, a excepción del Administrador de Base de Datos.

c) Es responsabilidad de la Unidad de Tecnología de la Información contar con los mecanismos que permitan definir los atributos de acceso definidos por el usuario dueño de los datos.

d) La Unidad de Tecnología de la Información garantizará a la entidad que el personal del GRA; reportadas como ausentes por motivo de vacaciones, incapacidades, licencias, término del servicio, etc., no podrá tener acceso a la red interna de la institución, salvo que se justifique y se realice por expresa solicitud y autorización del responsable de la Unidad de Tecnología de la Información.

e) La Unidad de Tecnología de la Información contará con personas responsables de la seguridad de acceso a los datos, de acuerdo a sus funciones en las diferentes plataformas.

f) Para cubrir eventualidades causadas por ausencia imprevista (incapacidades y fuerza mayor) del personal del GRA, que tiene a cargo operaciones críticas, se recurrirá a mantener creados pero inhabilitados, usuarios de Backup que permitan en forma rápida restaurar el servicio afectado. El Oficial de Seguridad de la Información revisará en forma periódica la utilización de estos perfiles.

9.6.18. Controles de Acceso a Aplicaciones

Las aplicaciones incluirán un adecuado control de acceso basado en el análisis de las funciones que la aplicación tiene desarrolladas y las autorizaciones por grupos de usuarios, roles y perfiles.

9.7. Adquisición, Desarrollo y Mantenimiento de Sistemas

9.7.1. Requerimientos de Seguridad

a) Las nuevas aplicaciones que se pondrán en operación en la entidad deben cumplir los requerimientos de seguridad mínimos establecidos para asegurar confidencialidad, integridad y disponibilidad en la información que manejan.

b) La Unidad de Tecnología de la Información es responsable de mantener a disposición de la entidad la infraestructura tecnológica más conveniente de acuerdo a sus requerimientos y lo que ofrece el mercado.

9.7.2. Datos para Pruebas

Gobierno Regional Amazonas, mantendrá por separado sus ambientes de producción, desarrollo y calidad, y en cada uno de ellos mantendrá únicamente los elementos que se consideren adecuados con el fin de mitigar los riesgos.

Es responsabilidad de la Unidad de Tecnología de la Información asegurar que los datos dispuestos para la realización de calidad y desarrollo cuenten con la debida protección para minimizar los riesgos con respecto a la confidencialidad.

9.7.3. Análisis de Vulnerabilidad

Es responsabilidad de la Unidad de Tecnología de la Información mantener un esquema de pruebas de vulnerabilidad a los componentes de la red dependiendo del análisis de riesgos.

9.7.4. Administración de Sistemas de Información

Gobierno Regional Amazonas, deberá cumplir el esquema general de ciclo de vida de los proyectos, de acuerdo a la metodología basada en la NTP 12207, que para el efecto elaboró la Unidad de Tecnología de la Información, esto es tanto para el mantenimiento de aplicaciones en producción, calidad o desarrollos nuevos.

9.7.5. Cifrado

En los medios y transmisiones electrónicas que el Gobierno Regional Amazonas, determine, se deberán mantener esquemas de cifrado que cumplan los requerimientos específicos establecidos para tal fin. Para esto creará una política específica que regule el uso de dicho esquema.

9.8. Gestión de Incidentes de Seguridad

9.8.1. Reporte de Incidentes y Eventos de Seguridad

a) Todo el personal del GRA (funcionarios, servidores, CAS, locadores de servicios y otros) debe reportar cualquier incidente de seguridad que detecte, al Oficial de Seguridad de la Información lo antes posible.

b) El alcance fundamental es que cualquier personal del GRA. (funcionarios, servidores, CAS, locadores de servicios y otros) pueda identificar, clasificar y reportar de manera sencilla los incidentes de seguridad, manteniendo abierta la posibilidad de reportar los

incidentes en forma oportuna, de tal forma que siempre haya habilitado por lo menos un mecanismo de reporte.

c) Todos estos incidentes y eventos de seguridad serán monitoreados y cuantificados a través del Sistema de Gestión de la Seguridad de la Información (SGSI), el cual al ser un sistema cíclico recibe información de los incidentes y eventos sucedidos ayudando a identificar cuáles son los que más se repiten o de gran impacto para la entidad; logrando que el sistema mejore constantemente, implementando controles más avanzados o adicionales, y así limitar la frecuencia, daño y costos de ocurrencias futuras.

9.8.2. Administración de Incidentes de Seguridad

El Oficial de Seguridad de la Información debe realizar el debido estudio y seguimiento de todos los incidentes de seguridad, valiéndose de la asistencia de todos los usuarios involucrados cuando éste lo requiera. Es responsabilidad del Oficial de Seguridad de la Información mantener actualizadas las estadísticas de mantenimiento de emergencia, clasificadas en técnicas y de usuario, siendo éstas reportadas mensualmente al responsable de la Unidad de Tecnología de la Información.

9.9. Administración de la Continuidad de Operaciones

9.9.1. Planeación del Plan de Continuidad de Operaciones

El Gobierno Regional Amazonas, diseñará y mantendrá vigente un Plan de Continuidad de Operaciones que atienda los requerimientos de Seguridad de la Información en la entidad según el análisis de riesgos determinado para tal fin, el cual deberá estar catalogado por niveles (1,2,3) de acuerdo con el grado de contingencia que se deba atender, por ejemplo: Grado 1, contingencias menores que se atienden con el personal dentro de las instalaciones. Grado 2, que no se permita el ingreso al edificio, grado 3, por desastre

9.9.2. Mantenimiento del Plan de Continuidad de Operaciones

La entidad realizará pruebas periódicas y mantenimiento al Plan de Continuidad de Operaciones por lo menos UNA vez en el año.

La entidad contará con un contrato de custodia externa de la información, como parte del plan de continuidad de operaciones.

9.10. Cumplimiento

9.10.1. Protección Legal

El Gobierno Regional Amazonas, conserva el derecho de retirar de los sistemas de información cualquier material que pueda ser considerado ofensivo o potencialmente ilegal.

9.10.2. Normatividad

Es responsabilidad del dueño de la información, definir los periodos de retención y la frecuencia de los Backups que garanticen el cumplimiento legal y los propios.

Las políticas de seguridad de la información del Gobierno Regional Amazonas, fueron diseñadas para ajustarse o exceder, sin contravenir, las medidas de protección establecidas en las leyes y regulaciones; si el personal del GRA. considera que alguna política de seguridad de la información está en conflicto con las leyes y regulaciones

existentes lo debe reportar en forma inmediata al Oficial de Seguridad de la Información de la información.

10. SANCIONES POR INCUMPLIMIENTO

El GRA, se reserva el derecho de tomar medidas administrativas disciplinarias de los trabajadores 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.