COMPENDIO DE POLÍTICAS COMPLEMENTARIAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

UNIDAD
DE RESTITUCIÓN
DE TIERRAS

Bogotá, julio de 2025

Clasificación de la Información: Publica ☒ Reservada ☐ Clasificada ☐ **Fecha de aprobación**: 2/07/2025

TABLA DE CONTENIDO

INTRODUCCIÓN

La Unidad Administrativa Especial de Gestión de Restitución de Tierras Despojadas (UAEGRTD) desempeña un papel crucial en la administración del proceso de restitución de tierras para las víctimas del despojo. Dada la naturaleza sensible de la información que maneja, relacionada con los derechos fundamentales de la población afectada por el desplazamiento forzado, la UAEGRTD ha implementado un Sistema de Gestión de Seguridad de la Información (SGSI).

Este SGSI, alineado con el Modelo de Seguridad y Privacidad de la Información (MSPI) y el Marco de Referencia de Arquitectura TI, generando un pilar fundamental de la Política de Gobierno Digital, con el objetivo primordial de salvaguardar la seguridad, integridad y confiabilidad de los datos que la entidad gestiona.

Las políticas y directrices que rigen este sistema se fundamentan en el MSPI, el Sistema de Gestión de Seguridad y Privacidad de la Información (SGSPI), la norma ISO/IEC 27001:2013, la Ley 1581 de 2012 de Protección de Datos Personales y la Ley 1712 de 2014 de Transparencia y Acceso a la Información Pública y Reservada, entre otras normativas adoptadas por la entidad.

A través de la implementación y mejora continua del SGSI, la UAEGRTD busca fortalecer su relación con los ciudadanos, usuarios y grupos de interés, promoviendo un uso seguro y confiable de las tecnologías de la información. El Compendio de Políticas Complementarias de Seguridad y Privacidad de la Información establece las responsabilidades y objetivos para la protección adecuada de los activos de información de la entidad, con el fin de mitigar el riesgo de divulgación, modificación, destrucción o uso indebido de dichos activos. Al mismo tiempo, estas políticas fortalecen el subsistema de Gestión de Seguridad de la Información, orientando y mejorando la administración de la seguridad de los activos y proporcionando las bases para el monitoreo en toda la UAEGRTD.

1 POLITICA DE SEGURIDAD DE LA INFORMACION

La Política de Seguridad de la Información hace parte del Sistema Integrado de Planeación y Gestión (SIPG), la cual debe garantizar el aseguramiento de la confidencialidad, integridad y disponibilidad de la información en la UAEGRTD y sus partes interesadas a través del establecimiento y mejora de la seguridad digital, la gestión de riesgos de seguridad de la información de acuerdo con lo dispuesto en la Política Nacional de Seguridad Digital y el Modelo de Seguridad y Privacidad de la Información.

La Política de Seguridad de la Información es la declaración general que representa la posición de la UAEGRTD, de incorporar la Seguridad y Privacidad de la Información en las perspectivas misional y de apoyo con sus respectivos procesos, identificando sus activos de información críticos, así como la protección de los datos personales, en cumplimiento de las disposiciones legales y gubernamentales, con miras a fortalecer la confianza ciudadana.

2 OBJETIVO

Establecer los lineamientos institucionales definidos por la Unidad Administrativa Especial de Gestión de Restitución de Tierras Despojadas (UAEGRTD), para la seguridad de la información, teniendo en cuenta el Modelo de Seguridad y Privacidad de la Información (MSPI), las políticas de Seguridad Digital, Gobierno Digital y demás requisitos basados en el ciclo PHVA (Planear, Hacer, Verificar y Actuar) y de acuerdo con la norma NTC, ISO/IEC27001:2013, así como, los demás requerimientos legales, normativos, técnicos y reglamentarios.

2.1 Objetivos Específicos

La presente política de seguridad de la información está orientada al cumplimiento de los siguientes objetivos específicos:

- Proteger la información de la UAEGRTD y de los ciudadanos que acceden a los servicios de la entidad salvaguardando su confidencialidad, integridad, disponibilidad a través del establecimiento de lineamientos que mitiguen los riesgos que vulneren los activos de información.
- Generar confianza en los ciudadanos, colaboradores y demás partes interesadas en el uso de los servicios de la UAEGRTD.
- Gestionar y mitigar los riesgos que se puedan presentar para proteger los activos de información de la UAEGRTD contra ataques, robo, intrusiones, accesos no autorizados y fuga de información, que afecten a la imagen, los intereses y el buen nombre de la UAEGRTD.
- Establecer las responsabilidades y obligaciones de seguridad de la información en la UAEGRTD.
- Mantener un nivel apropiado de concientización, conocimientos y habilidades necesarios para permitirles minimizar la ocurrencia de incidentes de seguridad de la información.
- Garantizar la continuidad de la Entidad frente a la ocurrencia de incidentes de seguridad de la información y eventos disruptivos.
- Definir las directrices basadas en el marco regulatorio y políticas vigentes.

2.2 Alcance / Aplicabilidad

Los lineamientos contenidos en la política de seguridad de la información y las políticas complementarias aplican para todos los procesos identificados en la entidad (estratégicos, misionales, apoyo y evaluación) que son soportados en todas las dependencias de la entidad y demás escenarios donde se desarrollen actividades de la UAEGRTD, incluidas la gestión con proveedores y terceras partes interesadas.

Adicionalmente, aplica a toda la información creada, procesada, custodiada y respaldada al interior de Unidad que hace parte de los diferentes procesos, sin importar el medio, formato, presentación o lugar en el cual se encuentre. Incluye la almacenada en bases de datos, computadores, dispositivos de almacenamiento masivo, entre otros:

- Respaldada en centros de datos.
- Almacenada en la nube Pública o Privada.
- Transmitida a través de redes públicas o privadas.
- Impresa o escrita a mano en papel o en tableros u otro medio semejante.
- Enviada por Scanner/fax o por cualquier otro medio similar.
- Archivo físico.
- Información grabada a través de los diferentes medios de comunicación y vigilancia.

Asimismo, cuenta con la declaración de aplicabilidad donde se especifica la pertinencia de implementar los controles de la Norma ISO 27001:2013, los cuales se encuentran en la declaracion de aplicabilidad.

Su aplicabilidad se hace extensiva a todos los usuarios internos y externos de la Unidad Administrativa Especial de Gestión de Restitución de Tierras Despojadas (UAEGRTD), funcionarios y/o contratistas, grupos de valor y partes interesadas, entidades del estado, entes de control y otros terceros que desempeñen alguna actividad en la Entidad.

3 TERMINOS Y DEFINICIONES

Activo de Información: Elementos de hardware y de software de procesamiento, almacenamiento y comunicaciones, bases de datos y procesos, procedimientos y recursos humanos asociados con el manejo de los datos y la información misional de la Unidad Administrativa Especial de Gestión de Restitución de Tierras Despojadas.

Acuerdo de Confidencialidad: Es el documento que suscriben los servidores públicos, contratistas, de la UAEGRTD, con el fin de afianzar su compromiso con la entidad respecto del uso pertinente de los recursos informáticos y de la información que la entidad dispone y que les entrega, o a la cual tiene acceso con ocasión al cumplimiento de sus funciones u obligaciones.

Acuerdo de Intercambio de Información: Es un contrato por medio del cual las partes se comprometen a intercambiar información y a no revelar la información de carácter confidencial que les es suministrada, en el cual se comprometen a custodiar, asegurar y a eliminar cuando se concluyan los términos del acuerdo de intercambio de información.

Acuerdo de Niveles de Servicio (ANS): Es un acuerdo escrito entre un proveedor de servicio y su cliente con objeto de fijar el nivel acordado para la calidad de dicho servicio. El ANS es una herramienta que ayuda a ambas partes a llegar a un consenso en términos del nivel de calidad del servicio, en aspectos tales como tiempo de respuesta, disponibilidad horaria, documentación disponible, usuario asignado al servicio.

Alta Disponibilidad: Característica de un sistema o servicio que permite reducir al mínimo el tiempo de indisponibilidad en caso de fallo o incidente; es decir, el tiempo en el que no estará accesible. Este nivel de funcionamiento (o el tiempo máximo de caída) ha de ser acordado entre el proveedor y el cliente en el caso de un servicio, en el marco de un Acuerdo de Nivel de Servicio.

Ambiente de Prueba: Es un sitio (servidores, URLs, computadores, etc.) donde se alojan las aplicaciones o servicios para que sean probadas (la mayoría de los usuarios aún no tiene acceso), previo a que sean publicados en ambiente de producción (donde todos los usuarios si tienen acceso).

Ambiente de Desarrollo: Es un sitio (servidores, URLs, computadores, etc.) que se usa para desarrollar o construir el software de un programa, aplicación o servicio tecnológico (generalmente se usan lenguajes de programación, librerías, frameworks, base de datos, entre otros).

Anonimización: Proceso de transformar datos de forma irreversible para que no puedan ser asociados con una persona identificada o identificable. Una vez anonimizados, los datos no pueden vincularse de nuevo a su titular original, incluso con información adicional, garantizando así la privacidad total.

Autenticación: Acción mediante la cual demostramos a otra persona o sistema que somos quien realmente decimos que somos, mediante un documento, una contraseña, rasgo biológico, etc.

BIA: Abreviatura de Business Impact Analysis. Se trata de un informe que nos muestra el coste ocasionado por la interrupción de los procesos críticos de negocio. Este informe nos permitirá asignar una criticidad a los procesos de negocio, definir los objetivos de recuperación y determinar un tiempo de recuperación a cada uno de ellos. (ISO 22301)

Cadena de Custodia: Es un conjunto de medidas que deben tomarse para proteger la identidad e integridad de un elemento o muestra que puede ser fuente de prueba de un posible hecho delictivo para asegurar su adecuada validez procesal. La cadena de custodia incluye la ubicación y el movimiento de la evidencia física o digital desde que se descubrió o se movió de la escena del incidente hasta que se presentó ante el juez1

Confidencialidad: Es la propiedad de la información, por la que se garantiza que está accesible únicamente a personal autorizado a acceder a dicha información. La confidencialidad de la información constituye la piedra angular de la seguridad de la información; Junto con la integridad y la disponibilidad suponen las tres dimensiones de la seguridad de la información.

Control de Acceso: Es un proceso mediante el cual los usuarios obtienen acceso y ciertos privilegios de los sistemas, recursos o información.

Criptografía: Es el proceso de convertir texto sin formato ordinario en texto ininteligible y viceversa. Es un método para almacenar y transmitir datos en una forma particular para que solo aquellos a quienes está destinado puedan leerlos y procesarlos.

Custodio de la Información: Es el funcionario o contratista encargado de administrar el activo de información, aplicar las políticas, procedimientos y protocolos definidos por la Entidad y por el dueño del Activo de Información.

Derecho de Autor: “Son los derechos de los creadores sobre creaciones intelectuales, como obras literarias,

artísticas y científicas. Las obras que se prestan a la protección por derecho de autor van desde los libros, la música, la pintura, la escultura y las películas hasta los programas informáticos, las bases de datos, los anuncios publicitarios, los mapas y los dibujos técnicos".

Denegación de Servicio: Ataque a un sistema, aplicación o dispositivo para dejarlo fuera de servicio debido a una saturación de peticiones. También llamado DoS.

Disponibilidad: Se refiere a la capacidad de un usuario para acceder a información o recursos en una ubicación específica y en el formato correcto.

Dispositivos Móviles: También conocidos como computadora de bolsillo o computadora de mano, con capacidades de procesamiento, con conexión a Internet, con memoria y pantalla. Se dividen en: Portátiles, Teléfonos inteligentes y Tabletas.

Ethical Hacking: Es el proceso de identificar y explotar las debilidades existentes en los sistemas de información e infraestructura tecnológica, haciendo pruebas de intrusión, que sirven para verificar y evaluar la seguridad física y lógica de los diferentes activos de información ejecutadas por parte de personas autorizadas por la entidad.

Firma Digital: Es un valor numérico que se adhiere a un mensaje de datos y que, utilizando un procedimiento matemático conocido, vinculado a la clave del iniciador y al texto del mensaje permite determinar que este valor se ha obtenido exclusivamente con la clave del iniciador y que el mensaje inicial no ha sido modificado después de efectuada la transformación.

Firma Electrónica: se refiere a métodos tales como, códigos, contraseñas, datos biométricos, o claves criptográficas privadas, que permite identificar a una persona, en relación con un mensaje de datos, siempre y cuando el mismo sea confiable y apropiado respecto de los fines para los que se utiliza la firma, atendidas todas las circunstancias del caso, así como cualquier acuerdo pertinente.

Gestión de Cambios: Es el proceso que reúne un conjunto de prácticas y procesos que ayudan al equipo a enfrentar las transformaciones que puedan ocurrir en la entidad. Esto permite que la oficina o dependencia de TI sustituya tecnologías desactualizadas por soluciones más eficaces o actualizadas.

Gestión de Proyectos: Es administrar, planificar, coordinar, seguir y controlar todas las actividades y los recursos asignados para un proyecto de una forma que se pueda cumplir con el alcance en el tiempo establecido y con los costos presupuestados.

Gobernanza: Son los procesos, procedimientos y prácticas a través de los cuales se toman las decisiones y se regulan las acciones de la Unidad, con el objetivo de dirigirla y asegurar el cumplimiento de objetivos y responsabilidades

IDS: Un sistema de detección de intrusos (o IDS de sus siglas en inglés Intrusion Detection System) es una aplicación usada para detectar accesos no autorizados a un computador, sistema de información o a una red. Estos accesos pueden ser ataques realizados por usuarios malintencionados con conocimientos de seguridad o usando herramientas automáticas. A diferencia de los IPS, estos sistemas sólo detectan intentos de acceso y no tratan de prevenir su ocurrencia.

Información Pública: Es toda información que un sujeto obligado genere, obtenga, adquiera, o controle en su calidad de tal.

Información Pública Reservada: Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de la ley 1712 de 2014.

Información Pública Clasificada: Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias o los derechos particulares o privados consagrados en el artículo 6 de la ley 1712 de 2014.

Integridad: Se refiere a la exactitud y consistencia generales de los datos o expresado de otra forma, como la ausencia de alteración cuando se realice cualquier tipo de operación con los datos, lo que significa que los

datos permanecen intactos y sin cambios.

Mejores Prácticas: Es una técnica o metodología que, a través de la experiencia y la investigación, ha demostrado llevar de forma fiable a un resultado deseado. Es un compromiso de utilizar todos los conocimientos y la tecnología a disposición de uno para asegurar el éxito.

Privacidad: Derecho de las personas y usuarios a proteger sus datos en Internet, además de controlar el acceso a los mismos y decidir qué información es visible para el resto de los actores.

Seudonimización: Es una técnica que consiste en reemplazar los identificadores directos de una persona (como su nombre) por seudónimos o valores artificiales. Esto permite usar los datos sin identificar directamente a la persona, pero conservando la posibilidad de revertir el proceso si se tiene acceso a la información adicional que vincula los seudónimos con la identidad original.

4 PRINCIPIOS DE LA POLITICA

Para dar cumplimiento a la política de Seguridad y Privacidad de la Información se establecen los siguientes elementos para su alcance:

- Fortalecer la cultura de seguridad de la información en los funcionarios y/o contratistas, grupos de valor y partes interesadas de la Entidad.
- Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.
- Minimizar el riesgo de todos los procesos de la entidad.
- Mejorar continuamente el Modelo de Seguridad y Privacidad de la Información.
- Implementar los controles tecnológicos necesarios para la protección de los activos de la entidad y para la reducción de los riesgos.
- Cumplir con los principios de seguridad de la información.
- Cumplir con los principios de la función administrativa
- Mantener la confianza de sus grupos de valor y partes interesadas.
- Proteger los activos tecnológicos y de información.
- Garantizar la continuidad del servicio frente a incidentes.
- Apoyar la innovación tecnológica.

