Ambiente

Manual de Políticas Específicas en Seguridad Privacidad de la Información

Proceso

Gestión Estratégica de Tecnologías de la Información

Versión 2

31/01/2025

TABLA DE CONTENIDO

INTRODUCCIÓN

El Ministerio de Ambiente y Desarrollo Sostenible, en adelante el Ministerio, debe identificar y definir políticas y estándares que faciliten la gestión y la gobernabilidad de TI, a través de un proceso integrado que permita asegurar su cumplimiento e interiorización entre los procesos de la Entidad, asociando la seguridad de la información, adquisición, desarrollo e implantación de sistemas de información, acceso a la tecnología, alineado al Modelo Integrado de Planeación y Gestión determinado en el Decreto 1499 de 2017, que establece el marco de referencia para dirigir, planear, ejecutar, hacer seguimiento, evaluar y controlar la gestión institucional a través de las políticas de gestión y desempeño, como habilitador transversal de los componentes de la política de gobierno digital, que busca que las entidades públicas implementen los lineamientos de seguridad de la información en todos sus procesos, trámites, servicios, sistemas de información, infraestructura y en general, en todos los activos de información con el fin de preservar la confidencialidad, integridad, disponibilidad y privacidad de la información, por medio de la estructura organizativa, políticas, planificación de actividades, roles, responsabilidades, procesos, procedimientos y recursos, para alcanzar los objetivos estratégicos.

En este sentido, el propósito del Sistema de Gestión de Seguridad de la Información es velar por la seguridad y adecuado tratamiento de la información institucional, documentando procesos, procedimientos, manuales, guías y demás que permitan gestionar la administración eficiente del acceso y protección de la información del Ministerio, de tal forma que los activos de información y sus riesgos de seguridad sean identificados, gestionados, asumidos y mitigados por la Entidad de forma documentada, sistemática, estructurada, eficiente y adaptada a los cambios que se produzcan en el entorno, la tecnología, directrices, normatividad y de esta manera fortalecer la continuidad de los servicios de TI, racionalización de recursos, reducción de riesgos e impacto de los incidentes de seguridad.

Teniendo en cuenta lo anterior, el presente manual se encuentra enmarcado por un conjunto de políticas específicas de seguridad de la información adoptadas por la Entidad. Para esto, todas las partes interesadas que tienen responsabilidades sobre la información, fuentes, repositorios y recursos tecnológicos de procesamiento de la información de la Entidad, deben conocer y cumplir con las políticas y directrices contenidas en el presente manual, así como los demás documentos relacionados, en aras de velar por la confidencialidad, integridad y disponibilidad de la información.

1. OBJETIVO

Proporcionar a los funcionarios, contratistas, y demás partes interesadas del Ministerio de Ambiente y Desarrollo Sostenible, las políticas y lineamientos de obligatorio cumplimiento con el fin de gestionar la seguridad de la información asegurando la integridad, confidencialidad y disponibilidad de la información, así como lo relacionado con la privacidad de la información (datos personales).

2. ALCANCE

Este manual inicia con la definición y adopción de las políticas específicas de seguridad y privacidad de la información y aplica a la protección de la información que produce, transforma y almacena el Ministerio, abarcando todos los procesos responsables de los activos de información, los servidores públicos, contratistas, proveedores y partes interesadas.

Este documento se debe revisar y ajustar de forma anual en caso de ser necesario, o cuando en la Entidad surjan cambios importantes que ameriten su actualización.

3. MARCO LEGAL

Resolución 500 de 2021, *"P*or la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la Política de Gobierno Digital".

Directiva Presidencial 02 Del 24 De febrero De 2022, "Para garantizar la implementación segura de la política de gobierno digital liderada por La Entidad de Tecnologías de la Información y las Comunicaciones (MinTIC)"

Ley 1273 de 2009 - Por medio de la cual se modifica el código penal, se crea un nuevo bien jurídico tutelado denominado "De la protección de la Información y de los Datos" y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones

Ley 527 de 1999 - Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las Entidades de certificación y se dictan otras disposiciones.

CONPES 3854 de 2016 Política Nacional de Seguridad Nacional busca fortalecer, identificar, gestionar, tratar y mitigar los riesgos de seguridad digital.

CONPES 3995 de 2020 - Política Nacional De Confianza y Seguridad Digital "Establecer medidas para desarrollar la confianza digital a través de la mejora la seguridad digital de manera que Colombia sea una sociedad incluyente y competitiva en el futuro digital mediante el fortalecimiento de capacidades

y la actualización del marco de gobernanza en seguridad digital, así como con la adopción de modelos con énfasis en nuevas tecnologías"

Norma técnica colombiana 27001 de 2013 Especifica los requisitos necesarios para establecer, implantar, mantener y mejorar un sistema de gestión de la seguridad de la información (SGSI).

El Modelo de Seguridad y Privacidad de la Información – MSPI, conduce a la preservación de la confidencialidad, integridad, disponibilidad de la información, permitiendo garantizar la **privacidad** de los datos, mediante la aplicación de un proceso de gestión del riesgo, brindando confianza a las partes interesadas.

Ley 1581 de 2012, Por medio de la cual se dictan disposiciones generales para la Protección de Datos Personales

Decreto 338 de 2022, establece los lineamientos generales para la gobernanza de seguridad digital, con el cual busca aunar y dinamizar el desarrollo legal, los avances técnicos, así como los conocimientos estatales y privados para fortalecer la ciberseguridad del país.

Resolución 1519 del 2020, "por la cual se definen los estándares y directrices para publicar la información señalada en la Ley 1712 del 2014 y se definen los requisitos en materia de acceso a la información pública, accesibilidad web, seguridad digital, y datos abiertos".

Lineamientos de Mintic, Modelo de Seguridad y Privacidad de la Información 3.0.2 29/07/2021 Manual de Gobierno Digital - Seguridad y privacidad de la información (mintic.gov.co)

DAFP, Guía para la administración del riesgo y el diseño de controles en Entidades públicas Versión 6 noviembre 2022

4. TÉRMINOS Y DEFINICIONES

Acceso a la información pública: Derecho fundamental consistente en la facultad que tienen todas las personas de conocer sobre la existencia y acceso a la información pública en posesión o bajo control de sujetos obligados. (Ley 1712 de 2014, art 4).

Activo: En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de ésta (sistemas, soportes, edificios, personas, etc.) que tenga valor para la Entidad. (ISO/IEC 27000).

Activos de información y recursos: se refiere a 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, operativa y administrativa de cada Entidad, órgano u organismo. (CONPES 3854 de 20116).

Archivo: Conjunto de documentos, sea cual fuere su fecha, forma y soporte material, acumulados en un proceso natural por una persona o Entidad pública o privada, en el transcurso de su gestión, conservados respetando aquel orden para servir como testimonio e información a la persona o institución que los produce y a los ciudadanos, o como fuentes de la historia. También se puede entender como la institución que está al servicio de la gestión administrativa, la información, la investigación y la cultura. (Ley 594 de 2000, art 3).

Amenazas: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la Entidad. (ISO/IEC 27000).

Análisis de riesgo: Proceso para comprender la naturaleza del riesgo y determinar el nivel de dicho riesgo. (ISO/IEC 27000).

Auditoría: Proceso sistemático, independiente y documentado para obtener evidencias de auditoría y obviamente para determinar el grado en el que se cumplen los criterios de auditoría. (ISO/IEC 27000).

Autorización: Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales (Ley 1581 de 2012, art 3).

Bases de datos personales: Conjunto organizado de datos personales que sea objeto de Tratamiento (Ley 1581 de 2012, art 3).

Ciberdefensa: Según CONPES 3701 de 2011 es la capacidad del Estado para prevenir y contrarrestar toda amenaza o incidente de naturaleza cibernética que afecte la soberanía nacional.

Ciberseguridad: Según CONPES 3701 de 2011 es la capacidad del Estado para minimizar el nivel de riesgo al que están expuestos sus ciudadanos, ante amenazas o incidentes de naturaleza cibernética.

CIGD: Comité Institucional de Gestión y Desempeño

Control: Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.

Confidencialidad: Según la norma ISO/IEC 27002:2013 es la propiedad de la información de no ponerse a disposición o ser revelada a individuos, Entidades o procesos no autorizados.

Credencial de grupo: Conjunto de identificadores de usuarios y contraseñas que son asignados a un grupo de servidores públicos o contratistas, con un propósito particular, para el acceso a un Sistema de Información o Servicio de la Entidad.

Credencial de usuario: Conjunto de identificadores de usuarios y contraseñas que son asignados a una persona de manera única e intransferible con el propósito de acceder a un Sistema de Información o Servicio dentro de la Entidad.

Criptografía: Es la ciencia que resguarda documentos y datos que actúa a través del uso de las cifras o códigos para escribir algo secreto en documentos y datos que se aplica a la información que circulan en las redes locales o en internet.

Datos abiertos: Son todos aquellos datos primarios o sin procesar, que se encuentran en formatos estándar e interoperables que facilitan su acceso y reutilización, los cuales están bajo la custodia de las Entidades públicas o privadas que cumplen con funciones públicas y que son puestos a disposición de cualquier ciudadano, de forma libre y sin restricciones, con el fin de que terceros puedan reutilizarlos y crear servicios derivados de los mismos (Ley 1712 de 2014, art 6).

Datos personales: Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables. (Ley 1581 de 2012, art 3).

Datos personales públicos: Es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva. (Decreto 1377 de 2013, art 3).

Datos personales privados: Es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular. (Ley 1581 de 2012, art 3 literal h).

Datos personales mixtos: Para efectos de este documento es la información que contiene datos personales públicos junto con datos privados o sensibles.

Datos personales sensibles: Se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier

partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual, y los datos biométricos. (Decreto 1377 de 2013, art 3).

Derecho a la intimidad: Derecho fundamental cuyo núcleo esencial lo constituye la existencia y goce de una órbita reservada en cada persona, exenta de la intervención del poder del Estado o de las intromisiones arbitrarias de la sociedad, que le permite a dicho individuo el pleno desarrollo de su vida personal, espiritual y cultural (Jurisprudencia Corte Constitucional).

Desastre: Cualquier evento accidental, natural o malintencionado que interrumpe las operaciones o servicios habituales de una organización durante el tiempo suficiente como para verse la misma afectada de manera significativa.

Disponibilidad: Según la norma ISO/IEC 27002:2013 Propiedad de la información de estar accesible y utilizable cuando lo requiera una Entidad autorizada.

Encargado del tratamiento de datos: Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el Tratamiento de datos personales por cuenta del responsable del Tratamiento. (Ley 1581 de 2012, art 3).

Gestión de incidentes de seguridad de la información: Procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información. (ISO/IEC 27000).

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 y los derechos particulares o privados consagrados en el artículo 18 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6).

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. (Ley 1712 de 2014, art 6).

Integridad: En consideración a la norma ISO/IEC 27002:2013 es la propiedad de la información relativa a su exactitud y completitud.

Ley de transparencia y acceso a la información pública: Se refiere a la Ley Estatutaria 1712 de 2014.

Mecanismos de protección de datos personales: Lo constituyen las distintas alternativas con que cuentan las Entidades destinatarias para ofrecer protección a los datos personales de los titulares tales como acceso controlado, anonimización o cifrado.

OTIC: Oficina de Tecnologías de la Información y la Comunicación.

Plan de continuidad del negocio: Plan orientado a permitir la continuación de las principales funciones misionales o del negocio en el caso de un evento imprevisto que las ponga en peligro. (ISO/IEC 27000).

Plan de tratamiento de riesgos: Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma. (ISO/IEC 27000).

Privacidad: la correlativa obligación de proteger dicha información en observancia En el contexto de este documento, por privacidad se entiende el derecho que tienen todos los titulares de la información en relación con la información que involucre datos personales y la información clasificada que estos hayan entregado o esté en poder de la Entidad en el marco de las funciones que a ella le compete realizar y que generan en las Entidades destinatarias del Manual de del marco legal vigente.

Registro nacional de bases de datos - RNBD: Directorio público de las bases de datos sujetas a tratamiento que operan en el país. (Ley 1581 de 2012, art 25).

Responsabilidad demostrada: Conducta desplegada por los responsables o encargados del tratamiento de datos personales bajo la cual a petición de la Superintendencia de Industria y Comercio debe estar en capacidad de demostrarle a dicho organismo de control que han implementado medidas apropiadas y efectivas para cumplir lo establecido en la Ley 1581 de 2012 y sus normas reglamentarias.

Responsable del tratamiento de datos: Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el Tratamiento de los datos. (Ley 1581 de 2012, art. 3).

Riesgo: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000).

Seguridad de la información: Preservación de la confidencialidad, integridad, y disponibilidad de la información en cualquier medio: impreso o digital. (ISO/IEC 27000).

Seguridad digital: Preservación de la confidencialidad, integridad, y disponibilidad de la información que se encuentra en medios digitales.

Titulares de la información: Personas naturales cuyos datos personales sean objeto de Tratamiento. (Ley 1581 de 2012, art 3).

Tratamiento de datos personales: Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión. (Ley 1581 de 2012, art 3).

Trazabilidad: Cualidad que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sean asociadas de modo inequívoco a un individuo o Entidad. (ISO/IEC 27000).

Vulnerabilidad: Debilidad de un activo o control que puede ser explotada por una o más amenazas. (ISO/IEC 27000).

Partes interesadas (Stakeholder): Persona o Entidad que puede afectar a, ser afectada por, o percibirse a sí misma como afectada por una decisión o actividad.

5. POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

5.1. Orientación de la Dirección para la Gestión de la Seguridad de la Información

5.1.1. Políticas para la seguridad de la información

Control: Definir un conjunto de políticas para la seguridad de la información, aprobada por la dirección, publicada y comunicada a los empleados y partes externas pertinentes.

- La OTIC, debe definir la Política General de Seguridad de la Información, la cual debe ser presentada para aprobación del Comité Institucional de Gestión y Desempeño y posteriormente socializarla y publicarla en la sede electrónica y en la herramienta del Sistema Integrado de Gestión.

- La OTIC, debe definir el Manual de Políticas Específicas de Seguridad y Privacidad de la Información y posteriormente socializarla y publicarla en la sede electrónica y en la herramienta del Sistema Integrado de Gestión.

- La OTIC, definir la Política de Tratamiento y Protección de Datos Personales, enviar a revisión de la Oficina Asesora Jurídica, posteriormente debe ser presentada para aprobación del Comité Institucional de Gestión y Desempeño y posteriormente socializada y publicada en la sede electrónica y en la herramienta del Sistema Integrado de Gestión.

5.1.2. Revisión de las políticas para seguridad de la información

Control: La verificación y revisión de las políticas específicas de seguridad de la información que se encuentran en este documento se debe revisar por lo menos una vez al año o cuando ocurran cambios en la Entidad o en el entorno legal de la misma.

- La OTIC debe revisar y actualizar anualmente o cuando se requiera el Manual de Políticas Específicas de Seguridad y Privacidad y la Política General de Seguridad.

- La OTIC debe revisar y actualizar anualmente o cuando se requiera la Política de Tratamiento y Protección de Datos Personales o en caso de presentarse nuevos lineamientos, requerimientos legales o directrices internas o externas que así lo indiquen.

6. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

6.1. Organización Interna

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

- La OTIC, debe liderar la adopción e implementación del Sistema de Gestión de Seguridad de la Información - SGSI en todos los Procesos de la Entidad (Estratégicos, Misionales, Apoyo y de Evaluación).

6.1.1. Roles y responsabilidades para la seguridad de la información

Control: Definir y asignar todas las responsabilidades de la seguridad de la información.

Se definen los siguientes roles y responsabilidades de acuerdo con los lineamientos, directrices y normatividad aplicable en materia de seguridad de la información.

Comité Institucional de Gestión y Desempeño (CIGD)

- La Entidad mediante la Resolución 2140 del 19 de oct de 2017, por la cual adopta el Modelo Integrado de Planeación y Gestión y el Comité Institucional de Gestión y Desempeño, y que tiene como función, entre otras, “asegurar la implementación y desarrollo de las políticas de gestión y directrices en materia de seguridad digital y de la información impartidas por la Presidencia de la Republica y el Ministerio de Tecnologías de la Información y las Comunicaciones”.
- Responsable de aprobar la documentación de su competencia, que surja frente a la implementación del SGSI.
- Gestionar los recursos necesarios para la implementación y sostenibilidad transversal del Modelo de Seguridad y Privacidad de la Información – MSPI de la Entidad.
- Aprobar y apoyar la implementación de los planes, programas, proyectos, estrategias y herramientas necesarias para el fortalecimiento y cumplimiento de las políticas de seguridad de la información.
- Apoyar y fortalecer la adoptación de la cultura de seguridad de la información al interior de la Entidad.
- Aprobar acciones y mejores prácticas que se requieran en la implementación del MSPI.
- Adoptar las decisiones que permitan la gestión y minimización de riesgos críticos de seguridad de la información.
- Las demás que tengan relación con el estudio, análisis y recomendaciones en materia de seguridad y privacidad de la información.

Oficina de Tecnologías de la Información y Comunicaciones (OTIC) – Seguridad de la Información:

- Asesorar a la Entidad en el diseño, implementación y mantenimiento del Modelo de Seguridad y Privacidad de la Información para la Entidad de conformidad con la regulación vigente.
- Identificar brechas en el Modelo de Seguridad y Privacidad de la Información – MSPI y la situación actual de la Entidad.
- Realizar la planificación y seguimiento a los cronogramas de la implementación del MSPI. (Planes).
- Definir, elaborar e implementar políticas, procedimientos, estándares o documentos que sean de su competencia para la operación del MSPI.
- Brindar acompañamiento a los procesos, áreas o dependencias en materia de seguridad y privacidad de la información (según solicitud).
- Definir, elaborar, actualizar y socializar la metodología para la gestión de activos de información y riesgos de seguridad de la información de la Entidad.
- Acompañar a los procesos en la identificación o actualización de los activos de información.
- Acompañar a los procesos de la Entidad en la gestión de riesgos de seguridad y privacidad de la información, así como en la identificación de los controles para su mitigación y plan de tratamiento de riesgos.
- Consolidar y gestionar la publicación del registro de activos de información.
- Gestionar la validación, aprobación y publicación del Índice de Información Clasificada y Reservada.
- Definir e implementar la estrategia de sensibilización y divulgación en materia de seguridad y privacidad de la información para los servidores públicos y contratistas de la Entidad.
- Definir, socializar e implementar el procedimiento de Gestión de Incidentes de seguridad de la información.
- Acompañar a la Alta Dirección, para asegurar el liderazgo y cumplimiento de los roles y responsabilidades de los líderes de los procesos en materia de seguridad y privacidad de la información.
- Informar a los responsables de los procesos cuando se detecten irregularidades, incidentes o prácticas que atenten contra la seguridad y privacidad de la información de acuerdo con la normativa vigente.
- Custodiar la documentación e información que por razón de su rol conserve bajo su cuidado o a la cual tenga acceso, e impedir o evitar la sustracción, destrucción, ocultamiento o utilización indebida.