4.1 Compromiso de la Alta Dirección

La Alta Dirección del La Unidad Administrativa Especial de Gestión de Restitución de Tierras Despojadas (UAEGRTD) se compromete a apoyar y liderar la implementación, mantenimiento y mejora del Modelo de Seguridad y Privacidad de la Información MSPI; revisar el avance y garantiza los recursos suficientes (tecnológicos y talento humano calificado), para lograr los objetivos misionales relativos al MSPI. Igualmente, UAEGRTD, reconoce la importancia de la seguridad de la información para el cumplimiento de su misión institucional y la protección de los derechos de los ciudadanos. En este sentido, se compromete a:

- Asume la responsabilidad de impulsar y guiar la implementación del MSPI, asignándole la prioridad necesaria para garantizar su éxito.
- Se compromete a realizar revisiones periódicas del progreso en la implementación del Modelo de Seguridad y Privacidad de la Información (MSPI), evaluando los resultados obtenidos y tomando las medidas correctivas necesarias para garantizar el cumplimiento de los objetivos establecidos.
- Asignar los recursos suficientes (tecnológicos y talento humano calificado) para el logro de los objetivos misionales relativos al MSPI.
- Fomentar una cultura de seguridad de la información entre los colaboradores de la UAEGRTD.
- Reconoce que la seguridad de la información es una responsabilidad de todos los servidores públicos y contratistas de la entidad, fortaleciéndola a través de campañas de sensibilización, capacitación y formación.
- Cumplir con los requerimientos legales, normativos, técnicos y reglamentarios aplicables en materia de seguridad de la información.
- Establecer un marco de confianza en el ejercicio misional de cara a los ciudadanos.

- Reconoce que la protección de la información es fundamental para mantener la confianza de los ciudadanos en la entidad.

4.2 Roles y Responsabilidades

La Unidad Administrativa Especial de Gestión de Restitución de Tierras Despojadas (UAEGRTD), define los roles y responsabilidades para la implementación del Modelo de Seguridad y Privacidad de la Información y el cumplimiento de los lineamientos de seguridad descritos en esta política y los demás documentos derivados como; manuales, procedimientos, formatos y guías.

Roles / Responsabilidades	Descripción
Comité Institucional de Gestión y Desempeño	Órgano rector, articulador y ejecutor, a nivel institucional, de las acciones y estrategias para la correcta implementación, operación, desarrollo, evaluación y seguimiento del Modelo Integrado de Planeación y Gestión el cual contiene la Política de Seguridad Digital. De acuerdo con el numeral 6 del Artículo 2 de la Resolución No. 544 del 2024, que señala las funciones del Comité Institucional de Gestión y Desempeño, le corresponde asegurar la implementación y desarrollo de las políticas de gestión y directrices en materia de seguridad digital y de información.
Subcomité de Gestión Digital	• Orienta las gestiones correspondientes al cumplimiento de la Política de Seguridad Digital.
Oficina Tecnologías de la Información - Seguridad y Privacidad de la Información	• Líder del Subsistema de Gestión de Seguridad de la Información (SGSI) quien es el Jefe de la Oficina de Tecnologías de la Información y genera las estrategias para la gestión de la seguridad de la información en la UAEGRTD. • Oficial de Seguridad de la Información, quien planifica, desarrolla, controla y gestiona las políticas, procedimientos y acciones con el fin de mejorar la seguridad de la información dentro de sus pilares fundamentales de confidencialidad, integridad y disponibilidad. • Profesional de seguridad de la información, a cargo de mantener y gestionar los servicios relacionados con la seguridad de la información.
Lideres de los subdominios de TI	▪ Gestionan y mantienes los servicios de TI relacionados con la información, los sistemas de información y los servicios tecnológicos. ▪ Uso y Apropiación, encargado de apoyar el plan de capacitación y sensibilización de seguridad de la información que incluye el diseño y divulgación de piezas gráficas y capacitaciones.
Oficina de Control Interno	▪ Realizar la auditoria al Sistema de Gestión de Seguridad de la Información. ▪ Apoyar en situaciones de posibles violaciones a las políticas de seguridad de la información.
Grupo de Gestión Contratación	▪ Verificar e implementar las medidas de seguridad de la información en la gestión con los proveedores y contratistas de la entidad. ▪ Procurar la protección de la seguridad de la información de todos los activos de la información que puedan verse involucrados en procesos o contratos.
Grupo de Gestión de Talento Humana	▪ Verificar e implementar las medidas de seguridad de la información en la gestión con el talento humano de la entidad. ▪ Procurar la protección de la seguridad de la información de todos los activos de la información que puedan verse involucrados en los procesos de Talento Humano.
Grupo de Gestión Documental	▪ Establecer y aplicar políticas y procedimientos para la creación, recepción, organización, acceso, uso, conservación y disposición final de los documentos, garantizando su confidencialidad, integridad y disponibilidad, tanto físicos como digitales, a lo largo de su ciclo de vida.
Grupo de Gestión de Seguimiento y Operación Administrativa	▪ Proteger los activos físicos lo que incluye implementar controles de acceso, vigilancia, protección contra incendios, desastres naturales y gestión del acceso de personal y visitantes a las instalaciones.
Oficina Asesora de Planeación	▪ Realiza seguimiento al cumplimiento del plan de comunicación de Seguridad de la Información.
Servidores Públicos, Contratistas y Partes Interesadas	▪ Propietarios y/o custodios de activos de información, lideres de procesos o sus representantes, encargados del tratamiento y/o custodia. ▪ Cumplir a cabalidad con las políticas y procedimientos de seguridad de la información definidos y aprobados, que utilizan la información procesada y suministrada por la UAEGRTD para el desarrollo de sus actividades.

4.3 Aprobación de la Política

Esta política estará vigente, después de su aprobación por el Comité institucional de Gestión y desempeño y su publicación, Según la Resolución No. 544 del 2024.

4.4 Sanciones

Todos los servidores públicos, contratistas, grupos de valor y partes interesada de la Unidad Administrativa Especial de Gestión de Restitución de Tierras Despojadas (UAEGRTD), son responsables de dar cumplimiento a la presente política; el incumplimiento traerá consigo, las consecuencias administrativas, disciplinarias y legales que apliquen, incluyendo lo establecido en la normatividad a nivel Nacional, en cuanto a la seguridad y privacidad de la Información se refiere.

4.5 Seguimiento

En la UAEGRTD, se llevarán a cabo revisiones periódicas del Modelo de Seguridad y Privacidad de la Información (MSPI), en coordinación con la Mesa del Sistema Integrado de Planeación y Gestión (SIPG), con el fin de garantizar la mejora continua y la adaptación a los cambios en el entorno y las necesidades de la Entidad.

4.6 Lineamientos y Políticas de Seguridad y Privacidad de la Información

La UAEGRTD a través de la Oficina Tecnologías de la Información OTI, implementara los siguientes controles definidos en el Anexo A de la norma ISO 27001:2013, estructurados según los 14 dominios.

- Políticas de Seguridad de la Información
- Organización de la Seguridad de la Información
- Seguridad relativa en los Recursos Humanos
- Gestión de Activos
- Control de Accesos
- Criptografía
- Seguridad física y del entorno
- Seguridad Operaciones
- Seguridad de Comunicaciones
- Adquisición, desarrollo y mantenimiento de los sistemas de Información
- Relación con proveedores
- Gestión de Incidentes de seguridad de la información
- Aspectos de seguridad de la información para la gestión de la continuidad del negocio
- Cumplimiento

5 POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

5.1 Directrices de Gestión de la Seguridad de la Información

Objetivo: Proporcionar orientación y apoyo de la Dirección para la seguridad de la información, de acuerdo con los requisitos de la Unidad y con las regulaciones y leyes pertinentes.

5.1.1 Políticas para la Seguridad de la Información

La Oficina Tecnologías de la Información OTI, adelantará las acciones para:

a. Emitir las políticas y lineamientos relacionados con la Seguridad y Privacidad de la Información en el campo de los datos y la información.
b. Establecer y revisar anualmente las políticas y lineamientos de seguridad y privacidad de la información, adaptándolos a las necesidades de la Unidad.
c. Someter dichas políticas y lineamientos al Comité Institucional de Gestión y Desempeño para su aprobación.
d. Gestionar la publicación de las políticas y lineamientos para garantizar el acceso a la información por parte de la ciudadanía.

5.1.2 Revisión de las Políticas Para la Seguridad de la Información

La Oficina Tecnologías de la Información OTI y la Oficina Asesora de Planeación, adelantarán las acciones para la revisión de las políticas de seguridad de la información, asegurando su adaptación constante a las necesidades y cambios del entorno, ya sea mediante revisiones planificadas o ante eventos significativos.

6 ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

6.1 Organización Interna

Objetivo: Establecer un marco de gestión para iniciar y controlar la implementación y la operación de la seguridad de la información dentro de la Unidad.

6.1.1 Roles y Responsabilidades en Seguridad de la Información

La Oficina Tecnologías de la Información OTI, adelantará las acciones para:

a. Implementar y gestionar el Modelo de Seguridad y Privacidad de la Información en la Unidad.
b. Generar, roles y responsabilidades, en seguridad y privacidad de la información.
c. Revisar y actualizar la matriz de roles y responsabilidades de seguridad y privacidad de la información, mínimo una vez al año o cada vez que se requiera.
d. Dar a conocer a los funcionarios y terceros de la UAEGRTD, el Modelo de Seguridad y Privacidad de la Información establecido en la Unidad.
e. Efectuar el monitoreo al grado de implementación del Modelo de Seguridad y Privacidad de la Información.

Los jefes de las dependencias adelantarán las acciones para:

a. Aplicar y cumplir los controles sobre los activos de información sobre los cuales son responsables, con el objeto de mitigar el riesgo de indisponibilidad, pérdida de confidencialidad y pérdida de integridad de la información.
b. Identificar y evaluar los riesgos de seguridad de la información, implementando y haciendo seguimiento a los planes de tratamiento y mitigación de estos riesgos.

6.1.2 Segregación de Tareas

La UAEGRTD establece la segregación de tareas como un principio fundamental para proteger la confidencialidad, integridad y disponibilidad de la información. es así como está comprometida en implementar la división de responsabilidades y la asignación de tareas críticas a diferentes individuos, asegurando que ninguna persona tenga el control total sobre un proceso o transacción sensible.

El propósito principal de esta política es evitar el acceso no autorizado, la modificación indebida de datos y la comisión de fraudes o errores. Para lo cual se implementarán controles que aseguren que las funciones

incompatibles estén separadas, minimizando así el riesgo de que una sola persona pueda comprometer los activos de información de la Unidad.

Los dueños y custodios de la información en las diferentes dependencias de la Unidad, con el apoyo de la Oficina Tecnologías de la Información OTI, ejercerán un control periódico para que ninguna persona externa, servidor público y/o contratista, pueda acceder a funciones incompatibles y modifique activos de información sin la debida autorización.

6.1.3 Contacto Con Las Autoridades

La Oficina Tecnologías de la Información OTI, adelantará las acciones para:

a. Garantizar que se mantenga una comunicación permanente con las autoridades pertinentes para estar informados sobre las tendencias de amenazas en temas de seguridad de la información y ciberseguridad.
b. Crear procedimientos, guías e instructivos que permitan especificar cuándo y a través de que escenarios se deben contactar las autoridades para informar la materialización de un incidente de seguridad de la información.

6.1.4 Contacto Con Grupos de Interés Especial

La Oficina de Tecnologías de la Información (OTI) o el responsable de la Seguridad de la Información establecerán y mantendrán una comunicación activa con grupos especializados en seguridad y privacidad de la información. Este contacto estratégico permitirá obtener recomendaciones y asesoramiento oportuno ante la ocurrencia de incidentes que puedan comprometer la confidencialidad, integridad y disponibilidad de los activos de información de la Unidad, fortaleciendo así la capacidad de respuesta y mitigación de riesgos.

6.1.5 Seguridad de la Información en Proyectos

La Oficina Tecnologías de la Información OTI y Proyectos o quien haga sus veces, adelantarán las acciones para:

a. Determinar la criticidad de la información que se utilizará en el proyecto, teniendo como base la clasificación de los activos de información.
b. Definir en el proyecto, el tiempo que la información será utilizada, los periodos de conservación de la información y la accesibilidad a la información por parte de los funcionarios y terceros de la entidad.
c. Incluir la privacidad de la información y los datos personales en el análisis de riesgos, previo al proyecto.
d. Gestionar los respectivos acuerdos de confidencialidad y de entrega de información según la normatividad vigente en la entidad.
e. Implementar las mejores prácticas relacionadas con el desarrollo seguro y pruebas de penetración para gestionar desde el inicio las debilidades de seguridad en los proyectos que incluyan desarrollo de sistemas de información.
f. Determinar si en el proyecto van a participar terceros y si aplica gestionar las cláusulas de cumplimiento según las normas aplicables, la autorización de tratamiento de datos, la cláusula de confidencialidad de la información y de aceptación de las políticas de seguridad.
g. Evaluar, tratar y hacer seguimiento a los riesgos de seguridad de la información y datos personales asociados a los proyectos, durante todo el ciclo de vida del proyecto (al inicio, durante la ejecución y al finalizar).

El responsable de la Seguridad de la Información acompañara en las actividades de definición de riesgos para cada uno de los proyectos que gestionan esta dependencia.

6.2 Los Dispositivos Móviles y el Teletrabajo

Objetivo: Garantizar la seguridad de la información que se accede, procesa o almacena utilizando dispositivos móviles y en ubicaciones de teletrabajo. Lo que incluye la implementación de controles que protejan la información contra accesos no autorizados, pérdidas, daños o divulgaciones indebidas, manteniendo la confidencialidad, integridad y disponibilidad de los activos de información de la Unidad cuando se utilizan dispositivos móviles y el teletrabajo.

6.2.1 Política de Dispositivos Móviles

A través de esta política, la UAEGRTD establece las directrices necesarias para asegurar la protección de la información sensible y crítica que puede ser accedida y procesada a través de dispositivos móviles y durante la práctica del teletrabajo, siguiendo las recomendaciones dispuestas en el Modelo de Seguridad y Privacidad de la Información (MSPI) de MinTIC y lineamientos de la norma ISO 27001.

6.2.2 Uso Aceptable de Dispositivos Móviles

a. Todos los dispositivos móviles que se utilicen para acceder a información de la UAEGRTD deben ser aprobados por la OTI y cumplir con los estándares de seguridad establecidos.
b. Todos los dispositivos móviles que accedan a la información de la UAEGRTD deben hacerlo a través de un sistema de autenticación fuerte.
c. Las credenciales de acceso son personales e intransferibles. Está prohibido compartir contraseñas o cualquier método de acceso.

6.2.3 Teletrabajo Seguro

a. Los colaboradores (funcionarios / contratistas) deben seguir los procedimientos establecidos por la UAEGRTD para garantizar la seguridad de la información durante el teletrabajo.
b. La información sensible, tanto en tránsito como en reposo en todos los dispositivos móviles utilizados para el teletrabajo debe estar cifrada.
c. Los colaboradores (funcionarios / contratistas) garantizarán que el entorno de trabajo remoto sea seguro y deben evitar conversación sobre temas sensibles en lugares públicos.
d. Los colaboradores (funcionarios / contratistas) asegurarán los dispositivos móviles y cualquier documento físico que contenga información confidencial o reservada de la UAEGRTD.
e. Todo incidente de seguridad relacionado con dispositivos móviles o teletrabajo debe ser reportado inmediatamente al equipo de seguridad de la información a través de la Mesa de Servicio.
f. Para todos los incidentes reportados se llevará a cabo una investigación adecuada y se implementarán las medidas correctivas necesarias.
g. Todos los acuerdos de teletrabajo deben ser revisados y aprobados por Talento Humano e incluirán obligaciones de seguridad de la información.

7 SEGURIDAD DEL RECURSOS HUMANO

7.1 Antes del Trabajo

Objetivo: Asegurar que los funcionarios y contratistas comprenden sus responsabilidades y son idóneos en los roles para los que se consideran.

7.1.1 Selección de Personal

La UAEGRTD a través Oficina Talento Humano y/o Contratación, adelantará las acciones para:

a. Llevar a cabo una verificación de antecedentes adecuados, previa a la contratación de colaboradores (funcionarios / contratistas), que incluya la validación de referencias laborales y verificación de credenciales, conforme a la normatividad vigente.
b. Todos los candidatos potenciales (funcionarios / contratistas), recibirán información sobre la importancia de la seguridad de la información y las políticas de la UAEGRTD durante el proceso de selección.