Oficina Asesora de Planeación

- Asesorar, orientar y apoyar al Despacho, Vice Despachos, Direcciones, Subdirecciones Oficinas y Grupos de Trabajo de la Entidad, en los temas relacionados con la realización, actualización o ajustes de los procedimientos, procesos, guías, formatos y manuales para

alinearlos con el Sistema Integrado de Gestión. De igual manera orientarlas en la Administración del Riesgo, realizando la revisión, análisis y consolidación de la información.
- Ejecutar, presentar y socializar a quien corresponda, los resultados de las auditorías en materia del Sistema de Gestión de Seguridad de la Información.
- Implementar los controles de seguridad de la información para sus activos de información, contará con el acompañamiento de la Oficina de Tecnologías de la Información y Comunicaciones, cuando sea solicitado.
- Custodiar y cuidar la documentación e información que por razón de su rol conserve bajo su cuidado o a la cual tenga acceso, e impedir o evitar la sustracción, destrucción, ocultamiento o utilización indebida.
- Tratar y salvaguardar la información de datos personales de los servidores públicos, contratistas y proveedores, en concordancia con sus funciones y la normatividad vigente.

Grupo de Talento Humano

- Controlar y salvaguardar la información del personal de planta de la Entidad, según la normatividad vigente.
- Reportar oportunamente a la OTIC las diferentes situaciones administrativas que se presenten, con el fin de gestionar el control de acceso a los diferentes sistemas de información y recursos tecnológicos de los usuarios.
- Implementar controles de seguridad de la información para sus activos, para lo cual contará con el acompañamiento de la **Oficina de Tecnologías de la Información y Comunicaciones**, cuando sea solicitado.
- Custodiar y cuidar la documentación e información que por razón de su rol conserve bajo su cuidado o a la cual tenga acceso, impedir o evitar la sustracción, destrucción, ocultamiento o utilización indebida.
- Implementar y custodiar los acuerdos de confidencialidad y de no divulgación de información en los actos administrativos de toma de posesión de cargos de los servidores públicos y demás documentos equivalentes que así lo requieran.
- Tratar y salvaguardar la información de datos personales de los servidores públicos de la Entidad, en concordancia con sus funciones y la normatividad vigente.

Oficina Asesora Jurídica

- Brindar asesoría a los procesos de la entidad en temas jurídicos y legales que involucren acciones ante las autoridades competentes relacionados con seguridad y privacidad de la información.
- Brindar asesoría al Comité Institucional de Gestión y Desempeño en materia de temas normativos, jurídicos y legales vigentes que involucren acciones ante las autoridades competentes relacionados con seguridad y privacidad de la información.
- Representar a la Entidad en procesos judiciales ante las autoridades competentes relacionados con seguridad y privacidad de la información

- Apoyar y asesorar a la Entidad frente al Índice de Información Clasificada y Reservada de los activos de información de acuerdo con la regulación vigente.
- Apoyar la construcción y automatización de los campos de clasificación de la información definidos en la matriz de activos de información conforme a la Ley 1712 de 2014, Transparencia y Acceso a la Información Pública.
- Asistir a las mesas de trabajo que se requieran para el levantamiento o actualización de los activos de información de su proceso y de los demás procesos de la Entidad.
- Validación del Índice de Información Clasificada y Reservada de todos los procesos y dependencias para presentarlo al Comité Institucional de Gestión y Desempeño para su respectiva aprobación.
- Implementar los controles de seguridad de la información para sus activos de información, contará con el acompañamiento de la Oficina de Tecnologías de la Información y Comunicaciones, cuando sea solicitado.
- Custodiar y cuidar la documentación e información que por razón de su rol conserve bajo su cuidado o a la cual tenga acceso, e impedir o evitar la sustracción, destrucción, ocultamiento o utilización indebida.
- Tratar y salvaguardar la información de datos personales que, con motivo del ejercicio de sus funciones, requiera recolectar, almacenar, gestionar, según la normatividad vigente.

Grupo de Contratos

- Responsable de la inclusión y actualización del clausulado con temas de seguridad de la información en los contratos a su vez son responsables del reporte oportuno a quien corresponda de la vinculación, finalización, terminación anticipada, terminación unilateral, cesión, entre otras novedades, con el fin de que la OTIC pueda gestionar la suspensión del acceso o privilegios a los diferentes sistemas de información y recursos tecnológicos.
- Verificar que los contratos o convenios de ingreso que por competencia deban suscribir los procesos, cuenten con cláusulas de derechos de autor, confidencialidad y no divulgación de la información según sea el caso.
- Implementar los controles de seguridad de la información para sus activos de información, contará con el acompañamiento de la **Oficina de Tecnologías de la Información y Comunicaciones**, cuando sea solicitado.
- Custodiar y cuidar la documentación e información que por razón de su rol conserve bajo su cuidado o a la cual tenga acceso, e impedir o evitar la sustracción, destrucción, ocultamiento o utilización indebida.
- Implementar y custodiar los acuerdos de confidencialidad y de no divulgación de información en los contratos de los contratistas y proveedores y demás documentos equivalentes que así lo requieran.
- Tratar y salvaguardar la información de datos personales de los contratistas y proveedores de la Entidad, en concordancia con sus funciones y la normatividad vigente.

Grupo de Comunicaciones

- Apoyar la elaboración y envío de piezas de comunicativas, boletines, noticias, socializaciones y demás relacionados con seguridad de la información.
- Realizar la publicación del registro de activos de información en la sede electrónica de la Entidad conforme a la solicitud realizada por parte del responsable de seguridad de la información.
- Implementar los controles de seguridad de la información para sus activos de información, contará con el acompañamiento de la **Oficina de Tecnologías de la Información y Comunicaciones**, cuando sea solicitado.
- Custodiar y cuidar la documentación e información que por razón de su rol conserve bajo su cuidado o a la cual tenga acceso, e impedir o evitar la sustracción, destrucción, ocultamiento o utilización indebida.
- Tratar y salvaguardar la información de datos personales que, con motivo del ejercicio de sus funciones, requiera recolectar, almacenar, gestionar, según la normatividad vigente.

Grupo de Gestión Documental

- Orientar a los procesos respecto a la gestión documental para identificar la clasificación de los activos tipo información relacionados con las Tablas de Retención Documental (TRD).
- Realizar el acompañamiento a los líderes y facilitadores de cada proceso respecto a la clasificación documental de la información.
- Implementar los controles de seguridad de la información para sus activos de información, contará con el acompañamiento de la **Oficina de Tecnologías de la Información y Comunicaciones**, cuando sea solicitado.
- Custodiar y cuidar la documentación e información que por razón de su rol conserve bajo su cuidado o a la cual tenga acceso, e impedir o evitar la sustracción, destrucción, ocultamiento o utilización indebida.
- Tratar y salvaguardar la información de datos personales que, con motivo del ejercicio de sus funciones, requiera recolectar, almacenar, gestionar, según la normatividad vigente.

Grupo de Control Interno Disciplinario

- Responsable de emprender acciones contra los servidores públicos que hayan cometido una violación a la seguridad de la información. Para lo que tiene estos procedimientos: P-A-DIS-01 Indagación Preliminar, **P-A-DIS-02** Investigación Disciplinaria, **P-A-DIS-03** Juzgamiento (Pliego de Cargos), **P-A-DIS-04** Segunda Instancia, **P-A-DIS-05** Disciplinario Verbal y la Ley 734 de 2002.
- Implementar los controles de seguridad de la información para sus activos de información, contará con el acompañamiento de la **Oficina de Tecnologías de la Información y Comunicaciones**, cuando sea solicitado.

- Custodiar y cuidar la documentación e información que por razón de su rol conserve bajo su cuidado o a la cual tenga acceso, e impedir o evitar la sustracción, destrucción, ocultamiento o utilización indebida.
- Tratar y salvaguardar la información de datos personales que, con motivo del ejercicio de sus funciones, requiera recolectar, almacenar, gestionar, según la normatividad vigente.

Unidad Coordinadora de Gobierno Abierto (UCGA)

- Gestionar la publicación del registro de activos de información en el portal de datos abiertos conforme a la solicitud realiza por parte de la OTIC.
- Implementar los controles de seguridad de la información para sus activos de información, contará con el acompañamiento de la **Oficina de Tecnologías de la Información y Comunicaciones**, cuando sea solicitado.
- Custodiar y cuidar la documentación e información que por razón de su rol conserve bajo su cuidado o a la cual tenga acceso, e impedir o evitar la sustracción, destrucción, ocultamiento o utilización indebida.
- Tratar y salvaguardar la información de datos personales que, con motivo del ejercicio de sus funciones, requiera recolectar, almacenar, gestionar, según la normatividad vigente.

Oficina de Control Interno

- Generar las recomendaciones y sugerencias que contribuyan al mejoramiento y optimización respecto a la gestión permanente de la Seguridad de la Información de la Entidad en caso de ser necesario.
- Implementar los controles de seguridad de la información para sus activos de información, contará con el acompañamiento de la **Oficina de Tecnologías de la Información y Comunicaciones**, cuando sea solicitado.
- Custodiar y cuidar la documentación e información que por razón de su rol conserve bajo su cuidado o a la cual tenga acceso, e impedir o evitar la sustracción, destrucción, ocultamiento o utilización indebida.
- Tratar y salvaguardar la información de datos personales que con ocasión del ejercicio de sus funciones requiera recolectar, almacenar, gestionar, de conformidad con la normatividad vigente.

Grupo de Servicios Administrativos

- Gestionar, implementar, controlar y supervisar los controles de acceso y seguridad física y del entorno como tipo biométrico, tarjeta de proximidad o similares en la Entidad.
- Gestionar y apoyar la implementación, seguimiento y supervisión de los controles de seguridad física en las oficinas, zonas de descarga, parqueaderos y centros de procesamiento y almacenamiento de información.

- Gestionar, implementar, controlar y supervisar los mecanismos de identificación para el acceso a la Entidad de los servidores públicos, contratistas, proveedores y ciudadanía en. general.
- Tratar y salvaguardar la información de datos personales que, con motivo del ejercicio de sus funciones, requiera recolectar, almacenar, gestionar, según la normatividad vigente.

Servidores Públicos, Contratistas y Proveedores

- Dar cumplimiento a los manuales, procedimientos, lineamientos y políticas del Sistema de Gestión de Seguridad de la Información.
- Custodiar y cuidar la documentación e información que por razón de su empleo, cargo o funciones conserve bajo su cuidado o a la cual tenga acceso, e impedir o evitar la sustracción, destrucción, ocultamiento o utilización indebida.
- Reportar inmediatamente los eventos o incidentes de seguridad de la información mediante la herramienta de mesa de asistencia.
- Dar cumplimiento a la Política de tratamiento y protección de datos personales de la Entidad.
- Aceptar, firmar y cumplir los acuerdos de confidencialidad y de no divulgación de la información.
- Participar en las sensibilizaciones y capacitaciones programadas en el marco del Sistema de Gestión de Seguridad de la Información.
- Mantener la confidencialidad de la información con terceros y fuera de la Entidad.
- Violar o incumplir las responsabilidades y lineamientos definidos en el Manual de políticas de seguridad de la información será causa de la aplicación de las acciones disciplinarias a que haya lugar.
- Clasificar la información e implementar los controles pertinentes de acuerdo con el nivel de confidencialidad, integridad y disponibilidad que se requiera.
- No se permite instalar ningún tipo de software en los equipos institucionales, sin la debida autorización y aprobación de la Oficina de Tecnologías de la Información y Comunicaciones.
- Hacer uso racional y ético de los servicios de TI tales como: internet, telefonía, aplicativos, herramientas colaborativas, correo electrónico y demás provistos por la Entidad, los cuales están dispuestos al debido cumplimiento de sus funciones y actividades contractuales, so pena de las acciones disciplinarias o legales a que haya lugar.
- Tratar y salvaguardar la información de datos personales que, con motivo del ejercicio de sus funciones u obligaciones, requiera recolectar, almacenar, gestionar, según la normatividad vigente.

6.1.2. Segregación de funciones

Control: Los deberes y áreas de responsabilidad en conflicto se debe separar para reducir las posibilidades de modificación no autorizada o no intencional, o el uso indebido de los activos de la Entidad.

- Se debe definir e implementar controles para la gestión efectiva de la separación de deberes o funciones cuando ello sea necesario por razones de seguridad, para reducir las posibilidades de modificación no autorizada o no intencional, o el uso indebido de los activos, conforme a las necesidades de la Entidad.

6.1.3. Contacto con las autoridades

Control: Se debe mantener los contactos apropiados con las autoridades pertinentes.

- La Entidad debe mantener contacto actualizado con las autoridades competentes para el cumplimiento de la Ley; como los organismos de control tales como el CSIRT Presidencia, CSIRT de Gobierno, ColCERT, Policía Nacional, Bomberos, fiscalía general de la Nación, Entidades de servicios públicos.
- En caso de presentarse incidentes de seguridad de la información, el servidor público, contratista o proveedor debe informar a la Oficina de Tecnologías de la Información y Comunicaciones por medio de la herramienta de mesa de asistencia, y la OTIC escalará de ser necesario a los organismos de control del Estado o autoridades competentes, por lo cual se para que el responsable de seguridad de la información informe a quien corresponda o se tomen las acciones pertinentes, para lo cual se tiene aprobado y publicado **DS-E-GET-03** Contacto con Autoridades y Grupos de Interés y **P-A-GTI-11** Gestión de la Operación de Servicios Tecnológicos.

Tabla 1: Contacto con las autoridades.

ENTIDAD	CONTACTO
Fiscalía General de la Nación	pqrs@fiscalia.gov.co
Policía Nacional	caivirtual@correo.policia.gov.co
CSIRT Presidencia	(601) 5629300 ext 3309 CSIRT@presidencia.gov.co segdig-gtd@presidencia.gov.co
CSIRT de Gobierno	CSIRTgob@mintic.gov.co 01 8000 910742 Opción 3
Comando Conjunto Cibernético	Correo: info@ccoc.mil.co Teléfono: (601) 315 0111 Ext. 21131

ENTIDAD	CONTACTO
COLCERT	**Línea de atención - 601** 570 20 00 **Contacto@**ColCERT.gov.co
Cuadrante 14 de Policía	Teléfono 311 6014726
CAI San Diego	Teléfono 301 7532915
CODENSA	Teléfono (115) o 601 5115115
Gas Natural - VANTI	Teléfono (164) y/o 315 2386788
ETB	Teléfono 601 3777777
Acueducto y Alcantarillado	Teléfono (116) o 601 3779500
Bomberos	Teléfono (119) o 601 5115115
Emergencias Médicas	Teléfono (125)
Cruz Roja	Teléfono (132)

6.1.4. Contacto con grupos de interés especial

Control: Es conveniente mantener contactos con grupos de interés especial u otros foros y asociaciones profesionales especializadas en seguridad.

- La Entidad a través de la OTIC debe mantener contacto con grupos de interés especial, foros y asociaciones profesionales en el campo de la seguridad de la información, con el fin de mantenerse actualizado en relación con la información de seguridad.
- La Entidad a través de la OTIC debe gestionar su participación en grupos de interés tales como:
  - Centro Cibernético Policial – CCP
  - CAI Virtual
  - Grupo de Respuesta a Emergencias Cibernéticas de Colombia (ColCERT),
  - CSIRT Presidencia y el Comando Conjunto Cibernético de las FFMM - CCOC.

6.1.5. Seguridad de la información en la gestión de proyectos

Control: La seguridad de la información se debe tratar en la gestión de proyectos, independientemente del tipo de proyecto.

- La OTIC debe establecer lineamientos de seguridad de la información para el desarrollo seguro de proyectos de TI.
- La seguridad de la información se debe tratar en la gestión de proyectos, independientemente del tipo de proyecto.
- Verificar el cumplimiento de la Ley de Protección de Datos Personales cuya responsabilidad es de las partes internas y externas involucradas en el proyecto.
- Los proyectos que incluyan desarrollo de sistemas de información o aplicativos, deben llevar a cabo buenas prácticas de desarrollo seguro y pruebas de vulnerabilidades, para gestionar las debilidades de seguridad que se puedan presentar durante el ciclo de vida de estos.

6.2. Dispositivos Móviles y Teletrabajo

Objetivo: Garantizar la seguridad del teletrabajo y el uso de dispositivos móviles.

6.2.1 Política para dispositivos móviles

Control: La Entidad debe adoptar una política para uso de dispositivos móviles y unas medidas de seguridad de soporte, para gestionar los riesgos introducidos por el uso de estos dispositivos.

- El Ministerio debe definir el protocolo de seguridad para el ingreso y salida de elementos y dispositivos móviles. **G-A-GSA-03** Protocolo de Seguridad Ministerio de Ambiente y Desarrollo Sostenible (Seguridad física y del Entorno). La OTIC debe definir lineamientos de operación para el uso de dispositivos móviles.
- Todos Los servidores públicos, contratistas y proveedores de la Entidad que accedan a información de la Entidad con dispositivos móviles debe implementar controles de acceso, y los demás controles que se consideren necesarios para garantizar la confidencialidad, integridad y disponibilidad de la información.
- Los servidores públicos, contratistas y proveedores de la Entidad deben usar las contraseñas de acceso, aplicando los lineamientos para generación de estas.
- No se debe descargar, almacenar o modificar información de la cual no se tenga autorización expresa por parte del propietario.
- Los funcionarios, contratistas y proveedores deben participar en las campañas de concientización sobre temas de riesgos, seguridad de la información y demás adelantadas por la Entidad.