7.1.2 Durante la Relación Contractual

Todos los colaboradores (funcionarios / contratistas) deben suscribir un Acuerdo de Confidencialidad el cual respalda su responsabilidad y compromiso frente a la no divulgación de información confidencial (clasificada y reservada) que conozca y /o tenga acceso en la UAEGRTD como parte del ejercicio de sus funciones.

7.2 Durante el Empleo

Objetivo: Asegurarse de que los funcionarios y contratistas tomen conciencia de sus responsabilidades de seguridad de la información y las -cumplan.

7.2.1 Responsabilidad de Gestión

a. La UAEGRTD comunica claramente los roles y responsabilidades en cuanto a la gestión de la seguridad de la información para asegurar que todos los empleados comprenden su papel en proteger los activos de información.
b. Las responsabilidades relacionadas con la seguridad de la información están documentadas en las descripciones de trabajo (estudios previos) y manuales de procedimientos, asegurando que son accesibles para todos los colaboradores (funcionarios / contratistas).

7.2.2 Concienciación, Educación y Capacitación en Seguridad de la Información

a. La UAEGRTD proporcionará formación continua sobre seguridad de la información a todos los colaboradores (funcionarios / contratistas) y terceros con acceso a la información sensible. Esta formación será impartida al inicio de la relación (laboral/contractual) y periódicamente durante su permanencia en la UAEGRTD.
b. La UAEGRTD fomenta continuamente una cultura de conciencia sobre la seguridad de la información, incentivando a los colaboradores (funcionarios / contratistas) a identificar, reportar y mitigar riesgos en este sentido.

7.2.3 Proceso Disciplinario

Cualquier incumplimiento de las políticas de la Seguridad de la Información, establecida y regulada en las normas de orden nacional y las reglamentarias de la UAEGRTD, puede conllevar el inicio de acciones disciplinarias en el marco del Código General Disciplinario (Ley 1952de 2019), tanto para servidores públicos como para contratistas y particulares que ejercen funciones públicas.

Es obligación de todos los colaboradores de la UAEGRTD (funcionarios / contratistas), dar cumplimiento a las políticas complementarias de seguridad de la información contenidas en el presente documento.

7.3 Finalización del Empleo o Cambio en el Puesto de Trabajo

Objetivo: Proteger los intereses de la Unidad en los procesos de cambio o terminación del contrato.

a. Al momento de la terminación de la relación laboral / contractual de un colaborador (funcionario / contratista), le serán revocados todos los derechos de acceso y recuperación de activos de información que tenga autorizados, a través del procedimiento establecido para tal propósito.
b. El área de Talento Humano y la Oficina de Tecnologías de la Información deberán asegurarse siempre de la devolución de los activos de información bajo responsabilidad del colaborador (funcionario / contratista) antes de su desvinculación de la UAEGRTD.
c. En la desvinculación de un colaborador (funcionario / contratista) de la UAEGRTD, el administrador o encargado de la plataforma de correo electrónico, deberá realizar la respectiva copia de respaldo del buzón del colaborador y alojarla en el servidor destinado para tal fin.
d. Las cuentas de correo electrónico respaldadas de colaboradores desvinculados podrán ser restauradas a solicitud del director del área o jefe inmediato / supervisor o cuando se requiera por fines de investigación ordenado por un juez de la república. La solicitud se hará a través de los canales dispuestos por la Oficina de Tecnologías de la Información. Los respaldos de los buzones de correo electrónico serán conservados teniendo en cuenta lo estipulado en las Tablas de Retención Documental de la UAEGRTD.
e. Cualquier cambio en las responsabilidades o reasignación de funciones de un colaborador (funcionario / contratista) será evaluado por el líder del proceso, el supervisor y por el responsable de seguridad de la información para asegurarse de que se mantenga un adecuado nivel de acceso a la información.

8 GESTIÓN DE ACTIVOS

8.1 Responsabilidad Sobre los Activos

Objetivo: Identificar los activos organizacionales y definir las responsabilidades de protección apropiadas.

8.1.1 Inventarios de Activos

Todos los activos de información deben estar identificados y registrados en un inventario centralizado. Este inventario incluye, la descripción del activo, el propietario, la ubicación, la clasificación y cualquier restricción de uso del mismo.

8.1.2 Propiedad de los Activos

Todos los activos de información de la UAEGRTD deben tener un propietario designado, quien es responsable de la supervisión y el uso adecuado del mismo. Los propietarios deben garantizar que se implementen y mantengan medidas de seguridad adecuadas para dichos activos.

8.1.3 Uso Aceptable de los Activos

La UAEGRTD establece normas claras sobre el uso aceptable de los activos de información. Estas normas incluyen, directrices sobre el uso de dispositivos de almacenamiento extraíbles, acceso a la red, uso de software y acceso a información sensible.

8.1.4 Mantenimiento de Activos

La UAEGRTD establece que todos los activos de información deben ser mantenidos de manera regular y adecuada para asegurar su funcionalidad, integridad y seguridad. Este mantenimiento debe incluir actualizaciones de software, parches de seguridad y auditorías periódicas.

Para tal propósito se llevará un registro de todas las acciones de mantenimiento realizadas sobre los activos para asegurar la trazabilidad y responsabilidad.

8.1.5 Devolución y Retiro de los Activos

La UAEGRTD establece que todos los activos de información deben seguir un proceso claro para el retiro seguro y eliminación cuando ya no sean necesarios. Este proceso debe incluir la destrucción segura de datos y la eliminación física cuando sea necesario.

Todos los activos desechados deben ser retirados de manera que se minimice el riesgo de que la información contenida en ellos sea recuperada indebidamente.

Para el traslado temporal o permanente de activos de información crítica de la UAEGRTD, debe contarse siempre con una autorización escrita del líder del proceso; si se trata de un activo de información tecnológico debe contarse también con la autorización del Jefe de la Oficina de Tecnologías de Información.

8.2 Clasificación de la Información

Objetivo: Identificar y clasificar los activos de información de acuerdo con su criticidad teniendo en cuenta la Confidencialidad, Integridad y Disponibilidad de la información y requisitos legales.

8.2.1 Categorización de la Información

a. Todos los activos de la UAEGRTD deben estar clasificados según su nivel de sensibilidad y criticidad en función de la Confidencialidad, Integridad y Disponibilidad que requieran.
b. Para la identificación, valoración y categorización de los activos de información debe seguirse la metodología documentada en **GT-GU-12 METODOLOGÍA DE IDENTIFICACIÓN, VALORACIÓN Y CLASIFICACIÓN DE LOS ACTIVOS DE INFORMACIÓN.**

8.2.2 Etiquetado de la Información

Todos los colaboradores (funcionarios / contratistas) deben recibir formación sobre sus responsabilidades en relación con los activos que manejen, incluyendo el manejo seguro y la protección de la información.

8.2.3 Manipulación de la Información

a. Todos los colaboradores (funcionarios / contratistas) garantizarán que los activos de información a que tienen acceso son utilizados para fines autorizados y que siguen las políticas de seguridad en el manejo de la información.
b. Todos los activos de información críticos deben estar ubicados en áreas seguras y protegidos contra amenazas que puedan afectar su buen uso, disponibilidad y confidencialidad.
c. Los activos de información críticos que sean de tipo digital deben estar protegidos con una contraseña u otro sistema que asegure que serán accedidos solamente por personal autorizado.

8.3 Manejo de Medios

Objetivo: Evitar la divulgación, la modificación, el retiro o la destrucción no autorizados de información almacenada en los medios.
Dentro de esta política se entiende como medios de información, cualquier dispositivo o soporte que contenga información, ya sea en formato digital o físico y aplica a todos los colaboradores (funcionarios / contratistas) que tengan acceso a los medios de información de la UAEGRTD incluyendo, pero no limitándose a medios electromagnéticos como discos duros y USB, medios ópticos, equipos de almacenamiento en la nube, documentos físicos y cualquier otro medio que pueda contener datos sensibles.

a. El término Destrucción de Medios: Corresponde al proceso mediante el cual se asegura que la información en los medios no puede ser recuperada.
b. La Transferencia de Medios: Es el movimiento físico o lógico de medios de un lugar a otro.

8.3.1 Gestión de Medios Extraíbles

a. Los medios que contengan información sensible en la UAEGRTD deben ser almacenados en lugares seguros y bajo un control de acceso adecuado.
b. Durante el transporte, los medios deben ser protegidos adecuadamente para evitar la pérdida, robo o daño.
c. El acceso a los medios estará limitado a personal autorizado únicamente.
d. En los equipos tecnológicos, el acceso a los puertos de unidades extraíbles (USB, CD/DVD) debe estar restringido y solo autorizado por la Oficina de Tecnologías de la Información.
e. Todos los medios extraíbles deben ser analizados con software antivirus actualizado cada vez que sean utilizados en los equipos de la UAEGRTD.
f. Siempre y cuando sea posible, los medios extraíbles de propiedad de la UAEGRTD deben estar cifrados y guardados en un lugar seguro para evitar la pérdida o robo de la información.
g. En los medios extraíbles de la UAEGRTD, no está permitido guardar información de tipo personal.
h. No está permitido conectar los medios extraíbles de la UAEGRTD en lugares que no ofrezcan las garantías de seguridad mínima que eviten la pérdida, robo o fuga de información o la contaminación por malware.

8.3.2 Disposición Final de Medios

a. Todos los medios que ya no sean necesarios para la UAEGRTD deben ser destruidos de manera segura, utilizando métodos aprobados que garanticen que la información ya no pueda ser recuperada.
b. Toda destrucción de medios en la UAEGRTD debe ser documentada, registrando el tipo de medio, la fecha de destrucción, el método utilizado y el responsable de su ejecución. En el caso de impresos / físicos, se debe utilizar en lo posible una máquina trituradora y en el caso de medios electrónicos esta actividad será ejecutada por la Mesa de Servicios de la OTI y aprobada por el Oficial de Seguridad de la Información.

8.3.3 Transferencia de Medios Físicos

a. Todas las transferencias de medios ya sean físicas o electrónicas, deben documentarse y seguir procedimientos de autorización determinados.
b. Toda la transferencia de medios a terceros debe hacerse previa firma de un acuerdo de confidencialidad y cumpliendo con las políticas de seguridad de la información de la UAEGRTD.

8.3.4 Capacitación y Conciencia

La UAEGRTD proporcionará capacitación adecuada a todos los colaboradores (funcionarios / contratistas) sobre el manejo seguro de medios y las consecuencias de la no observancia de esta política.

9 CONTROL DE ACCESOS

9.1 Requisitos de Negocio para el Control de Acceso

Objetivo: Establecer los lineamientos generales para el acceso controlado a la información de la UAEGRTD. Lo anterior, con el fin de minimizar afectación a la confidencialidad, integridad y disponibilidad de la información generada y procesada.

9.1.1 Política de Control de Acceso

Esta Política de Seguridad de la Información establece las directrices y procedimientos que deben cumplirse para proteger la información y los activos de información de la UAEGRTD, alineándose con el Modelo de Seguridad y Privacidad de la Información (MSPI) de MinTIC y los principios de la norma ISO 27001, referente al Control de Acceso, para garantizar que el acceso a la información y los sistemas es autorizado, controlado y monitoreado, minimizando el riesgo de acceso no autorizado y asegurando la confidencialidad, integridad y disponibilidad de la información.

9.1.2 Acceso a las Redes y a los Servicios de Red

Todo acceso a los sistemas de información, bases de datos y redes de la UAEGRTD debe ser solicitado formalmente mediante un formulario de solicitud de acceso por el líder del proceso correspondiente. El acceso se concede basado en el principio de "Mínimo Privilegio". Ningún colaborador (funcionario / contratista) deberá acceder ni intentar acceder a áreas seguras, información y/o plataformas tecnológicas de la UAEGRTD para las cuales no esté debidamente autorizado.

9.2 Gestión de Acceso de Usuarios

Objetivo: Asegurar el acceso de los usuarios autorizados y evitar el acceso no autorizado a sistemas y servicios de la UAEGRTD.

9.2.1 Registro de Usuarios

Los roles de usuarios se definirán y documentarán de manera clara, asignando permisos conforme a las funciones y responsabilidades. Los permisos otorgados serán revisados periódicamente para garantizar su actualización frente a los requerimientos de acceso del usuario según las actividades que ejecute para el desarrollo normal de su trabajo.

9.2.2 Acceso de Usuario

a. El acceso a áreas seguras, activos de información y plataformas tecnológicas de la UAEGRTD, por parte de los colaboradores (funcionarios / contratistas) y/o terceros autorizados, se hará exclusivamente a través de credenciales seguras utilizando contraseñas fuertes cuyas características están definidas en el documento GT-IN-04 ADMINISTRACION DE USUARIOS EN EL DIRECTORIO ACTIVO.
b. Las credenciales asignadas a los colaboradores (funcionarios / contratistas) son para el acceso y uso de los servicios tecnológicos, así como el ingreso a áreas seguras, son de carácter personal e intransferible.
c. Los colaboradores están obligados a hacer buen uso de sus credenciales asignadas, en caso de presentarse incidentes donde estás se vean comprometidas, serán responsables de las mismas y deberán atender las acciones disciplinarias y/o de ley a que haya lugar.

9.2.3 Gestión de Privilegios de Acceso

a. Los accesos privilegiados serán asignados únicamente a usuarios específicos cuya función así lo requiera.
b. El uso de programas utilitarios privilegiados está reservado solo a los usuarios con necesidades específicas y justificadas de la Oficina de Tecnologías de Información.
c. La autorización para los usuarios privilegiados debe ser aprobada por el jefe de la Oficina de Tecnología de Información

9.2.4 Gestión de la Información Secreta de Autenticación de los Usuarios

La UAEGRTD, implementará y gestionará mecanismos para la asignación de información reservada de autenticación para efectos de su control. Estos mecanismos deben contemplar los siguientes aspectos clave en la autenticación de los usuarios:

a. Definición clara de las características en la creación de contraseñas, incluyendo longitud mínima, complejidad (uso de mayúsculas, minúsculas, números y símbolos), prohibición de contraseñas obvias o reutilizadas y requisitos de cambio periódico.
b. Utilización de mecanismos seguros para almacenar las contraseñas y otra información de autenticación de forma cifrada que impida su fácil lectura en caso de una brecha de seguridad.
c. La transmisión de contraseñas deberá ser por canales seguros y cifrados en los procesos de inicio de sesión o cambio de contraseña.
d. Las actividades de creación, modificación, restablecimiento y eliminación de contraseñas deben hacerse a través de procedimientos seguros y establecidos formalmente.
e. Los usuarios deben ser informados y capacitados sobre la importancia de elegir contraseñas seguras, protegerlas y no compartirlas.
f. Después de un número determinado de intentos fallidos de inicio de sesión las cuentas serán bloqueadas para prevenir ataques de fuerza bruta.
g. Se contará con procesos seguros para facilitar el cambio de contraseñas a los usuarios, incluyendo restablecer contraseñas olvidadas, a través de procedimientos de verificación de identidad.
h. Se aplicarán principios de seguridad similares a otros métodos de autenticación secreta más allá de las contraseñas.

9.2.5 Revisión de los Derechos de Acceso de Usuario

Los derechos de acceso otorgados a los usuarios en los sistemas de información y datos de la UAEGRTD serán revisados anualmente o ante cambios significativos en el rol o responsabilidades de los usuarios, para asegurar que dichos permisos sigan siendo necesarios, apropiados y estén alineados con las responsabilidades y roles actuales de cada usuario.

Esta revisión será responsabilidad de cada líder de proceso y/o sistema utilizado por los usuarios respectivos, dejando un registro documental de su ejecución.

9.2.6 Revocación de Accesos

Tras la finalización del vínculo laboral, terminación del contrato o cuando ya no sea necesario para el rol del usuario, el acceso será revocado inmediatamente, siguiendo el procedimiento que se establezca para tal propósito, coordinado por las áreas de Talento Humano, líder de proceso o supervisor donde el colaborador prestaba sus servicios y la Oficina de Tecnologías de Información.

Para casos excepcionales, cuando se requieran mantener activas las credenciales de un usuario desvinculado de la UAEGRTD se podrá hacer, previa solicitud por parte del jefe o supervisor del usuario respectivo, a la Oficina de Tecnologías de la Información a través de la Mesa de Servicio.