- No compartir sus contraseñas con otras personas, ni dejarlas en lugares visibles de fácil acceso.
- Cumplir los lineamientos técnicos (mínimos) establecidos por la entidad para los dispositivos móviles o estaciones de trabajo que se emplearan para el teletrabajo. Dichos lineamientos entre otros estarán enfocadas a sistema operativo, herramienta de antivirus, capacidad del disco duro, ancho de banda de internet y demás aplicables de seguridad y salud en el trabajo.
- Permitir los procesos de actualización de aplicaciones y sistemas operativos de los dispositivos móviles usados para el teletrabajo.
- La protección física se encuentra a cargo del Grupo de servicios administrativos, mediante la aplicación de controles físicos tales como: sistema de videovigilancia, controles de ingresos y salidas físicas, contratos de vigilancia, entre otros, se encuentran en **G-A-GSA-03** Protocolo de Seguridad Ministerio de Ambiente y Desarrollo Sostenible.
- Restricciones para la instalación de software por medio de la aplicación de las políticas en el directorio activo en los equipos de la entidad.
- Restricción de la conexión a servicios de información por medio de los controles de seguridad aplicados para los diferentes perfiles de usuarios.
- Controles de acceso por medio de la aplicación de las políticas en el directorio activo.
- Se realizará protección contra software malicioso con la gestión del antivirus y el sistema de seguridad perimetral implementado en la Entidad.
- Se debe realizar desconexión remota o cierre por medio de la aplicación de las políticas y herramientas con que cuente la Entidad.
- Hacer uso de las herramientas colaborativas institucionales por medio de las cuales se podrá respaldar la información que estimen pertinentes.
- El uso de dispositivos móviles que interactúen con la infraestructura de procesamiento o información de la Entidad, se habilitará previa solicitud del responsable o líder, para aquellos colaboradores cuyo perfil, cargo y funciones lo requieran.
- Los servidores públicos, contratistas y proveedores que hagan uso de sus dispositivos móviles, se comprometen a asegurarlo física y lógicamente a fin de no poner en riesgo la información de la Entidad.
- Los servidores públicos, tener acceso a la información desde redes externas al Ministerio, debe solicitar a la OTIC la contratistas y proveedores autorizados para el uso de dispositivos móviles en la entidad, que requieran asignación de conexiones seguras (VPN). Estos recursos tecnológicos y de seguridad para las conexiones externas, debe ser suministrados por la Oficina de Tecnologías de la Información y Comunicaciones de acuerdo con la disponibilidad de estas.
- Se prohíbe el uso de herramientas de acceso remoto de terceros, las cuales no cuenten con el debido licenciamiento de la Entidad o del proveedor que así lo requiera.
- Los servidores públicos, contratistas y terceros no debe modificar las configuraciones de seguridad de los dispositivos móviles institucionales, ni instalar programas no autorizados, ni cambiar las configuraciones de software con las que fueron entregados por la Entidad.

- Los visitantes que requieran acceder a los servicios tecnológicos a través de dispositivos móviles deben hacer el registro de ingreso del dispositivo (computador portátil, tableta u otro) en la portería peatonal o vehicular.

6.2.2 Teletrabajo

Control: Se debe implementar una política y unas medidas de seguridad de soporte, para proteger la información a la que se tiene acceso, que es procesada o almacenada en los lugares en los que se realiza teletrabajo.

- La Entidad establece los lineamientos de seguridad de la información que debe ser aplicados en la modalidad de trabajo adoptada por la Entidad según la Resolución de Teletrabajo 404 de marzo 8 de 2016 “Adopción del Teletrabajo en Ministerio de Ambiente y Desarrollo Sostenible”, o de conformidad con los lineamientos y regulaciones que deroguen lo anterior.
- La Entidad define los lineamientos y directrices en materia de seguridad en el presente documento **M-E-GET-04** Manual de Políticas Específicas de Seguridad y Privacidad de la Información.
- La Entidad debe dar a conocer a los Teletrabajadores los lineamientos impartidos a través de la presente Política y con ello los riesgos de su proceso que se derivan por el uso de los equipos tecnológicos para la Seguridad de la información.
- La Entidad debe establecer procedimientos para la solicitud y autorización del Teletrabajo.
- El Grupo de Talento Humano se encargará de llevar el registro de los Teletrabajadores al servicio de la Entidad; en dicho registro se incluirá la información correspondiente a la identificación de cada uno, la ubicación de su puesto de trabajo, los teléfonos de contacto, las fechas de vigencia, modalidad aplicable (identificando los días que debe realizar sus labores desde su domicilio y los días que lo hará en la Entidad), la identificación de los equipos de cómputo que le fueron asignados, y demás que apliquen.
- La revocación de la autoridad y de los derechos de acceso, que se validan por parte del equipo de mesa de asistencia de la Entidad donde se revocan los permisos de acceso.
- La OTIC será la encargada de implementar los controles de seguridad lógicos y tecnológicos necesarios para proteger la confidencialidad, integridad y disponibilidad de la información en la modalidad de Teletrabajo.
- Las herramientas oficiales de chat, almacenamiento y reuniones aprobadas por La Entidad son las herramientas colaborativas licenciadas, las cuales todos los servidores públicos debe mantener activas durante su horario laboral y responder con la debida diligencia, tal como si estuviesen realizando sus funciones y actividades en las instalaciones de la Entidad.
- Los Servidores públicos deben cumplir los lineamientos técnicos (mínimos) establecidos por la entidad para los dispositivos móviles o estaciones de trabajo que se emplearan para el teletrabajo. Dichos lineamientos entre otros estarán enfocadas a sistema operativo,

herramienta de antivirus, capacidad del disco duro, ancho de banda de internet y demás aplicables de seguridad y salud en el trabajo.

7 SEGURIDAD DE LOS RECURSOS HUMANOS

7.1 Antes de Asumir el Empleo

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

Alcance: La presente política establece que todos los servidores públicos, contratistas y proveedores, debe dar cumplimiento a las Políticas de Seguridad y Privacidad de la información de MinAmbiente.

Lineamientos: Se debe dar cumplimiento a los siguientes lineamientos:

7.1.1 Selección

Control: Las verificaciones de los antecedentes de todos los candidatos a un empleo se debe llevar a cabo de acuerdo con las leyes, reglamentos y ética pertinentes, y debe ser proporcionales a los requisitos de negocio, a la clasificación de la información a que se va a tener acceso, y a los riesgos percibidos.

La Entidad reconoce la importancia que tiene el factor humano para el cumplimiento de sus objetivos misionales y, con el interés de contar con personal calificado, debe garantizar que la vinculación de los candidatos, aspirantes, contratistas, proveedores y terceros cumplan con los procesos de verificación necesarios, el cual estará orientado al perfil, a las funciones y/u obligaciones que debe desempeñar para desarrollar su labor.

confidencial, por ejemplo, información financiera o información muy confidencial, la organización debe también considerar verificaciones adicionales más detalladas (por ejemplo, estudio de seguridad, polígrafo, visita domiciliaria), se asegura con la firma del **F-A-CTR-36** Acta de Compromiso de Confidencialidad.

- El Grupo de Talento Humano debe garantizarse de aplicar el procedimiento **P-A-ATH-08** Provisión de Empleos Vinculación y el Formato, **F-A-ATH-32** Análisis Requisitos para Nombramiento.
- El Grupo de Talento Humano debe garantizar que la vinculación de los aspirantes a los diferentes cargos de planta cumpla con los requisitos mínimos legales.

- El Grupo de Talento Humano debe generar un mecanismo para que toda la planta de personal se informe y comprometa con los acuerdos de confidencialidad.
- El Grupo de Talento Humano debe considerar la información sobre todos los candidatos que se consideran para cargos dentro de la Entidad, adicionalmente se debe recolectar y manejar apropiadamente de acuerdo con la ley de protección de datos personales conforme a la **DS-E-GET-01** Política de Tratamiento y Protección de Datos Personales.
- Referencias satisfactorias cuya validación se aplica desde el procedimiento **P-A-ATH-08** Provisión de Empleos Vinculación y el formato **F-A-ATH-32** Análisis Requisitos para Nombramiento.
- El Grupo de Talento Humano debe realizar verificación de la de la hoja de vida del solicitante incluyendo certificaciones académicas y laborales; se aplica desde el procedimiento **P-A-ATH-08** Provisión de Empleos Vinculación y el formato **F-A-ATH-32** Análisis Requisitos para Nombramiento.
- El Grupo de Talento Humano debe realizar confirmación de las calificaciones académicas y profesionales declaradas; se aplica desde el **P-A-ATH-08** Provisión de Empleos Vinculación y el formato **F-A-ATH-32** Análisis Requisitos para Nombramiento.
- El Grupo de Talento Humano y el Grupo de Contratos debe notificar por medio de la herramienta de mesa de asistencia, cualquier novedad de los servidores públicos que se encuentren en las diferentes situaciones administrativas tales como: (licencias, vacaciones, incapacidades, traslado, retiro, entre otros); para que los responsables de las plataformas procedan a bloquear o suspender las cuentas de usuario, sus privilegios de acceso y/o se haga entrega de los elementos devolutivos según disponga su jefe inmediato o supervisor de contrato, incluyendo el paz y salvo cuando sea necesario
- El Grupo de Talento Humano y el Grupo de Contratos deben realizar verificación detallada, como de antecedentes penales. Cuando un individuo es contratado para un rol de seguridad de la información específico, las organizaciones deben asegurar que el aspirante tenga la competencia necesaria para desempeñar el rol de seguridad; se aplica desde el procedimiento **P-A-ATH-08** Provisión de Empleos Vinculación y el formato **F-A-ATH-32** Análisis Requisitos para Nombramiento.
- El Grupo de Talento Humano y el Grupo de Contratos debe verificar que el aspirante sea confiable para desempeñar el rol, especialmente si es crítico para la organización, se aplica desde el procedimiento **P-A-ATH-08** Provisión de Empleos Vinculación y el formato **F-A-ATH-32** Análisis Requisitos para Nombramiento.
- El Grupo de Contratos debe asegurar un proceso de selección para contratistas. En estos casos, el acuerdo entre la Entidad y el contratista debe especificar las responsabilidades por la realización de la selección, y los procedimientos de notificación que es necesario seguir si la selección no se ha finalizado, o si los resultados son motivo de duda o inquietud., mediante la **F-A-CTR-28** Verificación de Idoneidad y Experiencia Procesos Misionales.
- Cuando el servidor público, contratista o proveedor vaya a realizar un trabajo, ya sea una asignación o una promoción, implique que la persona tenga acceso a las instalaciones de procesamiento de información, y en, si ahí se maneja información incorporar dentro de las minutas contractuales, clausulas referentes a:

- Estricto cumplimiento del Manual de Políticas Específicas de Seguridad y Privacidad de la Información definida por la Entidad.
- Confidencialidad de la Información.
- Cláusulas de Tratamiento de Datos Personales

7.1.2 Términos y condiciones del empleo

Control: Los acuerdos contractuales con empleados y contratistas debe establecer sus responsabilidades y las de la organización en cuanto a la seguridad de la información.