Así mismo, serán inactivados todos los derechos de acceso en las ausencias temporales (vacaciones, incapacidades, licencias remuneradas, licencias no remuneradas, permisos, etc.) o en caso de sanción disciplinaria. La reactivación de los derechos de acceso para realizar actividades especiales inherentes al rol desempeñado por el usuario se hará a solicitud expresa del supervisor o jefe inmediato.

9.3 Responsabilidad de los Usuarios

Objetivo: Establecer la responsabilidad a los usuarios para salvaguardar la seguridad de la información de autenticación mediante el uso adecuado de los mecanismos establecidos en la Entidad.

9.3.1 Uso de la Información Secreta de Autenticación

a. El acceso a las redes y servicios críticos de la UAEGRTD se concederá aplicando mecanismos de autenticación fuerte (incluyendo autenticación multifactor cuando sea necesario).
b. La información secreta de autenticación, como contraseñas, pins, claves, etc.; debe ser custodiada diligentemente por cada usuario responsable, debiendo garantizar su almacenamiento de forma segura y no compartirla con terceros no autorizados.
c. Los usuarios son responsables de crear contraseñas robustas y cambiarlas periódicamente y proteger sus dispositivos de acceso no autorizado para evitar la exposición de sus credenciales.

9.4 Control de Acceso a Sistemas y Aplicaciones

Objetivo: Asegurar que solo los usuarios autenticados y autorizados puedan acceder a los sistemas y aplicaciones y, una vez que un usuario ha accedido, sus acciones y acceso a la información dentro de esos sistemas y aplicaciones estén restringidos de acuerdo con sus roles, responsabilidades y las políticas de control de acceso establecidas por la Unidad.

9.4.1 Restricción del Acceso a la Información

a. La UAEGRTD implementará controles de acceso adecuados para proteger la red de la Entidad, incluyendo firewalls, sistemas de detección de intrusos (IDS) y herramientas de gestión de seguridad.
b. El acceso a la información se restringirá a los usuarios y procesos que tengan una necesidad de conformidad a sus competencias. Para tal efecto se implementarán mecanismos de control de acceso lógico y físico, basados en roles y privilegios.

9.4.1.1 Uso de Carpetas Compartidas

En la UAEGRTD está restringido el uso de carpetas compartidas. Para su uso los colaboradores (funcionarios / contratistas) deben observar los siguientes lineamientos:

a. Los servicios de carpetas compartidas ofrecidos por la Oficina de Tecnologías de Información son File Server y SharePoint, cada carpeta podrá ser administrada por una o varias personas (si hay subgrupos) quienes velarán por el buen uso de la información y de las carpetas.
b. La información CLASIFICADA o RESERVADA, debe reposar en las carpetas destinadas en el File Server, para que sean incluidos en las políticas de respaldo de información.
c. La información PUBLICA deberá almacenarse en la carpeta de SharePoint de cada dependencia.
d. El uso de OneDrive se debe utilizar solamente para almacenar información PUBLICA que es producida por cada colaborador.
e. Cada colaborador deberá depurar su carpeta personal de OneDrive, eliminando la información que no utiliza.
f. Se restringe el acceso a las carpetas compartidas a colaboradores (funcionarios / contratistas) desde equipos de cómputo que no cuenten con antivirus actualizado.
g. Solamente está permitido el acceso a las carpetas compartidas por los colaboradores (funcionarios / contratistas) de la UAEGRTD.
h. La Oficina de Tecnologías de Información realizará monitoreo y revisiones periódicas, con el fin de velar por una correcta administración de las carpetas compartidas al menos cada semestre.

9.4.1.2 Uso Adecuado del Internet

El acceso a Internet dentro de la entidad se configura como una herramienta de uso estrictamente laboral, destinada al cumplimiento de las funciones asignadas. En consecuencia, cualquier actividad o propósito que no esté directamente relacionado con las funciones asignadas no está permitido; dicha restricción a asegurar el debido uso de los recursos públicos y la mitigación de posibles riesgos de seguridad.

a. Los privilegios de uso de Internet estarán definidos de acuerdo con la necesidad de acceso que requiera el desarrollo de la función de cada usuario y acordes con los procesos que gestionan, siempre y cuando se realice de manera ética, razonable, responsable, no abusiva y sin afectar la productividad ni la protección de la información.
b. Los colaboradores (funcionarios / contratistas), no pueden asumir en nombre de la UAEGRTD, posiciones personales en encuestas de opinión, foros u otros accesos web similares.
c. Está estrictamente prohibido el ingreso a páginas web con contenido que se considere inapropiado, ofensivo, ilegal o que pueda atentar contra la seguridad de la información.
d. El usuario no debe descargar ningún programa o software, sin la debida autorización, de la Oficina de Tecnologías de Información.
e. El manejo de información en la nube únicamente está autorizado a través de la herramienta One Drive.
f. Cualquier cambio o excepción deberá estar soportado y contar con las aprobaciones respectivas.

9.4.2 Procedimientos Seguros de Inicio de Sesión

La UAEGRTD establecerá procedimientos seguros para el inicio de la sesión de los usuarios en sistemas y aplicaciones, garantizando la identidad de los usuarios y evitando el acceso no autorizado a los sistemas y aplicaciones a través del uso de contraseñas robustas, la exigencia de autenticación multifactor y la gestión adecuada de intentos fallidos de inicio de sesión y del cierre de esta.

9.4.3 Sistemas de Gestión de Contraseñas

La UAEGRTD aplicará sistemas de gestión de contraseñas que garanticen la seguridad del uso las credenciales de autenticación de los usuarios, que incluirán parámetros mínimos para la creación de contraseñas robustas

9.4.4 Uso de Utilidades con Privilegios del Sistema

Las herramientas con capacidad de modificar la configuración, la seguridad o el funcionamiento normal de los sistemas de información y las aplicaciones de la UAEGRTD estarán restringidos para uso exclusivo de personal autorizado y su uso será registrado y monitoreado para facilitar la identificación de accesos no autorizados y la realización de auditorías periódicas.

9.4.5 Control de Acceso al Código Fuente de los Programas

a. El acceso al código fuente de programas desarrollados y en uso en la UAEGRTD estará limitado a personal autorizado según sus roles y necesidades laborales.
b. Se utilizarán sistemas de control de versiones que registren todas las modificaciones realizadas al código fuente, incluyendo la identidad del autor y la fecha de modificación.
c. Se implementarán revisiones de código periódicas para garantizar que solo el personal autorizado esté accediendo al código y que las modificaciones sean legítimas y aprobadas.

10 CRIPTOGRAFÍA

10.1 Controles Criptográficos

Objetivo: Asegurar el uso apropiado y eficaz de la criptografía para proteger la confidencialidad, la autenticidad y/o la integridad de la información en la Unidad.

10.1.1 Política de Uso de Controles Criptográficos

La UAEGRTD implementará controles criptográficos para proteger la información sensible y crítica, asegurando que la utilización de criptografía sea apropiada y esté alineada con las normativas y regulaciones aplicables.

Toda información en tránsito por líneas de comunicación, alojada en dispositivos transportables o móviles que se considere sensible por su confidencialidad debe protegerse ante el acceso no autorizado mediante mecanismos de cifrado de la información. Se deberá tener en cuenta la fortaleza de los mecanismos de cifrado a utilizar de acuerdo con el nivel de confidencialidad de la información (longitudes de clave mínimas, tipo, fortaleza y calidad del algoritmo de encriptación requerido).

El líder de proceso o responsable del activo de información, con la colaboración de la OTI, deberá tener en cuenta los siguientes aspectos para la definición de los criterios criptográficos:

a. Contar con herramientas y mecanismos de cifrado simétricos y asimétricos (Certificados digitales) en la entidad.
b. La sensibilidad de la información y su nivel de clasificación, así como los sistemas y líneas de comunicaciones por los que se almacena, procesa o transmite la información.
c. La generación, custodia, renovación y revocación de claves criptográficas.
d. Recuperación de la información cifrada en caso de pérdida o destrucción de las claves.

Todos los aplicativos que se encuentran expuestos a internet deben tener implementados certificados digitales para proteger los servicios internos.

10.1.2 Gestión de Claves

a. Las llaves, claves, tokens, certificados y firmas digitales serán gestionados y almacenados en lugares seguros, los medios digitales deben contar con respaldos periódicos para recuperarse en caso de pérdida del original.
b. Aquellos colaboradores (funcionario / contratista) a quienes se les haya asignado un token virtual o clave para firmar digitalmente en el desempeño de sus funciones, serán responsables del uso y manejo adecuado de dicho token, considerando:
   - El token o clave solo podrá ser empleado para trámites exclusivos de la UAEGRTD.
   - Debe ser mantenido bajo su custodia y no permitir que sea accedido por terceros.
   - Debe notificar con anterioridad las novedades del token virtual como, emisión, bloqueo o revocación entre otras.
   - Atender las recomendaciones dadas en el momento de la entrega.
   - Preservar los archivos firmados digitalmente.
   - Atender los lineamientos dados por Gestión Documental para el uso de las firmas digitales.
c. Los administradores de infraestructura y de sistemas deberán usar una herramienta para la gestión de las claves, definida por la OTI, así como hacer la entrega de la clave maestra al jefe o supervisor para que la custodie y en un caso fortuito una tercera parte autorizada pueda tener acceso para poder descifrar los datos.
d. Siempre que se compartan claves, se debe garantizar su confidencialidad en el intercambio de las mismas a través de un canal seguro y diferente al que se envía la información.
e. La UAEGRTD llevará a cabo auditorías y monitoreos periódicos sobre la gestión de claves y el uso de controles criptográficos para asegurarse de que se cumplan las políticas establecidas y se identifiquen posibles vulnerabilidades.
f. Dentro del plan de comunicaciones de la función de seguridad y privacidad de la información, se ofrecerán capacitaciones / piezas gráficas de concienciación para todos los colaboradores (funcionarios / contratistas) sobre el correcto uso de controles criptográficos y la gestión de claves, destacando la importancia de seguir las políticas y procedimientos establecidos.

11 SEGURIDAD FISICA Y DEL ENTORNO

11.1 Áreas Seguras

Objetivo: Prevenir el acceso físico no autorizado, el daño y la interferencia a la información y a las instalaciones de procesamiento de información de la organización.

11.1.1 Perímetros de Seguridad Física

a. La Oficina de Tecnología de la Información OTI, definirá el perímetro de las áreas seguras de tecnología que contienen la información y sus instalaciones de procesamiento sensible o crítico, las cuales deben estar cerradas y protegidas de accesos no autorizados (cerraduras, alarmas, construcciones sólidas, mecanismos de control).
b. La UAEGRTD efectuará un análisis de riesgos y planes de tratamiento específicos para cada una de las oficinas territoriales que permitan aplicar los lineamientos relacionados con la seguridad perimetral para sus instalaciones.
c. Los eventos e incidentes que involucren la pérdida, daño, robo o compromiso de activos de información de la UAEGRTD, producto de inconvenientes en los perímetros de seguridad física, deberán ser reportados a la Oficina de Tecnología de la Información por el área o dependencia donde haya ocurrido y cuando se tenga conocimiento.

11.1.2 Controles de Acceso Físico

El acceso físico a las instalaciones de la UAEGRTD estará restringido únicamente al personal autorizado mediante:

a. Sistemas de control de acceso, como tarjetas de proximidad, biometría o códigos de acceso.
b. Registro y auditoría de todas las entradas y salidas a áreas restringidas.
c. Capacitación continua al personal sobre los procedimientos de acceso y la importancia de mantener la confidencialidad de los métodos de ingreso.
d. Todos los visitantes deberán identificarse en la recepción y deben ser recibidos por un colaborador para el acompañamiento obligatorio dentro de las instalaciones, en cumplimiento de los procedimientos establecidos en el proceso de gestión logística y recursos físicos y los lineamientos emitidos por el Grupo de Gestión de Seguimiento y Operación Administrativa.
e. El cumplimiento del procedimiento de control de acceso físico es responsabilidad de todos los colaboradores al asegurar el acompañamiento de sus visitantes en las instalaciones de la UAEGRTD.

11.1.3 Seguridad de Oficinas, Recintos e Instalaciones

Las oficinas y recintos de la UAEGRTD deberán estar asegurados mediante:

a. Equipos de seguridad como alarmas y sistemas de videovigilancia que deberán ser objeto de mantenimiento regular.
b. Designación de zonas de trabajo que mantengan la información sensible resguardada y con control de acceso restringido.
c. Cámaras de video en sitios estratégicos de la UAEGRTD que permitan realizar seguimiento al cumplimiento de las políticas de seguridad física. Las imágenes deben ser conservadas por el tiempo que sea establecido localmente en cada uno de los sitios de trabajo, o en el caso en que la imagen respectiva sea objeto o soporte de una reclamación, queja, o cualquier proceso de tipo judicial, hasta el momento en que sea resuelto.
d. La instalación de las cámaras debe ser acorde a la identificación de áreas sensibles y las imágenes se deben monitorear con el fin de identificar situaciones que requieran la ejecución de acciones disciplinarias o de mejoramiento.

e. La UAEGRTD gestionará el diseño, monitoreo y mantenimiento de un esquema de vigilancia que permita garantizar el cumplimiento de las políticas de seguridad física, salvaguardar los activos de información de la Unidad y proteger la integridad de los colaboradores (funcionarios / contratistas) y visitantes.

11.1.4 Protección Contra las Amenazas Externas y Ambientales

Para proteger las instalaciones de la UAEGRTD de amenazas externas y ambientales, se establecerán las siguientes medidas específicas:

a. Evaluaciones periódicas de riesgos para identificar y mitigar amenazas externas (ej. incendios, inundaciones, vandalismo).
b. Implementación de sistemas de detección y extinción de incendios apropiados.
c. Planes de continuidad del negocio y recuperación ante desastres que consideren incidentes externos y ambientales.

11.1.5 El Trabajo en Áreas Seguras

Para la UAEGRTD se consideran áreas seguras los centros de datos, cuartos técnicos, la Tesorería, espacios para el archivo de información y cuartos de videovigilancia. También los espacios físicos que el dueño del activo de información considere, de acuerdo con la criticidad de la operación que ejecute. El acceso a estas áreas estará restringido solo a personal autorizado y capacitado para trabajar con información sensible.

11.1.6 Áreas de Carga y Descarga

Las áreas designadas para el despacho, carga y descarga de bienes, documentos o cualquier otro activo de información de la UAEGRTD estarán sujetas a los lineamientos y controles de seguridad de la información que permitan prevenir el acceso no autorizado, la pérdida, el daño, robo o cualquier otra amenaza a la confidencialidad, integridad y disponibilidad de la información y los activos durante las operaciones de despacho y carga. Esto incluye:

a. El acceso a las áreas de despacho carga y descarga estará restringido al personal autorizado y a los visitantes que hayan sido debidamente identificados y registrados.
b. La UAEGRTD mantendrá un registro de ingresos y salidas de personal y vehículos a las áreas de despacho y carga, cuando sea apropiado.
c. Los privilegios de acceso a estas áreas serán revisados periódicamente.
d. Se establecerán procedimientos para la correcta identificación, embalaje y etiquetado de los activos que se van a despachar, cargar y descargar.
e. Se tomarán medidas para proteger las áreas de despacho y carga contra condiciones ambientales adversas que puedan dañar la información o los activos (humedad, temperatura extrema, polvo).
f. Se establecerán y comunicarán procedimientos para responder a situaciones de emergencia que puedan afectar la seguridad de la información o los activos en las áreas de despacho y carga (incendios, robos, incidentes de seguridad).

11.2 Seguridad de Equipos

Objetivo: Prevenir la perdida, daño, robo o compromiso de activos y, la interrupción de las operaciones de la Unidad.

11.2.1 Equipos de Cómputo y Comunicaciones

La UAEGRTD establece que todos los equipos de cómputo y comunicaciones deben estar ubicados y protegidos para reducir los riesgos de amenazas y peligros del entorno y las posibilidades de acceso no autorizado, daño, interferencia o pérdida.

11.2.1.1 Ubicación y Protección de los Equipos

Al interior de la UAEGRTD todos los equipos de información deben ubicarse en áreas controladas que limiten el acceso físico a personal no autorizado.

a. Se implementarán medidas de seguridad, como acceso restringido y videovigilancia, en las zonas donde se encuentran estos equipos.
b. Deberá hacerse un inventario anual de los equipos para asegurar su correcta localización y protección.

11.2.2 Servicios de Suministro

Todos los proveedores de servicios deberán cumplir con los requisitos de seguridad establecidos por la UAEGRTD antes de que se les permita acceder a los equipos e instalaciones.

a. Se deberá evaluar la seguridad de los servicios de suministro que involucren el manejo de datos sensibles o críticos.
b. Los contratos con proveedores incluirán cláusulas que especifiquen las medidas de seguridad que deben aplicarse.

11.2.3 Seguridad de Cableado

La red de datos de la UAEGRTD seguirá las normativas internacionales de cableado estructurado, está prohibido (salvo autorización o supervisión expresa de la OTI) la intervención física de los usuarios sobre los recursos de la red institucional (cables, enlaces, estaciones de trabajo, dispositivos de red).

a. El cableado que conecta los equipos de información debe instalarse de manera que minimice el riesgo de daños y accesos no autorizados.
b. Se implementarán controles físicos para proteger el cableado de interferencias, daños o manipulaciones, incluyendo canalizaciones adecuadas y etiquetas de identificación.
c. El cableado será objeto de mantenimiento adecuado para asegurar su correcta operatividad.

11.2.4 Mantenimiento de Equipos de Cómputo y Comunicaciones

Todo mantenimiento de los equipos de información será realizado de acuerdo con un programa establecido que garantice las normas de seguridad pertinentes.

a. Solo personal autorizado y debidamente capacitado podrá realizar tareas de mantenimiento y se seguirán procedimientos de registro y auditoría de dichas actividades.
b. Los equipos en mantenimiento deberán ser etiquetados y segregados de aquellos que estén en operación. El soporte técnico, actualización y mantenimiento a las estaciones de trabajo y servidores de la entidad se hará acorde a las especificaciones de los fabricantes de los equipos.

11.2.5 Retiro de Equipos de Cómputo y Comunicaciones

a. Los equipos que sean dados de baja y retirados de la UAEGRTD deben ser desmantelados y/o destruidos de acuerdo con procedimientos establecidos para la eliminación segura de los datos y componentes.
b. La Oficina de Tecnologías de Información mantendrá un registro de todos los equipos informáticos dados de baja y retirados, asegurando que se sigan los protocolos de seguridad establecidos para la protección de información sensible.
c. Se realizarán evaluaciones periódicas para garantizar que los procedimientos de retiro de activos sean efectivos y cumplan con las normativas aplicables.

11.2.6 Seguridad de los Equipos Fuera de las Instalaciones

Todos los equipos de cómputo, comunicaciones y accesorios como unidades de almacenamiento que contengan información confidencial o sensible de la UAEGRTD deben ser protegidos adecuadamente cuando se encuentren fuera de las instalaciones de Unidad. Es responsabilidad de los custodios respectivos adoptar las medidas de protección necesarias para resguardar la seguridad de estos equipos.

a. Los colaboradores (funcionarios / contratistas) deben utilizar medios seguros para transportar estos equipos, como maletines cerrados y dispositivos de seguridad como candados o sistemas de rastreo si es el caso.
b. El uso de conexiones a redes públicas no seguras (Wi-Fi) debe evitarse en todo momento. En caso de ser necesario, se debe utilizar una conexión VPN.
c. Los dispositivos deben ser asegurados y supervisados todo el tiempo al ser utilizados en espacios públicos.

11.2.7 Disposición Segura o Reutilización de Equipos

Antes de la disposición o reutilización de cualquier equipo, debe llevarse a cabo un proceso de limpieza que garantice la eliminación definitiva de cualquier información sensible.

a. Deberán utilizarse herramientas de borrado certificadas para asegurar que toda la información almacenada sea irrecuperable.
b. La documentación relacionada con el proceso de disposición final debe mantenerse como registro para controlar las acciones de seguridad realizadas.

11.2.8 Equipo de Usuario Desatendidos

Es obligación de todos los colaboradores (funcionarios / contratistas) asegurarse de que todos los equipos que contengan información confidencial o sensible sean protegidos cuando estén desatendidos.

Para todo equipo que quede desatendido, el usuario deberá bloquear la pantalla de forma inmediata o apagar el dispositivo si la ausencia será prolongada.

Dentro de los controles para restringir el acceso a los equipos de cómputo de la Unidad, se implementarán a través del directorio activo, un tiempo máximo de terminal desatendida antes de que la misma quede bloqueada por no uso.

11.2.9 Política de Escritorio y Pantalla Limpia

a. Todos los colaboradores (funcionarios / contratistas) deben mantener un entorno de trabajo limpio, donde no haya documentos o dispositivos que contengan información confidencial o sensible visibles cuando no estén en uso. Un entorno ordenado facilita la ubicación de los elementos y la identificación rápida ante posibles pérdidas.
b. Ningún colaborador (funcionario / contratista) deberá dejar información impresa que contenga datos sensibles en escritorios, impresoras o espacios públicos. En caso de ausentarse del puesto de trabajo, el escritorio debe quedar libre de carpetas, oficios o cualquier otro documento los cuales deberán ser salvaguardados bajo llave; de igual manera, todo documento que se imprima debe ser retirado inmediatamente de las impresoras.
c. Al final de cada jornada laboral, los colaboradores (funcionarios / contratistas) deben guardar o destruir información impresa que no sea necesaria y asegurar que sus pantallas estén protegidas. Los documentos de la UAEGRTD deben estar disponibles únicamente a las personas autorizadas y bajo la responsabilidad del custodio que salvaguarda la información.
d. La pantalla y escritorio de los computadores deben permanecer libre de iconos y/o accesos directos innecesarios; las estaciones de trabajo, equipos portátiles y computadores de escritorio deben tener el fondo de escritorio y protector de pantalla institucional, de forma que se active ante un tiempo

específico sin uso. Al ingresar a la cuenta, la pantalla debe solicitar únicamente el nombre de usuario y contraseña.

e. La UAEGRTD promoverá la cultura del "escritorio limpio" mediante capacitaciones periódicas y recordatorios sobre la importancia de la seguridad de la información.

11.2.10 Uso de Computadores Personales – (BYOD, Bring Your Own Device)

Los colaboradores (funcionarios / contratistas) de la UAEGRTD y terceros que por sus labores requieren tener acceso a los recursos de información de la Unidad a través de sus computadores y/o dispositivos de uso personal, deben acatar las políticas y controles que se establezcan con el fin de proteger los activos de información a los cuales acceden. No habrá dispositivos con información de la UAEGRTD que no cuenten con los lineamientos definidos por la Unidad.

a. La información que pueden visualizar los colaboradores (funcionarios / contratistas) a través de los dispositivos que ingresen a la UAEGRTD es confidencial y de uso exclusivo para el desarrollo de sus labores dentro de la Unidad.
b. La configuración de este servicio en los dispositivos de los colaboradores y terceros de la UAEGRTD se realizará únicamente a quienes dadas sus obligaciones requieran de su uso.

Los colaboradores (funcionarios / contratistas) deberán firmar el formato **GT-FO-32 ACEPTACIÓN DE LA POLÍTICA COMPLEMENTARIA PARA EL USO DE DISPOSITIVOS PERSONALES** en donde expresan que conocen, entienden, aceptan y se comprometen a cumplir las Políticas de Seguridad de la Información de la UAEGRTD.

a. Los dispositivos de uso personal con que se requiera el acceso a los recursos e información de la UAEGRTD deben ser validados por el personal de soporte de la Unidad con el fin de garantizar que cuenten con un software antivirus legal y actualizado, adicionalmente se registrará información básica para identificar el dispositivo con marca, modelo, serial, sistema operativo, antivirus y MAC (número de identificación de la tarjeta de red del dispositivo).
b. Es responsabilidad del colaborador (funcionario/contratista) propietario del dispositivo mantenerlo actualizado, tanto en su sistema operativo como en el software antivirus que tenga instalado durante su vinculación con la Unidad.
c. Los colaboradores (funcionarios / contratistas) son responsables de salvaguardar toda la información que se almacena en sus dispositivos, la UAEGRTD no se hace responsable por la realización de copias de respaldo. Así mismo, son responsables de la eliminación y entrega de la información propia de la UAEGRTD en el momento de la desvinculación o terminación del contrato.
d. El servicio de soporte técnico provisto en la UAEGRTD está disponible únicamente para los dispositivos propiedad de la Unidad, cualquier tipo de mantenimiento o reparación por daño de equipos de uso personal es responsabilidad del propietario.
e. Está prohibido que el servicio de soporte de la Unidad adelante labores de mantenimiento de hardware y/o software a dispositivos propiedad de terceros dentro de las instalaciones de la UAEGRTD y/o con recursos de la misma.
f. La UAEGRTD se reserva el derecho de monitorear y restringir las actividades que puedan vulnerar la confidencialidad, integridad y disponibilidad de la información de todos los dispositivos que accedan a recursos de la Unidad. Igualmente podrá remover los derechos de acceso a los sistemas y la información en el momento de la desvinculación, terminación del contrato o por solicitud unilateral de la OTI.

12 SEGURIDAD DE LAS OPERACIONES

12.1 Procedimientos y Responsabilidades Operacionales

Objetivo: Asegurar las operaciones correctas y seguras de las instalaciones de procesamiento de información.

12.1.1 Procedimientos de Operación Documentados

Para todas las operaciones críticas que involucren el manejo y almacenamiento de la información en la UAEGRTD se establecerán y mantendrán procedimientos documentados. Estos procedimientos deben ser accesibles a las partes interesadas y revisados periódicamente para asegurar su eficacia y adecuación. La documentación incluirá, pero no se limitará a:

a. Procesos de gestión de incidentes de seguridad.
b. Métodos de backup y recuperación de información.
c. Protocolos de acceso a sistemas y datos.

12.1.2 Gestión de Cambios

Para la gestión de cambios en los sistemas se implementará un proceso formal que asegure que todas las modificaciones a la infraestructura, sistemas y aplicaciones sean evaluadas, aprobadas, documentadas y comunicadas. Este proceso debe incluir:

a. Evaluaciones de riesgo antes de la implementación de cualquier cambio.
b. Pruebas adecuadas de los cambios en un ambiente controlado antes de su despliegue en producción.
c. Registros de cambios que permitan rastrear la historia de modificaciones.

12.1.3 Gestión de Capacidad

Aplicando buenas prácticas en gestión de capacidad en TI, la UAEGRTD a través de la Oficina de Tecnologías de Información llevará a cabo revisiones periódicas de la capacidad de los sistemas e infraestructura para garantizar su desempeño óptimo y prevenir la saturación. Se realizarán:

a. Evaluaciones regulares del uso de recursos.
b. Planeamiento para futuras necesidades de capacidad basado en el crecimiento proyectado y en la demanda del servicio.
c. Implementación de controles para prevenir sobrecargas en los sistemas.

12.1.4 Separación de los Ambientes de Desarrollo, Pruebas y Operación

Las actividades de desarrollo, pruebas y operaciones de sistemas tendrán entornos separados para evitar interferencias no autorizadas y proteger la integridad de los sistemas de producción. Se incluirá:

a. Restricciones de acceso claras y diferenciadas entre cada ambiente.
b. Protocolo de migración formal para mover código y configuraciones desde los ambientes de desarrollo y pruebas hacia producción.
c. Revisiones de seguridad en los entornos de desarrollo y pruebas para asegurar que no se introduzcan vulnerabilidades.

12.2 Protección Contra el Software Malicioso (Malware)

La UAEGRTD La información y las instalaciones de procesamiento de información en la Unidad estarán protegidas contra códigos maliciosos.

12.2.1 Protección Contra Malware

La UAEGRTD implementará controles de detección, de prevención y de recuperación, combinados con la toma de conciencia apropiada de los usuarios, para protegerse contra códigos maliciosos, considerando:

a. Instalar y mantener actualizado software antivirus y antimalware en todos los dispositivos de la Unidad, servidores y otros sistemas relevantes.

b. Implementar soluciones de filtrado de correo electrónico para detectar y bloquear correos electrónicos sospechosos
c. Utilizar filtros web para bloquear el acceso a sitios web conocidos por distribuir malware o por tener contenido malicioso.
d. Implementar prácticas de codificación segura para prevenir la intrusión de vulnerabilidades que puedan ser explotadas por malware. Realizar pruebas de seguridad del código.
e. Establecer un proceso para identificar, evaluar y mitigar las vulnerabilidades en los sistemas operativos, aplicaciones y software de terceros que podrían ser aprovechadas por el malware.
f. Configurar los sistemas y las cuentas de usuario con los mínimos privilegios necesarios para realizar sus tareas, limitando el daño potencial en caso de infección por malware.
g. Concientizar funcionarios y/o contratistas sobre los riesgos del malware, cómo identificar correos electrónicos y sitios web sospechosos, y las políticas de seguridad relacionadas con el uso de software y dispositivos externos.
h. Implementar y documentar lineamientos para verificar la información relacionada con el software malicioso y emitir comunicados informativos y de advertencia.
i. Tomar acciones pertinentes para contener los incidentes asociados a software malicioso en caso de que se presenten, con el fin de evitar impactos catastróficos.

12.3 Copias de Seguridad

Objetivo: Asegurar la disponibilidad de la información la UAEGRTD en caso de fallas, desastres o cualquier otro evento que pueda comprometer su integridad o disponibilidad.

12.3.1 Respaldo de la Información

La UAEGRTD implementará las medidas necesarias para que su información sea preservada y protegida contra pérdidas, daños o accesos no autorizados a través de procesos de respaldo.

12.3.1.1 Frecuencia y Programación de Respaldos

a. Se utilizará la clasificación de la información para identificar aquella que es vital para la operación la Unidad y que requiera ser respaldada de forma prioritaria.
b. La frecuencia de las copias de respaldo se definirá en función de la criticidad de la información y los Objetivos de Punto de Recuperación (RPO) establecidos. Se considerarán copias completas, incrementales o diferenciales según sea necesario.
c. La programación de los respaldos deberá ser documentada y comunicada por los colaboradores (funcionarios / contratistas) del área de Infraestructura, responsable de ejecutar los respaldos, siguiendo los procedimientos establecidos y utilizando las tecnologías y métodos adecuados.
d. Se mantendrá una documentación clara y actualizada de los procedimientos de copias de respaldo, incluyendo la identificación de la información respaldada, la frecuencia, los medios de almacenamiento, las ubicaciones, los responsables y los procedimientos de restauración.

12.3.1.2 Almacenamiento de Respaldos

a. Se implementará una estrategia de almacenamiento que incluya al menos una copia de respaldo almacenada en una ubicación física separada del sitio principal (ubicación off-site) para proteger contra eventos que afecten la infraestructura principal. Se garantizarán condiciones ambientales adecuadas para la conservación de los medios de respaldo.
b. Se utilizarán medios de almacenamiento seguros y confiables para las copias de respaldo, considerando factores como la capacidad, durabilidad y portabilidad. Estos medios podrán incluir discos duros externos, cintas magnéticas, almacenamiento en la nube u otras soluciones apropiadas.

c. El acceso a las copias de respaldo estará restringido y controlado, otorgándose únicamente al personal autorizado. Se implementarán medidas de seguridad física y lógica para prevenir el acceso no autorizado, la modificación o la destrucción de las copias.
d. Se definirá un periodo de retención para cada tipo de copia de respaldo, basado en los requisitos legales, regulatorios y las necesidades del negocio. Las copias obsoletas se eliminarán de forma segura.

12.3.1.3 Pruebas de Restauración

a. Se realizará un proceso de pruebas periódicas de restauración de los respaldos para asegurar que la información puede ser recuperada de manera efectiva y dentro de los tiempos acordados. Los resultados de estas pruebas se documentarán y se utilizarán para realizar ajustes y mejoras en el proceso de respaldo.

12.4 Registro y Supervisión

Objetivo: Asegurar la detección temprana, el análisis efectivo y la respuesta oportuna a incidentes que puedan comprometer la confidencialidad, integridad y disponibilidad de la información, así como la mejora continua del SGSI.

12.4.1 Registro y Seguimiento

Al interior de la UAEGRTD se establecerán procesos para la recopilación, revisión y análisis de registros de eventos relacionados con la seguridad de la información. Estos registros deben ser suficientes para permitir la identificación de eventos inusuales, accesos no autorizados o cualquier incidente de seguridad.