El Grupo de Talento Humano y el Grupo de Contratos deben incorporar dentro de los acuerdos contractuales con los empleados y contratistas, las responsabilidades que debe cumplir en el marco del Sistema de gestión de Seguridad de la Información.

- El Grupo de Talento Humano y el Grupo de Contratos debe emplear los mecanismos para proteger la confidencialidad de la información y la no divulgación de la información reservada de la Entidad, mediante la formalización de los acuerdos de confidencialidad.
- Todo funcionario y contratista que se vincule a la entidad debe firmar y dar cumplimiento a cada una de las responsabilidades de seguridad de la información establecidas en los actos administrativos y contratos de la entidad.

7.2 Durante la Ejecución del Empleo

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

- El Grupo de Talento Humano debe notificar por medio de la herramienta de mesa de asistencia, cualquier novedad de servidores públicos que se encuentren en situaciones administrativas tales como: (licencias, vacaciones, traslado, retiro, entre otros); para que los responsables de las plataformas de control de acceso procedan a habilitar, bloquear o suspender las cuentas de usuario, sus privilegios de acceso y/o se haga entrega de los elementos devolutivos según disponga su jefe inmediato o supervisor de contrato.
- El Grupo de Talento Humano debe notificar por medio de la herramienta de mesa de asistencia, cualquier novedad relacionada con el retiro de practicantes; para que los responsables de las plataformas de control de acceso procedan a habilitar, bloquear o suspender las cuentas de usuario, sus privilegios de acceso y/o se haga entrega de los elementos devolutivos según disponga el supervisor de la práctica.
- El supervisor(es) de contratos, debe notificar por medio de la herramienta de mesa de asistencia, cualquier novedad de los contratistas, proveedores y terceros tales como: (iniciar, suspender, ceder, terminar contratos, entre otros), de conformidad con el establecido en **M-**

E-GET-04 Manual de Políticas Específicas de Seguridad y Privacidad de la Información referente a su vinculación o relación comercial con la Entidad para que los responsables de las plataformas de control de acceso procedan a habilitar, bloquear o suspender las cuentas de usuario, sus privilegios de acceso y/o se haga entrega de los elementos devolutivos según disponga el supervisor de contrato.

- El Grupo de Talento Humano y Grupo de Contratos debe considerar la información sobre todos los servidores y contratistas que se consideran para cargos o roles en la Entidad, por lo cual se debe tener en cuenta el cumplimiento de la Ley de protección de datos personales conforme a la **DS-E-GET-01** Política de Tratamiento y Protección de Datos Personales.
- El Grupo de Talento Humano y el Grupo de Contratos debe dar cumplimiento al uso del **F-A-CTR-36** Acta de compromiso de confidencialidad en los casos que aplique.
- El Grupo de Talento Humano y el Grupo de Contratos debe dar cumplimiento a la ley y la normatividad vigente tanto para servidores públicos como para contratistas, que se encuentra en formatos y procedimientos de talento humano y contratos, así como en resoluciones de secretaria general, manual de contratación, manual de funciones, minutas contractuales y demás inherentes al cumplimiento de sus funciones.

7.2.1 Responsabilidades de la dirección

Control: La Entidad debe exigir a todos los servidores públicos, contratistas y proveedores la aplicación de la seguridad de la información de acuerdo con las políticas y lineamientos establecidos.

- El Grupo de Talento Humano y Grupo de Contratos deben informar a los servidores públicos y contratistas sobre sus roles y responsabilidades de seguridad de la información, antes de que se les otorgue el acceso a información o sistemas de información confidenciales, cuya información esta consignada en el **M-E-GET-04** Manual de Políticas Específicas de Seguridad y Privacidad de la Información. De igual forma se encuentra articulado con el proceso de inducción.
- Los servidores públicos y contratistas deben acatar las directrices que establecen las expectativas de seguridad de la información de sus roles dentro de la Entidad, con las sensibilizaciones programadas por el equipo de seguridad de la información.
- La Entidad debe implementar un mecanismo para que los servidores públicos y contratistas logren un nivel de toma de conciencia sobre seguridad de la información pertinente a sus roles y responsabilidades dentro de la organización y estén motivados para cumplir con las políticas mediante las sensibilizaciones programadas por el equipo de seguridad de la información.

7.2.2 Toma de conciencia, educación y formación en la seguridad de la información

Control: Todos los empleados de la organización, y en donde sea pertinente, los contratistas, deben recibir la educación y la formación en toma de conciencia apropiada, y actualizaciones regulares sobre las políticas y procedimientos pertinentes para su cargo.

- El responsable de Seguridad de la Información debe definir, actualizar, publicar y ejecutar el Plan de Sensibilización y Comunicación en Seguridad de la Información.
- El responsable de Seguridad de la Información debe desarrollar campañas, piezas comunicativas y boletines de seguridad, los cuales se ejecutarán conforme al **G-E-GET-41** Plan de Sensibilización y Comunicaciones en Seguridad de la Información.
- Se debe realizar jornadas de inducción y reinducción por parte del Grupo de Talento Humano, en donde se mencionen aspectos y recomendaciones de buenas prácticas de seguridad de la información.
- Los servidores públicos y contratistas deben conocer y apropiar la normativa relacionada con la seguridad de la información de la Entidad, toda vez que el desconocimiento de esta no los exonerará de los procesos disciplinarios ante posibles violaciones o incumplimiento de las políticas de seguridad.
- Se debe evaluar la importancia de la información divulgada en las sesiones de sensibilización en seguridad de la información.
- Los servidores públicos y contratistas de la Entidad deben reportar los incidentes de seguridad en la herramienta de Mesa de asistencia.
- Los nuevos servidores públicos y contratistas de la Entidad deben participar en las jornadas de sensibilización de Seguridad de la Información previstas en **G-E-GET-41** Plan de Sensibilización y Comunicaciones en Seguridad de la Información.
- Las evidencias de la ejecución del **G-E-GET-41** Plan de Sensibilización y Comunicaciones en Seguridad de la Información tales como: lista de asistencia, material de apoyo, grabaciones y demás, quedan registradas en el repositorio de información de la Oficina de Tecnologías de la Información y Comunicaciones.
- Se debe incluir en los temas de toma de conciencia los procedimientos de seguridad de la información (tales como el reporte de incidentes de seguridad de la información) y los controles de línea base (tales como la seguridad de las contraseñas, los controles del software malicioso, y los escritorios limpios), entre otros.
- Los servidores públicos, contratistas y proveedores que requieran de acceso privilegiado debe ser consientes respecto a sus roles y responsabilidades, no obstante, se debe formalizar la entrega de esta información conforme lo dispuesto en **M-E-GET-04** Manual de Políticas Específicas de Seguridad y Privacidad de la Información.

7.2.3 Proceso disciplinario

Control: Se debe contar con un proceso disciplinario formal el cual debe ser comunicado, para emprender acciones contra empleados que hayan cometido una violación a la seguridad de la información.

- La Entidad a través del Grupo de Control Interno Disciplinario emprenderá acciones contra los servidores públicos que hayan cometido una violación a la seguridad de la información. Para lo cual cuenta con los siguientes procedimientos: Ver procedimientos: **P-A-DIS-01** Indagación

Preliminar, **P-A-DIS-02** Investigación Disciplinaria, **P-A-DIS-03** Juzgamiento (Pliego de Cargos), **P-A-DIS-04** Segunda Instancia, **P-A-DIS-05** Disciplinario Verbal y la Ley 734 de 2002.

.

- La Entidad adoptará y tomará las medidas pertinentes en el caso que haya ocurrido una violación a la seguridad de la información, conforme a lo consignado en el documento **M-E-GET-04** Manual de Políticas Específicas de Seguridad y Privacidad de la Información.

7.3 Terminación o Cambio de Empleo

Objetivo: Proteger los intereses de la Entidad como parte del proceso de cambio o terminación del empleo.

7.3.1 Terminación o cambio de responsabilidades de empleo

Control: Las responsabilidades y los deberes de seguridad de la información que permanecen validos después de la terminación o cambio de empleo o contrato se debe definir, comunicar al servidor público o contratista y se debe hacer cumplir.

- El Grupo de Talento Humano debe dar cumplimiento al procedimiento establecido para la culminación o retiro de la Entidad que se encuentra documentado en el **F-A-ATH-06** Legalización Retiro del Servicio.
- La Entidad debe garantizar un mecanismo a fin de adoptar un registro o acta firmada por el jefe inmediato o supervisor donde se asegura de la transferencia apropiada de información al sucesor del cargo o rol e informe o documento equivalente de la gestión y estado de las actividades realizadas.

8 GESTIÓN DE ACTIVOS

8.1 Responsabilidad por los Activos

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

8.1.1 Inventario de activos

Control: Se debe identificar los activos asociados con la información y las instalaciones de procesamiento de información, y se debe elaborar y mantener un inventario de estos activos.