12.4.1.1 Registro de Eventos (Logs)

En todos los sistemas y aplicaciones críticas de la UAEGRTD deben generarse registros de eventos relacionados con la seguridad de la información. Los eventos para registrar incluyen, pero no se limitan a:

a. Intentos de acceso no autorizados.
b. Cambios en la configuración del sistema.
c. Eventos relacionados con la administración de usuarios.

Los registros deben estar disponibles para análisis y auditoría posterior y se conservarán durante un período determinado de acuerdo con los lineamientos dados por Gestión Documental.

12.4.2 Protección de la Información de Registro

Los registros de eventos guardados en la UAEGRTD deberán ser protegidos contra alteraciones, pérdidas o accesos no autorizados; solo el personal autorizado podrá accederlos.

12.4.3 Registros del Administrador y del Operador

a. Los registros realizados por administradores y operadores de sistemas deberán ser guardados de manera que se garantice su integridad y confidencialidad.
b. Las actividades administrativas, tales como accesos a sistemas críticos, cambios en configuraciones y gestión de usuarios, deberán ser registradas y revisadas periódicamente.
c. Se establecerán auditorías regulares para verificar el correcto manejo de estos registros y detectar eventuales irregularidades.

12.4.4 Sincronización del Relojes

Todos los sistemas críticos deben estar sincronizados con el Instituto Nacional de Metrología, quien genera, monitorea, coordina y difunde la hora legal de la República de Colombia, para garantizar la precisión de los registros en todos los sistemas de la UAEGRTD.

a. Para la sincronización de relojes se utilizará un protocolo de tiempo estándar (NTP) que asegure que todas las aplicaciones y registros mantengan una alineación temporal precisa.
b. No está permitida la desactivación del sistema de sincronización o la manipulación manual de la hora en los dispositivos de la UAEGRTD, las discrepancias en la sincronización de relojes que se detecten deberán ser reportadas y corregidas de inmediato.

12.5 Control del Software en Producción

Objetivo: Prevenir la introducción, uso no autorizado y modificación indebida del software que pueda comprometer los activos de información y la continuidad de las operaciones.

12.5.1 Instalación y Gestión de Software Operacional

a. Toda instalación de software en los sistemas operativos debe estar preautorizada por la Oficina de Tecnologías de Información. Esto incluye la evaluación del software para garantizar que cumple con los estándares de seguridad.
b. Todas las instalaciones de software deben quedar documentadas, incluyendo el nombre del software, la versión, la fecha de instalación, la justificación de su uso y el responsable de la instalación.
c. Las actualizaciones y parches de seguridad deberán aplicarse de manera regular siempre que estén disponibles. El responsable de mantenimiento de cada sistema deberá elaborar un calendario de actualizaciones y realizar reuniones de seguimiento para verificar su aplicación.

12.6 Gestión de la Vulnerabilidad Técnica

Objetivo: Establecer y mantener un proceso sistemático para identificar, evaluar, tratar y mitigar las vulnerabilidades técnicas en los sistemas de información y la infraestructura tecnológica, con el fin de reducir el riesgo de incidentes de seguridad, proteger la confidencialidad, integridad y disponibilidad de la información, y asegurar la continuidad de las operaciones del negocio.

12.6.1 Gestión de las Vulnerabilidades Técnicas

a. Se deberán realizar evaluaciones periódicas para identificar vulnerabilidades en la infraestructura y el software instalado. Para ello, se utilizarán herramientas de análisis de vulnerabilidades y se monitorearán las alertas de seguridad relevantes.
b. Las vulnerabilidades identificadas deben ser clasificadas según su impacto potencial y probabilidad de explotación. Se llevará un registro de estas vulnerabilidades y su estado de mitigación.
c. La remediación de las vulnerabilidades críticas serán objeto de un plan de acción en un plazo establecido, garantizando que se sigan las mejores prácticas de seguridad en el proceso de su implementación.

12.6.2 Restricciones Sobre la Instalación de Software

a. Está prohibida la instalación de software no autorizado o no verificado en los sistemas operativos. Las excepciones deben ser solicitadas formalmente y justificadas ante la Oficina de Tecnologías de Información. El personal de la Mesa de Servicio y los ingenieros territoriales de soporte de TI son los únicos autorizados para la instalación de software en los equipos de la Unidad.

b. Solo se permite el uso de software que esté aprobado y registrado en el inventario de software de la UAEGRTD; este inventario debe ser revisado y actualizado regularmente para reflejar el software autorizado y permitido.

12.7 Consideraciones Sobre la Auditoria de Sistemas de Información

Objetivo: Asegurar que los requisitos de auditoría relacionados con los sistemas de información se planifiquen e implementen de manera efectiva y segura, minimizando la interrupción de los procesos organizacionales y garantizando la confidencialidad, integridad y disponibilidad de la información auditada.

12.7.1 Control de Auditorías de Sistemas de Información

a. Todos los sistemas de información deberán mantener registros de auditoría que identifiquen el acceso y la actividad de los usuarios, así como los cambios en las configuraciones y accesos a datos.
b. Los registros de auditoría deberán estar protegidos y accesibles solo a personal autorizado. Los accesos deben ser monitoreados y registrados.
c. Los registros de auditoría serán revisados de forma periódica para detectar actividades inusuales o no autorizadas, así como para asegurar el cumplimiento de políticas y procedimientos internos.
d. Los registros de auditoría se almacenarán durante un periodo mínimo según los lineamientos dados por Gestión Documental y serán eliminados de acuerdo con las políticas de retención de datos de la UAEGRTD.
e. Cualquier incidente o irregularidad detectada durante el proceso de auditoría deberá ser reportado de inmediato al responsable de Seguridad de la Información, quien evaluará la situación y coordinará acciones correctivas y preventivas.
f. Al menos una vez al año se llevarán a cabo auditorías internas para evaluar la efectividad de los controles de auditoría y el cumplimiento de esta política, sujeto al plan de auditoría establecido por la Unidad.

13 SEGURIDAD DE COMUNICACIONES

13.1 Gestión de la Seguridad de las Redes

Objetivo: Garantizar la confidencialidad, integridad y disponibilidad de la información y los servicios de la organización mediante la implementación y el mantenimiento de controles de seguridad eficaces en la infraestructura de red.

13.1.1 Control de Redes

La UAEGRTD implementará la segmentación de redes para limitar el acceso y proteger la información sensible.

a. Las redes deberán estar divididas en segmentos adecuados en función de los niveles de seguridad requeridos para los datos y servicios. Esta segmentación deberá estar debidamente documentada por parte del personal responsable de su gestión respectiva.
b. Se deberán establecer mecanismos de monitoreo para detectar actividades no autorizadas en las redes.
c. Todos los eventos de seguridad relevantes serán registrados y revisados periódicamente para la detección de incidentes.
d. Se deberán establecer medidas de control de acceso para asegurar que solo el personal autorizado tenga acceso a las redes críticas.
e. Se utilizarán autenticaciones fuertes y métodos de acceso remoto seguro.

13.1.2 Seguridad de los Servicios de Red

a. Todos los dispositivos de red deberán configurarse de acuerdo con las mejores prácticas de seguridad recomendadas.
b. Se llevarán a cabo revisiones periódicas de la configuración para identificar y mitigar vulnerabilidades.
c. Se implementarán tecnologías de detección y prevención de intrusiones para proteger los servicios de red contra ataques.
d. Se realizarán actualizaciones regulares de software y parches de seguridad en todos los dispositivos de red.
e. Los datos en tránsito se cifrarán utilizando protocolos seguros para proteger la confidencialidad e integridad de la información transmitida.
f. Se evaluará y aplicará el cifrado de datos sensibles que circulan por las redes de la UAEGRTD.

13.1.3 Separación en las Redes

a. Se deberá mantener una clara separación entre las redes de producción, desarrollo y prueba para minimizar los riesgos de seguridad.
b. Las pruebas de nuevos sistemas o programas deben realizarse en entornos aislados.
c. Los sistemas que manejen información altamente confidencial deberán estar aislados en redes separadas para reducir el riesgo de accesos indebidos.
d. Se evaluarán y revisarán las medidas de separación de redes de manera continua.
e. Las conexiones a redes externas (como Internet u otras organizaciones) se realizarán a través de controles de seguridad apropiados, como cortafuegos y gateways seguros.
f. Se realizará una evaluación de riesgos antes de establecer conexiones con redes externas.

13.2 Transferencia de Información

Objetivo: Asegurar la protección de la información durante su transferencia, tanto interna como externamente, a través de la implementación y mantenimiento de controles apropiados que prevengan accesos no autorizados, divulgación, modificación o destrucción, garantizando así su confidencialidad, integridad y disponibilidad.

13.2.1 Políticas y Procedimientos de Transferencia de Información

Todas las transferencias de información deben realizarse de manera segura y controlada, alineadas con las clasificaciones de la información establecidas por la UAEGRTD.

Se deben seguir los lineamientos de seguridad establecidos en el modelo de interoperabilidad definido en la UAEGRTD, con el fin de garantizar la confidencialidad, integridad, disponibilidad, autenticación, autorización, auditoria y el no repudio, que se requiere para el intercambio seguro de datos.

La transferencia de información sensible y/o crítica, debe hacerse solo por el personal autorizado.

Se debe documentar y mantener registros de las transferencias de información que incluyan:

- Tipo de información transferida
- Medio utilizado
- Propósito de la transferencia
- Destinatarios
- Fecha y Hora
- Dirección IP
- Usuario
- Transmisión exitosa / fallida
- Tamaño de los datos transmitidos
- Algoritmo de cifrado o firmado

Las transferencias de información deberán ser objeto de una evaluación de riesgos para identificar posibles amenazas y vulnerabilidades asociadas. Se deberán implementar medidas de mitigación adecuadas.

13.2.2 Acuerdos Sobre Transferencia de Información

a. La transferencia de información con terceros debe estar sujeta a acuerdos de confidencialidad, donde se especifiquen las responsabilidades de cada parte en cuanto a la protección de la información transferida.
b. Los acuerdos deberán incluir cláusulas sobre el manejo, almacenamiento y eliminación de la información tras la finalización del acuerdo, así como medidas de seguridad aplicables durante la transferencia.
c. Los acuerdos sobre la transferencia de información deberán revisarse periódicamente para asegurar que sigan cumpliendo con las normativas aplicables y las políticas internas de la UAEGRTD.

13.2.3 Mensajería Electrónica

Está prohibido el uso del correo electrónico corporativo para asuntos diferentes a los relacionados con la misión y actividades relacionados con la UAEGRTD.

a. Las cuentas personales de correo electrónico (Yahoo, Hotmail, Gmail, etc.), deben estar bloqueadas en los equipos de la UAEGRTD. Las excepciones para hacer uso de correo personal deben ser documentadas y justificadas.
b. Solo se asignarán cuentas de correo electrónico institucional a los colaboradores con vínculo laboral o contractual con la UAEGRTD. Las cuentas de correo electrónico son personales intransferibles y de uso exclusivo para el desarrollo de las funciones de cada uno de los colaboradores; por lo tanto, la información gestionada a través de este medio es responsabilidad de cada usuario y debe cumplir con las condiciones de confidencialidad, integridad y disponibilidad reglamentadas en esta política. La información gestionada a través de este medio es propiedad de la UAEGRTD.
c. Con el fin de propender por la movilidad y productividad se permitirá el acceso al correo electrónico desde cualquier lugar a través de internet, siempre y cuando se tenga presente el cuidado de los activos de información que estén bajo su responsabilidad.
d. Está prohibido el uso del correo electrónico en la UAEGRTD en los siguientes casos:
   - Envío o recepción de archivos ejecutables. (ej. exe, bat, etc.)
   - Envío de cadenas de correo, mensajes con contenido religioso, político, racista, pornográfico o cualquier tipo de mensaje que atente contra la integridad de las personas, las leyes y la moral. El correo electrónico institucional no debe usarse para actividades que comprometan la reputación de la Unidad, los activos de información y los recursos de la UAEGRTD.
   - Enviar mensajes mal intencionados que puedan afectar los sistemas internos o de terceros, mensajes que vayan en contra de las leyes, la moral y las buenas costumbres y mensajes que inciten a realizar prácticas ilícitas o promuevan actividades ilegales.
   - Utilizar la dirección de correo electrónico de la UAEGRTD como punto de contacto en comunidades interactivas de contacto social, tales como Facebook, X, Instagram, entre otras, o cualquier otro sitio, a menos que sea utilizado con fines de comunicación, representación en eventos y publicaciones oficiales de la entidad informando siempre al área de Comunicaciones.
   - Enviar información clasificada o reservada a cuentas personales.
   - Enviar información clasificada o reservada a otras entidades sin la autorización escrita correspondiente.

13.2.4 Acuerdos de Confidencialidad o no Divulgación

a. Definir un compromiso de confidencialidad y de no divulgación que incluya el tratamiento de los datos personales y los requisitos establecidos en este documento.
b. Establecer lineamientos para que tanto funcionarios como contratistas firmen el compromiso de confidencialidad y no divulgación.

c. Hacer que todos los contratistas firmen el compromiso de confidencialidad y no divulgación cuando se vinculan a la entidad.

14 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN

14.1 Requisitos de Seguridad en los Sistemas de Información

Objetivo: Asegurar que la seguridad de la información sea una parte integral de los sistemas de información durante todo el ciclo de vida. Esto incluye también los requisitos para sistemas de información que prestan servicios en redes públicas.

14.1.1 Análisis de Requisitos y Especificaciones de Seguridad de la Información

Una parte fundamental del desarrollo, adquisición, implementación o mantenimiento de sistemas de información es la definición clara de los requerimientos, para lo cual se debe tener en consideración:

a. Al interior de la UAEGRTD el área solicitante de un nuevo desarrollo o de una nueva funcionalidad para la mejora de los procesos debe realizar la correspondiente solicitud a la Oficina de Tecnología de la Información de conformidad a las instrucciones reglamentarias internas.
b. Se debe tener en cuenta los requisitos mínimos relacionados con la Seguridad de la Información, que incluyan las exigencias para los nuevos sistemas de información o mejas a los sistemas de información existente.
c. Conjuntamente entre el área solicitante y la Oficina de Tecnología de la Información, realizarán la aprobación final del requerimiento.

14.1.2 Asegurar los Servicios de Aplicaciones en Redes Publicas

Todos los servicios de aplicaciones de la UAEGRTD que pasan sobre redes públicas deben estar protegidos de actividades fraudulentas, disputas contractuales, divulgación y modificaciones no autorizadas. Para lo cual se debe considerar:

a. Implementación de cifrado robusto utilizando protocolos de cifrado fuertes (como TLS/SSL con configuraciones seguras).
b. Autenticación y autorización seguras como autenticación multifactor para verificar la identidad de los usuarios antes de permitir el acceso a los servicios de las aplicaciones.
c. Implementar medidas de seguridad para mitigar riesgos como ataques de Man-in-the-Middle, robo de credenciales, inyección de código y otras vulnerabilidades comunes en entornos de redes públicas.
d. Implementar mecanismos seguros para la gestión de sesiones de usuario, incluyendo la configuración de tiempos de inactividad adecuados, la invalidación segura de sesiones y la protección contra el secuestro de sesiones.
e. Evitar la exposición innecesaria de información sensible en las interfaces públicas de las aplicaciones y en los mensajes de error.
f. Implementar mecanismos de registro y monitoreo de los accesos a los servicios de las aplicaciones desde redes públicas para detectar y responder a actividades sospechosas o no autorizadas.
g. Brindar conciencia y formación a los usuarios sobre los riesgos de seguridad asociados con el acceso a servicios de aplicaciones a través de redes públicas y sobre las medidas de seguridad que deben adoptarse.

14.1.3 Protección de las Transacciones de Servicios de Aplicaciones

La UAEGRTD implementará mecanismos de control para proteger la integridad y confidencialidad de la información durante las transacciones realizadas a través de los servicios de las aplicaciones. Estos mecanismos deben incluir:

a. Métodos de autenticación fuertes para verificar la identidad de los usuarios antes de permitir el acceso y la realización de transacciones.
b. Asegurar que los usuarios solo puedan acceder y realizar las transacciones para las cuales están debidamente autorizados, aplicando el principio de mínimo privilegio.
c. Mecanismos para detectar y prevenir la manipulación no autorizada de los datos durante la transmisión y el procesamiento de las transacciones.
d. Protección de la información sensible involucrada en las transacciones mediante el uso de técnicas de cifrado durante la transmisión (SFTP, VPN, HTTPS) y, cuando sea apropiado, en reposo.
e. Registros detallados de las transacciones, incluyendo la identidad del usuario, la fecha y hora, las acciones realizadas y los datos involucrados. Estos registros deben ser protegidos contra modificaciones no autorizadas y revisados periódicamente para detectar cualquier actividad sospechosa.
f. Implementación de controles para validar los datos de entrada de las transacciones y prevenir errores, inconsistencias y posibles vulnerabilidades de seguridad.
g. Sesiones seguras para las transacciones, incluyendo la implementación de tiempos de espera (timeouts) y la invalidación adecuada de las sesiones.
h. Pruebas de seguridad periódicas en los servicios de las aplicaciones para identificar y abordar posibles vulnerabilidades relacionadas con la protección de las transacciones.

14.2 Seguridad en los Procesos de Desarrollo y Soporte

Objetivo: Asegurar que la seguridad de la información se integre y mantenga a lo largo de todo el ciclo de vida de los sistemas de información, desde su concepción y desarrollo hasta su implementación, mantenimiento y soporte, con el fin de proteger la confidencialidad, integridad y disponibilidad de los activos de información involucrados.

14.2.1 Política de Desarrollo Seguro

El desarrollo seguro de aplicaciones en la UAEGRTD se rige bajo directrices claras que contemplan los siguientes aspectos:

a. Identificación e integración de los requisitos de seguridad relevantes en las etapas iniciales del desarrollo, considerando los riesgos de seguridad de la información y los requisitos normativos y contractuales aplicables.
b. Aplicación de principios de diseño seguro para minimizar las vulnerabilidades inherentes en el software, tales como la defensa en profundidad, el privilegio mínimo y la separación de funciones.
c. Directrices de codificación segura para prevenir vulnerabilidades comunes, como inyecciones de código, desbordamientos de búfer y errores de validación de entrada. Estas directrices deben basarse en estándares de la industria y mejores prácticas.
d. Pruebas de seguridad exhaustivas durante las diferentes etapas del desarrollo, incluyendo pruebas estáticas y dinámicas, análisis de vulnerabilidades y pruebas de penetración, según sea apropiado.
e. Implementar un proceso para identificar, evaluar, clasificar y tratar las vulnerabilidades de seguridad descubiertas durante el desarrollo y después del despliegue.
f. Implementar procedimientos de gestión de cambios seguros para garantizar que las modificaciones al software y a los sistemas de información se realicen de manera controlada y sin introducir nuevas vulnerabilidades.
g. Mantener medidas de seguridad adecuadas para proteger el entorno de desarrollo, incluyendo el control de acceso, la segregación de entornos y la protección contra software malicioso.
h. Promover e implementar y técnicas para que los datos sean adecuadamente seudonimizados o anonimizados considerando todos los elementos de la información que sean sensibles.
i. Proporcionar formación y concientización en desarrollo seguro a todo el personal involucrado en el ciclo de vida del desarrollo de software.

14.2.2 Procedimiento de Control de Cambios en Sistemas

a. Todos los cambios en los sistemas de información e infraestructura deben ser registrados, evaluados, autorizados y comunicados adecuadamente a través de un procedimiento documentado para la gestión de cambios en los sistemas.
b. Todos los cambios realizados a los sistemas serán objeto de pruebas para asegurar que no impactan negativamente en la seguridad de la información. Los cambios no autorizados serán considerados incidentes de seguridad.

14.2.3 Revisión Técnica de las Aplicaciones Después de Cambios en la Plataforma

Después de realizar cambios en la plataforma de producción, debe llevarse a cabo una revisión técnica de las aplicaciones afectadas. Esta revisión debe incluir la verificación de configuraciones de seguridad, la compatibilidad con sistemas existentes y la identificación de vulnerabilidades introducidas por los cambios.

14.2.4 Restricciones a los Cambios en los Paquetes de Software

Ningún paquete de software adquirido externamente debe ser modificados sin una evaluación previa de seguridad. Cualquier modificación debe ser consultada con el área de seguridad de la información y se debe documentar el cambio junto con las justificaciones y las pruebas de seguridad realizadas.

14.2.5 Principios de Construcción de Sistemas Seguros

Todos los sistemas y aplicaciones deben ser diseñados, desarrollados e implementados con principios de seguridad fuerte para reducir las vulnerabilidades y garantizar la protección de la información, considerando:

a. Diseño Seguro: Se deben aplicar principios de diseño seguro en todas las etapas del ciclo de vida de los sistemas de información, incluyendo la definición de requisitos, el diseño arquitectónico, el desarrollo, las pruebas y la implementación.
b. Desarrollo Seguro: Los procesos de desarrollo de software deben incorporar prácticas de codificación segura para prevenir vulnerabilidades comunes (inyecciones SQL, cross-site scripting (XSS) y desbordamientos de búfer) y realizar revisiones de código y pruebas de seguridad durante el desarrollo para identificar y corregir posibles fallos de seguridad.
c. Implementación Segura: Los sistemas de información deben implementarse de manera segura, siguiendo las configuraciones recomendadas y aplicando los controles de seguridad necesarios, documentando los procedimientos de implementación segura y capacitar al personal involucrado.
d. Gestión de Vulnerabilidades: Se debe establecer un proceso para identificar, evaluar y tratar las vulnerabilidades de seguridad en los sistemas de información.
e. Pruebas de Seguridad: Se deben llevar a cabo pruebas de seguridad exhaustivas antes de la puesta en producción de nuevos sistemas o actualizaciones significativas.
f. Documentación de Seguridad: Se debe mantener una documentación clara y actualizada de la arquitectura de seguridad de los sistemas, los controles de seguridad implementados y los procedimientos operativos relacionados con la seguridad.
g. Capacitación: El personal involucrado en el diseño, desarrollo, implementación y mantenimiento de los sistemas de información debe recibir capacitación adecuada en principios de seguridad y prácticas de desarrollo seguro.

14.2.6 Ambiente de Desarrollo Seguro

Para las labores de desarrollo de sistemas se establecerán controles de seguridad para el entorno; los ambientes de desarrollo, prueba y producción deben estar separados. El acceso al entorno de desarrollo estará restringido a personas autorizadas y se utilizarán herramientas de seguridad para detectar vulnerabilidades antes de la implementación de nuevas versiones.

14.2.7 Desarrollo Contratado Externamente

Para los desarrollos de software contratados externamente, debe evaluarse la seguridad y la capacidad de protección de datos del proveedor. En todos los casos se firmarán acuerdos de nivel de servicio (SLA) que incluyan requisitos de seguridad alineados con las políticas la.

14.2.8 Pruebas de Seguridad de Sistemas

Para todos los desarrollos se adelantarán pruebas de seguridad antes de su implementación. Esto incluye pruebas de penetración y análisis de vulnerabilidades. Los hallazgos deben ser mitigados antes de que el sistema sea puesto en producción.

14.2.9 Pruebas de Aceptación de Sistemas

Antes de que un sistema sea aceptado y puesto en producción, se deberá realizar una prueba de aceptación que incluya una revisión de sus funcionalidades y controles de seguridad. La aceptación formal del sistema debe ser documentada, asegurando que cumple todos los requisitos de seguridad establecidos.

14.3 Datos de Prueba

Objetivo: Asegurar la confidencialidad, integridad y disponibilidad de los datos utilizados en las actividades de prueba, minimizando los riesgos asociados a su uso indebido o exposición no autorizada en los entornos de desarrollo y pruebas de la UAEGRTD.

14.3.1 Protección de los Datos de Prueba

a. Certificar que no se revele información confidencial de los ambientes de producción.
b. No usar, durante la ejecución de pruebas en ambientes de desarrollo, datos que contengan información personal o información sensible que esté contenida en el ambiente de producción de los sistemas de información. Cuando se vayan a utilizar se deben anonimizar.
c. Aplicar los procedimientos de control de acceso, tanto a los ambientes de producción, como a los ambientes desarrollo y/o pruebas.
d. Enmascarar la información entregada para las pruebas.

15 RELACION CON PROVEEDORES

15.1 Seguridad en las Relaciones con Proveedores

Objetivo: Establecer y mantener un marco de trabajo seguro para gestionar los riesgos de seguridad de la información asociados con los proveedores y garantizar la protección de los activos de información de la UAEGRTD que son accesibles, procesados o gestionados por terceros, lo cual incluye definir los requisitos de seguridad, implementar controles apropiados y supervisar el cumplimiento para preservar la confidencialidad, integridad y disponibilidad de la información en las relaciones con los proveedores.

15.1.1 Política de Seguridad de la Información para las Relaciones con Proveedores

La UAEGRTD establece y mantiene una política de seguridad de la información que armoniza las expectativas y requisitos en relación con la seguridad para todas las interacciones con proveedores y comprende:

a. Procedimientos para la evaluación inicial y continua de la seguridad de la información de los proveedores, asegurando que cumplan con los estándares de seguridad necesarios antes de la firma de acuerdos.

b. Definición de requisitos mínimos de seguridad que deberán cumplir los proveedores en toda la relación comercial, incluidos controles técnicos, físicos y organizativos.
c. Provisión de formación y concienciación sobre seguridad de la información para los colaboradores (funcionarios / contratistas) que gestionan relaciones con proveedores, asegurando que entienden su responsabilidad en la protección de la información.

15.1.2 Tratamiento de la Seguridad Dentro de los Acuerdos con Proveedores

Los acuerdos con proveedores incluirán cláusulas específicas vinculadas a la seguridad de la información que deben contemplar:

a. **Confidencialidad:** Compromisos claros sobre la confidencialidad de la información que el proveedor pueda acceder y cómo debe ser manejada.
b. **Gestión de Incidentes:** Protocolo de notificación en caso de incidentes de seguridad que comprometan información o sistemas de la UAEGRTD, especificando plazos y procedimientos para la escalación de incidentes.
c. **Derecho de Auditoría:** la UAEGRTD se reserva el derecho de realizar auditorías y evaluaciones regulares en las instalaciones del proveedor, con el fin de verificar el cumplimiento de los requisitos de seguridad establecidos.
d. **Finalización de Contrato:** Provisión sobre el proceso de retorno, destrucción o eliminación de información sensible al finalizar la relación con el proveedor.

Todo contrato con un contratista/proveedor debe incluir una cláusula de confidencialidad o la firma de un acuerdo de confidencialidad, protección de datos, derechos de propiedad intelectual y derechos de autor.

Se deberá dar a conocer a los contratistas/proveedores, las políticas complementarias de seguridad de la información, especialmente la Política de Uso Aceptable de los Activos y Política de Control de Acceso.

En todo contrato se deben identificar los riesgos asociados a los activos de información involucrados en el objeto del contrato.

Durante la etapa post contractual, será obligación del supervisor y/o interventoría asignada, hacer seguimiento a los controles establecidos durante la etapa precontractual y contractual para asegurar la confidencialidad, integridad y disponibilidad de la información, frente a los riesgos previamente identificados.

Al momento del cumplimiento de los requisitos de ejecución, el supervisor debe socializar a los contratistas/proveedores la política para la gestión de incidentes de seguridad de la información y acordar el canal para su debido reporte.

Toda gestión del contratista/proveedor que represente una modificación, mantenimiento, revisión al servicio de tecnología de la información, comunicaciones o equipos de suministros, debe ser objeto de lo establecido en el Procedimiento Gestión de Cambios de la OTI, antes de su ejecución.

Para la contratación de servicios y/o componentes de infraestructura de TI y/o áreas seguras, se debe exigir a los contratistas/proveedores la presentación de los planes de continuidad de negocio que aseguren la disponibilidad de los activos de información y del proceso o servicio suministrado.

Si el proveedor proporciona equipos de cómputo para manejar información de la Unidad, deben seguir las siguientes actividades para la eliminación de información:

a. Disponer de software licenciado para efectuar la eliminación segura de la información residente en los discos duros de los equipos salientes, así mismo, cuando se presenten daños de discos duros durante el plazo de ejecución o para el reemplazo de un equipo de cómputo.
b. Realizar el formateo de los discos duros lo cual debe realizarse antes de retirar los equipos de las instalaciones de la UAEGRTD, la eliminación segura debe realizarse en presencia del personal de mesa de servicio de la UAEGRTD y su asistencia será desde el inicio y hasta el final del procedimiento para verificar su correcta ejecución.

c. Si se trata de un reemplazo de disco duro y se realiza migración de información, los medios utilizados para este fin también deben ser sometidos al mismo procedimiento de eliminación.
d. Certificar la eliminación de la información en el equipo a retirar, en el formato dispuesto para ello.

15.1.3 Cadena de Suministro de Tecnología de Información y Comunicación

La UAEGRTD implementará procesos para gestionar la seguridad de la cadena de suministro relacionada con la tecnología de la información y la comunicación (TIC):

a. **Selección de Proveedores de TIC:** Los proveedores de TIC deberán cumplir con estándares de seguridad apropiados, incluyendo la realización de auditorías y revisiones de seguridad periódicas.
b. **Monitoreo Continuo:** Implementar un mecanismo de monitoreo continuo de la seguridad de la información en la cadena de suministro, garantizando una revisión regular de las relaciones con proveedores y su cumplimiento con las políticas de seguridad de información de la UAEGRTD.

15.2 Gestión de la Presentación de Servicios de Proveedores

Objetivo: Mantener el nivel acordado de seguridad de la información y de prestación del servicio en línea con los acuerdos con los proveedores, gestionando los riesgos asociados a la prestación de servicios por parte de estos, asegurando que la información sensible y crítica se trate con el mismo nivel de seguridad que se aplica internamente. Las relaciones con los proveedores deben establecerse mediante acuerdos claros que incorporen cláusulas de confidencialidad y seguridad de la información.

15.2.1 Seguimiento y Revisión de los Servicios de los Proveedores

a. Se establecerán mecanismos para el seguimiento regular del rendimiento de los proveedores en relación con los servicios contratados, así como su cumplimiento de las políticas de seguridad de la información.
b. Se llevarán a cabo revisiones periódicas de las actividades y controles de seguridad implementados por los proveedores. Estas revisiones se realizarán al menos una vez al año o con la frecuencia necesaria según el nivel de riesgo identificado.

15.2.2 Gestión de Cambios en los Servicios de los Proveedores

a. Los proveedores deben notificar a la UAEGRTD de cualquier cambio significativo en los servicios ofrecidos que pueda afectar la seguridad de la información. Esto incluye cambios en infraestructura, procesos, o personal clave.
b. La UAEGRTD evaluará cualquier cambio notificado para determinar su impacto en la seguridad de la información y en los riesgos asociados. Esta evaluación deberá realizarse antes de aprobar el cambio.
c. Todos los cambios y las evaluaciones asociadas deben ser documentados adecuadamente, manteniendo un registro accesible para auditorías y revisiones.
d. La UAEGRTD revisará y actualizará los acuerdos de servicio (SLA) y los contratos según sea necesario en función de los cambios realizados por los proveedores.

16 GESTION DE INCIDENTES DE SEGURIDAD DE LA INFORMACION

16.1 Gestión de Incidentes de Seguridad de la Información y Mejoras

Objetivo: Establecer un marco de trabajo eficaz para la gestión de incidentes de seguridad de la información, garantizando su identificación, respuesta, tratamiento y aprendizaje continuo, con el fin de minimizar su impacto en la confidencialidad, integridad y disponibilidad de la información y fomentar la mejora continua del sistema de gestión de seguridad de la información.

16.1.1 Responsabilidades y Procedimientos

La gestión de incidentes de seguridad de la información es responsabilidad de todos los colaboradores (funcionarios / contratistas) de la UAEGRTD. Se designará un Equipo de Respuesta a Incidentes (ERI) responsable de la coordinación y gestión de incidentes. Este equipo tendrá las responsabilidades de:

a. Detectar y clasificar los incidentes de seguridad de la información.
b. Implementar y mantener procedimientos documentados para la gestión de incidentes.
c. Realizar revisiones periódicas de los procedimientos y capacitaciones.

16.1.2 Reporte de Eventos de Seguridad de la Información

Todos los colaboradores (funcionarios / contratistas) deben reportar de inmediato cualquier evento de seguridad de la información a su superior y al ERI a través de un canal de comunicación establecido. Se proporcionará capacitación sobre cómo identificar y reportar estos eventos, fomentando una cultura de reporte sin temor a represalias.