- La OTIC debe tener como marco de referencia la guía "**I-E-GET-02** Metodología para la Identificación Gestión y Clasificación de Activos de Información", con el fin de establecer los lineamientos necesarios para la gestión de los activos de información de la Entidad de manera organizada y estructurada**.**
- La OTIC debe realizar acompañamiento anual a los procesos para la actualización, identificación y clasificación del inventario de activos de información, el cual se presentará para aprobación ante el Comité Institucional de Gestión y Desempeño - CIGD.
- El propietario del activo debe registrarse en la matriz "", con el fin de realizar una gestión eficaz y la asignación de responsabilidades con respecto a los activos de información.
- La OTIC y el dueño de los activos deben gestionar a través de las áreas responsables la publicación de la matriz de identificación y clasificación de activos de información en la página web del Ministerio y en el portal de datos abiertos, con el fin de garantizar su accesibilidad.
- El líder del proceso será el responsable de actualizar por lo menos una vez al año y/o cuando se presenten:
    - Cambios en la tabla de retención documental
    - Identificación de nuevos activos de información, actualización de información de activos existentes y retiro de activos de información.
    - La OTIC en articulación con la Unidad Coordinadora de Gobierno Abierto – UCGA, gestionarán la publicación del registro de activos de información en el portal de datos abiertos de acuerdo con la normatividad vigente.
    - El Ministerio a través del líder de cada proceso o dueño de los activos de información tanto físicos como digitales, debe generar un mecanismo para etiquetar la información documentada de la Entidad, de acuerdo con su clasificación, con el objetivo de asegurar que cada tipo de información reciba el nivel de protección adecuado.

8.1.2 Propiedad de los activos

Control: Los activos mantenidos en el inventario deben tener un propietario.

- El propietario del activo de información será responsable de definir los criterios de calificación en cuanto a su clasificación según su importancia, así como definir y revisar periódicamente las restricciones y autorizaciones de acceso.
- La matriz "**F-E-GET-18** Matriz Inventario de Activos de Información Ministerio de Ambiente y Desarrollo Sostenible - AMBIENTE" deberá incluir la identificación e información del propietario del activo de información por cada uno de los procesos, así como su clasificación y las medidas de protección a tomar por su parte.

- Se debe acatar el documento "**I-E-GET-02** Metodología para la Identificación Gestión y Clasificación de Activos de Información", el cual define los lineamientos para la identificación y clasificación de los activos de información en la Entidad.
- Es responsabilidad del propietario de los activos de información actualizar, revisar periódicamente y validar las restricciones y clasificaciones de dichos activos, considerando las políticas de control de acceso aplicables a los mismos.
- Anualmente se debe realizar un ejercicio de identificación y actualización de activos de información donde participe el propietario o delegado del activo, La matriz de inventario generada (**F-E-GET-18** Matriz Inventario de Activos de Información Ministerio de Ambiente y Desarrollo Sostenible - AMBIENTE) deberá ser llevada ante el Comité Institucional de Gestión y Desempeño (CIGD) para su aprobación.

8.1.3 Uso aceptable de los activos

Control: Se debe identificar, documentar e implementar reglas para el uso aceptable de información y de activos asociados con información e instalaciones de procesamiento de información.

- La información, archivos físicos y digitales, sistemas de información, servicios tecnológicos, e infraestructura son activos de la Entidad, y se proporcionan a los servidores públicos, contratistas y terceros autorizados para cumplir con los propósitos y funciones del Ministerio. Por lo tanto, no deben ser utilizados para fines personales o no autorizados.
- Todos los servidores públicos y contratistas deben etiquetar la información y darle el uso y protección adecuados según su clasificación, siguiendo las directrices propias del Ministerio y de la ley 1712 del 2014 "Por medio del cual se crea la ley de transparencia y del derecho de acceso a la información pública ", cuya aplicación en la Entidad se encuentra documentada en el instructivo - **I-E-GET-02** Metodología para la Identificación Gestión y Clasificación de Activos de Información.
- Los servidores públicos, contratistas, proveedores y terceros que posean información de la Entidad deben reportar los eventos o incidentes de seguridad de la información de los que tengan conocimiento, de acuerdo con lo establecido en el **M-A-GTI-03** Manual para la Gestión de Incidentes de Seguridad y Privacidad de la Información**.**
- Está prohibido que servidores públicos, contratistas, proveedores o terceros ajenos a la Oficina TIC manipulen, destapen o retiren partes de los equipos de cómputo propios de la Entidad. Cualquier intervención técnica debe ser realizada únicamente por personal autorizado de la Oficina TIC.
- Los usuarios deben asegurarse de proteger los activos de información físicos y digitales contra acceso no autorizado, pérdida, daño o alteración. Esto incluye la protección física de dispositivos tales como computadores, impresoras, computadores portátiles, discos duros de la Entidad, así como la protección digital mediante contraseñas seguras, cifrado, entre otras medidas de seguridad.

8.1.3.1 Uso de la información

- Toda actividad del ciclo de vida de la información institucional tales como creación, almacenamiento, transformación, transmisión, eliminación y demás, deben estar orientadas única y exclusivamente a cumplir con los objetivos misionales, estratégicos y funcionales de la Entidad.
- Los servidores públicos, contratistas, proveedores y terceros que tengan acceso a la información de la Entidad, deben aplicar los controles de seguridad definidos en el presente manual, para reducir riesgos que afecten la integridad, confidencialidad y disponibilidad de los activos de información.
- La información que contenga y almacene o use datos personales de tipo “privado, sensible y de niños, niñas y adolescentes”, debe cumplir con la normatividad de datos personales, de igual forma contar con acceso controlado, el cual debe ser gestionado y validado por el propietario de la información.
- Ningún servidor público, contratista, proveedor o tercero de la Entidad puede compartir sus credenciales de autenticación y acceso a la información.
- Cualquier modificación que los servidores públicos, contratistas, proveedores y terceros requieran hacer a la información debe ser autorizada y verificada por su propietario.
- Se prohíbe el uso de los recursos tecnológicos de la Entidad para difundir o participar en actividades políticas y/o personales. Se debe respetar la propiedad intelectual y material de la documentación oficial producida por la Entidad. No se permite reproducir, copiar, redistribuir, o usar la documentación oficial de propiedad de la Entidad para fines ajenos a la misma.

8.1.3.2 Uso de los equipos de cómputo

- La información, equipos de cómputo y recursos tecnológicos provistos por la Entidad deben utilizarse exclusivamente para actividades autorizadas en el marco de las funciones laborales asignadas, Se prohíbe su uso para asuntos personales o ajenos a los objetivos de la Entidad.
- La información, equipos de cómputo y recursos tecnológicos provistos por la Entidad que se usen fuera de sus instalaciones, deben ser protegidos por los servidores públicos, contratistas, proveedores y terceros, de la misma manera que si estuvieran en la oficina.
- Utilizar los recursos proporcionados por la Entidad para realizar otras tareas que no concuerden con la labor asignada constituye una violación a las políticas de seguridad de la información.
- Los equipos portátiles proporcionados por la Entidad son sensibles a robo o pérdida, por lo cual requieren medidas de seguridad adicionales. Es fundamental no dejarlos desatendidos en el puesto de trabajo o en cualquier lugar donde se utilicen.
- Los equipos portátiles proporcionados por la Entidad, deben ser tratados de forma adecuada y con buen uso, garantizando la protección física, funcional y el cuidado de la información que contienen.

- No se permite modificar la configuración ni instalar programas no aprobados por la Entidad en los equipos de cómputo, ya sea su uso se realice dentro o fuera de sus instalaciones. La instalación de software debe ser realizada únicamente por el personal autorizado de la OTIC.
- No se permite brindar asistencia técnica remota con herramientas que no se encuentran licenciadas por la Entidad o sus proveedores.
- No debe abrirse, retirar o cambiar componentes de los equipos por parte de personal no autorizado y sin la previa autorización de la OTIC.
- Está prohibido remover, romper o alterar los sellos de inventario colocados en los equipos de cómputo de la Entidad.

8.1.3.3 Uso correo electrónico y herramientas colaborativas

- Los servidores públicos, contratistas, proveedores y terceros a quienes la Entidad les asigne una cuenta de correo electrónico y/o herramientas colaborativas, aceptan expresamente que son servicios de comunicaciones institucionales y se obligan a respetar y cumplir con los lineamientos de buen uso.
- La cuenta de correo electrónico institucional es personal e intransferible. Los servidores públicos, contratistas, proveedores y terceros son responsables del buen uso y de toda acción efectuada con esta y con las herramientas colaborativas asociadas a la misma.
- Los correos electrónicos institucionales deben tener obligatoriamente la firma del servidor público, contratista, en donde se incluyan los siguientes datos:
    - Logo institucional
    - Nombre completo
    - Cargo
    - Área
    - Teléfono y extensión (si aplica)
    - Dirección de la Entidad
    - URL Sede electrónica
    - Mensaje de privacidad o disclaimer

- **Autenticación de Doble Factor (2FA)**
    - Los funcionarios, contratistas, proveedores y terceros deberán activar y utilizar obligatoriamente la autenticación de doble factor (2FA), cuya implementación será gestionada por la OTIC. Este requisito aplica a todo el personal que acceda al correo electrónico de la entidad.
    - Los usuarios deben asegurar la protección de los dispositivos utilizados para la autenticación (por ejemplo, no compartir claves o códigos de autenticación).
    - Se debe instalar y configurar la aplicación Microsoft Authenticator, para proteger la cuenta de correo institucional, este proceso contará con el apoyo de la OTIC.
    - La OTIC debe realizar campañas de socialización para garantizar que los usuarios comprendan cómo usar 2FA y por qué es importante.