16.1.3 Reportes de Debilidades de Seguridad de la Información

Cualquier debilidad identificada en los sistemas de seguridad de la información deberá ser reportada al ERI. Se deberán establecer mecanismos para que los colaboradores (funcionarios / contratistas) puedan informar sobre estas debilidades de manera anónima si lo desean. El ERI evaluará estas debilidades y tomará las medidas adecuadas de mitigación.

16.1.4 Evaluación de Eventos de Seguridad de la Información y Decisiones sobre Ellos

El ERI evaluará todos los eventos reportados para determinar su naturaleza, impacto y severidad. Se establecerá criterio para la priorización de la respuesta a los incidentes, basándose en su potencial de daño a la UAEGRTD. Las decisiones sobre cómo responder se documentarán detalladamente.

16.1.5 Respuestas a Incidentes de Seguridad de la Información

El ERI deberá implementar un plan de respuesta a incidentes que contemple las siguientes acciones:

a. Contener el incidente para minimizar su impacto.
b. Erradicar la causa raíz del incidente.
c. Recuperar los sistemas y servicios afectados y restaurar la operación normal.
d. Informar a las partes interesadas sobre el incidente y la respuesta adoptada.

16.1.6 Aprendizaje Obtenido de los Incidentes de Seguridad de la Información

Después de cada incidente, se realizará una revisión post-incidente para identificar lecciones aprendidas y oportunidades de mejora en los procedimientos existentes. Se generará un informe de revisión que incluirá recomendaciones para evitar reincidencias.

16.1.7 Recolección de Evidencia

Se deberá mantener un protocolo para la recolección de evidencia en caso de un incidente de seguridad. Esta recolección debe realizarse de manera que se preserven la integridad y la cadena de custodia de la evidencia. El ERI será responsable de garantizar que la recolección, almacenamiento y análisis de la evidencia cumpla con la normativa y las regulaciones aplicables.

17 SEGURIDAD DE LA INFORMACION EN GESTION DE CONTINUIDAD DE NEGOCIO

17.1 Continuidad de la Seguridad de la Información

Objetivo: Asegurar la capacidad de continuar las operaciones y mantener la seguridad de la información a un nivel aceptable predefinido durante y después de interrupciones que afecten a la UAEGRTD. Esto implica establecer, implementar y mantener planes, procesos y controles para gestionar incidentes disruptivos y garantizar la disponibilidad, integridad y confidencialidad de la información crítica para el negocio.

17.1.1 Planificación de la Continuidad de la Seguridad de la Información

Identificación de Riesgos. Debe llevarse a cabo un análisis exhaustivo de riesgos para identificar amenazas potenciales que puedan afectar la seguridad de la información. Esto incluirá:

a. Evaluación de impacto en la seguridad de la información.
b. Identificación de activos críticos y sus interdependencias.
c. Determinación de medidas preventivas y de mitigación.

Desarrollo de un Plan de Continuidad. Se desarrollará un Plan de Continuidad de la Seguridad de la Información (PCSI) que deberá incluir:

a. Objetivos de recuperación.
b. Procesos de comunicación en caso de incidentes.
c. Recursos necesarios para la implementación del plan.
d. Definición de roles y responsabilidades.

17.1.2 Implementación de la Continuidad de la Seguridad de la Información

Ejecución del Plan. Se establecerán procedimientos para la implementación del PCSI, que incluirán:

a. Despliegue de controles técnicos y administrativos.
b. Capacitación y concientización del personal respecto a la continuidad de la seguridad de la información.
c. Creación de un equipo de respuesta ante incidentes que conozca el PCSI.

Pruebas y Simulaciones. Se adelantarán pruebas periódicas y simulaciones del PCSI para asegurarse de que:

a. El personal esté familiarizado con los procedimientos.
b. Se identifiquen áreas de mejora.
c. Se verifiquen los tiempos de recuperación y efectividad de los controles implementados.

17.1.3 Verificación Revisión y Evaluación de la Continuidad de la Seguridad de la Información

Se llevarán a cabo auditorías internas a intervalos regulares para evaluar la efectividad del PCSI y el cumplimiento de esta política, sujeto al plan de auditoría establecido por la Unidad.

Revisión Continua. La política de continuidad de la seguridad de la información deberá ser revisada anualmente o siempre que ocurra un cambio significativo en la estructura de la UAEGRTD, los procesos de negocio, o se identifique un nuevo riesgo. Esto incluirá:

a. Revisión de incidentes y lecciones aprendidas.
b. Actualización del análisis de riesgos y del PCSI.

Mejora Continua. Se establecerá un proceso para la identificación e implementación de mejoras en el PCSI, basado en:

a. Resultados de auditorías internas.
b. Revisión de pruebas y simulaciones.
c. Nuevas amenazas y vulnerabilidades identificadas.

17.2 Redundancias

Objetivo: Garantizar la disponibilidad y continuidad de las operaciones críticas de la UAEGRTD ante fallos o interrupciones, mediante la implementación y mantenimiento de redundancias efectivas en la infraestructura tecnológica y los procesos clave de negocio. Esto incluye la duplicación de componentes esenciales, la implementación de mecanismos de conmutación por error y la planificación de la recuperación ante desastres, con el fin de minimizar el impacto de eventos disruptivos y asegurar la reanudación oportuna de las actividades.

17.2.1 Disponibilidad de Instalaciones de Procesamiento de Información

En las instalaciones físicas y virtuales que se utilicen para el procesamiento, almacenamiento y transmisión de información, incluidos centros de datos, servidores, redes, aplicaciones, y cualquier otro recurso asociado, la UAEGRTD gestionará la disponibilidad considerando:

a. Redundancia. Se establecerá mecanismos de redundancia para los sistemas críticos, asegurando que exista un respaldo disponible en caso de falla del sistema primario. Podrán considerarse mecanismos como la duplicación de hardware, aplicaciones y conexiones de red.
b. Planificación de Capacidad. Se realizarán periódicamente análisis de capacidad y planificación de recursos para asegurar que la infraestructura pueda soportar picos de demanda y proporcionar un rendimiento adecuado incluso bajo carga máxima.
c. Mantenimiento. Se implementará un programa de mantenimiento preventivo regular para garantizar que todos los equipos y sistemas funcionen de manera óptima. Esto incluirá actualizaciones de software, parches de seguridad y revisión de hardware.
d. Respaldo de Datos: Se establecerán políticas de respaldo de datos que garanticen la integridad y disponibilidad de la información crítica. Los respaldos se realizarán regularmente y se almacenarán en ubicaciones geográficamente separadas.
e. Plan de Continuidad de Negocio: Se desarrollará y mantendrá un plan de continuidad de negocio que contemple escenarios de falla crítica. Este plan incluirá hojas de ruta, procedimientos de recuperación y asignación de responsabilidades que garanticen la continuidad de las operaciones.

18 CUMPLIMIENTO

18.1 Cumplimiento de los Requisitos Legales y Contractuales

Objetivo: Garantizar que la UAEGRTD identifique, comprenda y cumpla consistentemente con todas las obligaciones legales, estatutarias, regulatorias y contractuales relevantes para la seguridad de la información, protegiendo así sus activos de información y evitando posibles incumplimientos y sus consecuencias.

18.1.1 Legislación Aplicable y Requisitos Contractuales

a. La UAEGRTD está comprometida a identificar y cumplir todas las leyes, regulaciones y normativas relevantes que rigen la seguridad de la información, lo que incluye leyes de protección de datos personales, propiedad intelectual, derechos de autor y normativas sobre privacidad y confidencialidad de la información.
b. La UAEGRTD contará con un responsable de monitorear los requisitos contractuales asociados a la gestión de información de la organización para asegurar que se cumplan las obligaciones legales y contractuales.
c. La UAEGRTD garantiza que todos los contratos y acuerdos con terceros incluyen cláusulas que aborden la seguridad de la información y el cumplimiento de las legislaciones aplicables.

d. La UAEGRTD cuenta con procedimientos para revisar y evaluar los contratos existentes en relación con los requisitos de seguridad de la información y su alineación con las regulaciones pertinentes.

18.1.2 Derechos de Propiedad Intelectual

La UAEGRTD garantiza:

a. Respeto y protección a los derechos de propiedad intelectual, incluyendo, pero no limitándose a derechos de autor, patentes, marcas registradas y secretos comerciales.
b. Que todos los colaboradores (funcionarios / contratistas) sean capacitados sobre la importancia de la propiedad intelectual y las normativas correspondientes.
c. Que todos los colaboradores (funcionarios / contratistas) deben mantener estricta reserva y confidencialidad sobre la información que conozca por causa o con ocasión del cumplimiento de sus obligaciones o funciones, así como, respetar la titularidad de los derechos de autor, en relación con los documentos, obras, creaciones que se desarrollen en su labor y que son propiedad exclusiva de la UAEGRTD.
d. Tomar medidas adecuadas para prevenir el uso no autorizado de los activos de propiedad intelectual de la organización y de terceros.

18.1.3 Protección de Registros

La UAEGRTD cuenta con:

a. Políticas y procedimientos para la creación, uso, almacenamiento, acceso y eliminación de registros que garanticen su integridad, confidencialidad y disponibilidad.
b. Clasificación de registros según su sensibilidad y controles apropiados para proteger la información.
c. Procedimientos para mantener registros de auditoría que documenten el acceso y uso de información crítica para permitir la trazabilidad y el cumplimiento.

18.1.4 Privacidad y Protección de Información de Datos Personales

La UAEGRTD adoptará las siguientes directrices respecto a la protección de datos personales:

a. Cumplir con todas las leyes y regulaciones aplicables relacionadas con la protección de datos personales, incluyendo, pero no limitándose a, la Ley de Protección de Datos Personales correspondiente.
b. Realizar evaluaciones de impacto sobre la privacidad cuando se implementen nuevos proyectos o servicios que puedan afectar la información personal.
c. Garantizar que la recopilación, procesamiento y almacenamiento de datos personales se realice con el consentimiento explícito de los interesados y que se les informe de su derecho a acceder, corregir y borrar sus datos, estableciendo el procedimiento para realizar la autorización de uso de la información, consultas y reclamos de los titulares de los Datos Personales.

18.1.5 Reglamentación de Controles Criptográficos

La UAEGRTD está comprometido con:

a. Implementar controles criptográficos para proteger la confidencialidad, integridad y disponibilidad de la información sensible y de los datos personales.
b. Utilizar tecnologías de cifrado de datos que cumplan con los estándares requeridos para la transmisión y almacenamiento de información.
c. Establecer directrices para la gestión de claves criptográficas, asegurando que estén protegidas y controladas según los principios de confidencialidad y acceso restringido.

18.2 Revisiones de Seguridad de la Información

Objetivo: Asegurar que la seguridad de la información se implemente y opere de acuerdo con las políticas y procedimientos organizacionales.

18.2.1 Revisión Independiente de la Seguridad de la Información

La UAEGRTD llevará a cabo una revisión independiente de la seguridad de la información de manera regular, al menos una vez al año, o con mayor frecuencia si ocurren cambios significativos en el entorno interno o externo que puedan afectar la seguridad de la información.

a. La revisión será realizada por un auditor interno o externo calificado, con experiencia en estándares de seguridad de la información.
b. Los resultados de la revisión se documentarán detalladamente e incluirán conclusiones, recomendaciones y un plan de acción para subsanar cualquier vulnerabilidad identificada.
c. La Alta Dirección será informada sobre los hallazgos de la revisión y el progreso en la implementación de las recomendaciones.

18.2.2 Cumplimiento con las Políticas y Normas de Seguridad

Al interior de la UAEGRTD se establecerá un programa de auditoría interna para verificar el cumplimiento de las políticas y normas de seguridad de la información de la Unidad.

a. Las auditorías se realizarán al menos una vez al año y cubrirán todos los aspectos relacionados con la seguridad de la información, incluyendo la gestión de riesgos, el control de accesos y, la protección de datos.
b. Las no conformidades detectadas durante las auditorías se documentarán y se asignarán a responsables para su resolución en un plazo definido.
c. La Alta Dirección recibirá informes periódicos sobre el estado de cumplimiento y las acciones correctivas implementadas.

18.2.3 Revisión del Cumplimiento Técnico

La UAEGRTD llevará a cabo una revisión técnica de los controles de seguridad de la información de forma regular. Esta revisión incluirá pruebas de penetración, auditorías de configuración y evaluaciones de vulnerabilidad.

a. La revisión técnica permitirá identificar y mitigar riesgos asociados con la infraestructura tecnológica y la disponibilidad de los sistemas de información críticos.
b. Resultados y análisis obtenidos de las revisiones técnicas se documentarán y serán utilizados para mejorar continuamente las medidas de seguridad implementadas.
c. La UAEGRTD se asegurará de que el equipo técnico esté capacitado en las últimas normativas y tecnologías para llevar a cabo efectivamente las revisiones técnicas.

19 CONTROLES ADICIONALES

19.1 Inteligencia Artificial

Objetivo: Asegurar la integridad, disponibilidad y confidencialidad de la información de los procesos de la UAEGRTD al gestionar datos mediante el uso de Inteligencia Artificial (IA), mitigando los riesgos asociados.

a. Asistir a dependencias de la UAEGRTD en los proyectos de tecnología y en los procesos que utilicen Inteligencia Artificial (IA), garantizando la protección de la confidencialidad e integridad de la información utilizada,

b. Analizar de manera previa la información que será gestionada en los proyectos y/o procesos de inteligencia artificial, aplicando los controles necesarios para mitigar la afectación a la confidencialidad, integridad y disponibilidad
c. Aplicar un enfoque de gestión de riesgos de seguridad de la información en cada fase del ciclo de vida del proyecto relacionados con IA.
d. Verificar que los proyectos de Inteligencia Artificial incluyan componentes de educación y capacitación para el personal, fomentando el desarrollo seguro y sostenible de estas tecnologías.

19.2 Analítica de Datos

Objetivo: Hacer recolección, almacenamiento y procesamiento de datos digitales y usar adecuadamente técnicas para la analítica de datos en la UAEGRTD.

a. Definir roles, responsabilidades y accesos para salvaguardar la seguridad de la información utilizada en los procesos de analítica de datos.
b. Establecer métodos seguros para el abastecimiento y recolección de datos en analítica, con el fin de prevenir la fuga de información.
c. Identificar, tratar y hacer seguimiento de riesgos de seguridad de la información que involucren la analítica de datos de la información que se vaya a utilizar.

20 EXCEPCIONES A LA PRESENTE POLÍTICA

Las excepciones a la presente política deberán estar justificadas, documentadas y autorizadas por el Jefe de la Oficina de Tecnologías de la Información. Estas excepciones deben ser revisadas periódicamente para garantizar su adecuado uso. Cabe anotar que estas excepciones serán recopiladas por el dominio de Seguridad de la Información.

21 DOCUMENTOS RELACIONADOS

- GT-GU-12 Metodología de Identificación, Valoración y Clasificación de los Activos de Información
- GT-IN-04 Administración de Usuarios en el Directorio Activo
- GT-FO-32 Aceptación de la Política Complementaria Para el Uso de Dispositivos Personales

22 CONTROL DE CAMBIOS

Versión 7.0

Se realizaron las siguientes modificaciones al documento:

- Se realizó un cambio al documento para alinearlo con los controles del anexo A del estándar ISO 27001:2013 y su numeración estructurada en los 14 dominios y 114 controles del estándar.
- Se robustecieron los conceptos política de seguridad, objetivo, alcance, roles y responsabilidades para su cumplimiento.
- Se crearon lineamientos sobre: aprobación de la política, sanciones y seguimiento.

Participantes en la Elaboración

Carlos de la Ossa – Jefe Oficina - Oficina de Tecnologías de la Información.

César Caro Amaya – Contratista en la función de Oficial de Seguridad – Oficina de Tecnologías de la Información.

Cielo Constanza Lozano D. – Contratista – Oficina de Tecnologías de la Información.

Clasificación de la Información: Publica ☒ Reservada ☐ Clasificada ☐ **Fecha de aprobación**: 2/07/2025

Fecha aprobación Subcomité Técnico de Gobierno y Transformación Digital: 27/06/2025

Fecha aprobación Comité Institucional de Evaluación y Desempeño: 02/07/2025