- El administrador de la consola de correo electrónico institucional debe realizar periódicamente la revisión de las cuentas de correo que llevan más de 60 días inactivas o sin ningún acceso, con lo cual se procederá a validar con el responsable; de acuerdo con la retroalimentación, se puede proceder a su eliminación para hacer uso de la licencia.
- Todas las cuentas genéricas de correo del Ministerio deben tener un responsable asignado de planta, quien será encargado de gestionar su uso y supervisar la actividad relacionada. En caso de cambios de responsabilidad en las Dependencias, el nuevo responsable deberá ser designado antes de la transición para evitar que estas cuentas queden sin supervisión o en el caso de que la cuenta ya no sea necesaria, deberá informarse a la OTIC para que proceda con su eliminación.
- El envío y recepción de información institucional debe realizarse exclusivamente desde la cuenta de correo electrónico institucional.
- Dado que el correo electrónico es una herramienta clave de comunicación, los servidores públicos y contratistas deben revisarlo de manera continua durante la jornada laboral, asegurando una respuesta oportuna a los mensajes recibidos.
- En el marco del cumplimiento de la política de cero papeles se debe priorizar el uso del correo institucional para el envío de documentos, limitando la impresión y el envío en físico a aquellos casos en los que sea estrictamente necesario.
- Los servidores públicos, contratistas, proveedores y terceros pueden solicitar apoyo en la descarga del backup de su buzón de correo electrónico institucional antes de finalizar su vinculación con la Entidad. Dicha solicitud se realizará por medio de la herramienta de mesa de asistencia. Si el contratista o funcionario utiliza herramientas colaborativas, como Forms, Power BI, PowerApps, entre otras, se deberá informar a la OTIC para realizar el respectivo backup antes de que la cuenta sea eliminada.
- Los servidores públicos, contratistas, proveedores y terceros deben configurar las reglas de respuesta en caso de ausencia o, en su defecto, deben realizar la solicitud por medio de la herramienta de mesa de asistencia para que el responsable de la OTIC realice dicha configuración.
- Los mensajes que contengan información confidencial, ya sea en el cuerpo del correo o en un archivo adjunto, deben ser cifrados utilizando las opciones disponibles en la herramienta de correo, para garantizar la protección de su confidencialidad.
- Las comunicaciones oficiales, ya sea a través de correo electrónico, chat o reuniones, tanto internas como externas, deben llevarse a cabo exclusivamente mediante las herramientas oficiales y licenciadas de la Entidad.
- Los mensajes de correo electrónico institucional deben llevar el siguiente mensaje de privacidad o disclaimer:
    - AVISO LEGAL: Este correo electrónico contiene información confidencial del Ministerio de Ambiente y Desarrollo Sostenible. Si Usted no es el destinatario, le informamos que no podrá usar, retener, imprimir, copiar, distribuir o hacer público su contenido, de hacerlo podría tener consecuencias legales como las contenidas en la Ley 1273 del 5 de Enero de 2009 y todas las que le apliquen. Si ha recibido este correo por error, por favor informe al remitente y luego bórrelo. Si usted es el

destinatario, le solicitamos mantener reserva sobre el contenido, los datos o información de contacto del remitente y en general sobre la información de este documento y/o archivos adjuntos, a no ser que exista una autorización explícita.

LEGAL NOTICE: This e-mail transmission contains confidential information of Ministerio de Ambiente y Desarrollo Sostenible. If you are not the intended recipient, you should not use, hold, print, copy, distribute or make public its content, on the contrary it could have legal repercussions as contained in Law 1273 of 5 January 2009 and all that apply. If you have received this e-mail transmission in error, Please inform the sender and then delete it. If you are the intended recipient, we ask you not to make public the content, the data or contact information of the sender and in general the information of this document or attached file, unless a written authorization exists.

- **No se encuentra permitido el uso del correo electrónico institucional para**:
    - Utilizar la cuenta de correo electrónico institucional como medio de comunicación con sitios ajenos a las entidades que hacen parte de la administración pública.
    - Utiizar la cuenta de correo para el registro en aplicaciones externas o privadas. Enviar cadenas de correo, mensajes con contenido religioso, político, racista, sexista, pornográfico, publicitario, mensajes mal intencionados o cualquier otro tipo de contenido que se pueda considerar como inadecuado o mal uso del servicio.
    - Envío, recepción y ejecución de archivos que no contengan extensiones, intentado evadir las herramientas de seguridad, o que incluya chivos ejecutables tipo .exe, .bat, entre otros, que puedan comprometer la seguridad de la información y los recursos institucionales.
    - Abrir mensajes y adjuntos que provengan de remitentes desconocidos o sospechosos, que puedan venir asegurados con contraseña y la cual se mencione de forma clara en el cuerpo del mensaje, toda vez que estos intentan evadir los sistemas de seguridad de la Entidad y pueden llegar a ser causantes de ataques cibernéticos.
    - Usar o suplantar la identidad de cuentas de correo electrónico institucional pertenecientes a otros usuarios.
    - Compartir las credenciales de acceso a la cuenta de correo electrónico.
    - Realizar otras acciones no especificadas anteriormente que puedan afectar o atentar contra la imagen y reputación de la Entidad.
    - Envío de correos masivos sin la debida autorización, que pueda provocar el bloqueo de cuentas y afectar la disponibilidad del servicio en la Entidad. En caso de que esto ocurra, el servicio de correo electrónico podría verse bloqueado para toda la Entidad durante más de 24 horas.
    - Enviar datos de usuarios y contraseñas de acceso a los servicios tecnológicos de la Entidad a través de correo electrónico u otros medios no seguros. Esta práctica compromete la seguridad de los sistemas y puede facilitar accesos no autorizados.

8.1.3.4 Uso del Internet

- Se deben adoptar los controles necesarios para fomentar el uso racional y pertinente del servicio de Internet, con el propósito de minimizar los riesgos derivados de su uso.
- El servicio de Internet debe usarse de manera responsable y exclusivamente para fines propios del desarrollo de las funciones y obligaciones asignadas por la entidad.
- No se debe visitar páginas no fiables, sospechosas o que no cumplan con los estándares mínimos de seguridad, con el fin de evitar posibles incidentes de seguridad de la información.
- No se debe proporcionar información de la Entidad en foros, chats, y demás sitios externos, que conlleve a que pueda ser utilizada de forma fraudulenta.
- Está prohibido divulgar o dar a conocer cualquier tipo de información de la Entidad, de sus recursos tecnológicos, activos de información, datos personales, funcionamiento interno, sin la respectiva autorización expresa e informada de los responsables designados.
- Antes de utilizar información obtenida de internet para el cumplimiento de las funciones en la Entidad, los servidores públicos, contratistas, proveedores y terceros, deben verificar los derechos de autor, así como los aspectos de propiedad intelectual, empresarial, comercial o institucional de la información, para asegurar el cumplimiento de las normativas legales y evitar el uso indebido de contenido protegido.
- Se debe filtrar, restringir y monitorear todo el contenido web que vaya en contra de los intereses de la Entidad, incluyendo entre otros los siguientes tipos de contenido:
    - Ofensivos, obscenos, pornográficos
    - Abusivos, bromistas o amenazantes
    - Ilegales y/o fraudulentos
    - Piratería de software
    - Anónimos o diseñados para molestar u hostigar
- No se encuentra permitido el uso de aplicaciones de tipo chat de ninguna red social (Ejemplo: WhatsApp, Telegram, YouTube, Instagram, FaceBook, otras), vía web o instalarlas en los equipos de cómputo de la Entidad. Solo se permiten aquellas aplicaciones que cuenten con autorización expresa para el desempeño de funciones específicas del colaborador debidamente autorizado, con el objetivo de prevenir fugas de información y posibles vectores de ataque a los activos de información de la entidad.
- Los servicios de internet a los que los servidores públicos, contratistas, proveedores y terceros puedan acceder estará determinado por el rol que desempeñan en la Entidad y los permisos correspondientes.
- Los servidores públicos, contratistas, proveedores y terceros deben notificar si tienen acceso a contenidos o servicios no autorizados o que no se correspondan con sus funciones o roles en la Entidad.
- Se prohíbe el acceso a los recursos de internet que puedan poner en riesgo los activos de información de la Entidad.

- La Entidad podrá bloquear el acceso a los sitios de internet considerados inapropiados. El acceso intencional y recurrente a estos sitios puede dar lugar a acciones disciplinarias.

8.1.4 Devolución de activos

Control: Todos los servidores públicos, contratistas y partes externas deben devolver todos los activos de la Entidad que se encuentren a su cargo, al terminar su empleo, contrato o acuerdo.

- Todo servidor público y contratista debe gestionar la devolución de sus activos físicos y sistematizados que tiene a su cargo al terminar su empleo o contrato, gestionando el Formato F-A-ATH-06 Legalización retiro del servicio.
- Es deber de todo servidor y contratista que preste servicios a la Entidad, al finalizar su relación laboral, entregar toda la información producto del trabajo realizado, diligenciando el Formato F-A-ATH-06 Legalización retiro del servicio.
- La Entidad llevará a cabo el seguimiento respecto a la devolución de los activos de información mediante el trámite y firma del formato F-A-CTR-35 Paz y salvo contrato de prestación de servicios. Lo anterior aplica para los activos físicos y accesos a los servicios tecnológicos de la entidad.
- Una vez finalizado el vínculo con la Entidad, el jefe de área o supervisor del contrato, según corresponda. debe solicitar a la Mesa de Asistencia, la aplicación de las herramientas de borrado seguro sobre la información institucional almacenada en los equipos asignados para la ejecución de sus funciones u obligaciones contractuales. Esto debe realizarse posteriormente a la generación del backup de dicha Información.
- El Directivo, Jefe de Oficina, Coordinador de Grupo o Supervisor del Contrato, según corresponda, debe asegurarse que los activos de información que se encuentren bajo su custodia sean:
    - Reasignados a un funcionario, colaborador o parte interesada de la Entidad.
    - Devueltos al líder de proceso, archivo, bodega o almacén de la Entidad según corresponda.
    - Traspasados a otra área, dependencia o proceso.
    - Destruidos, dados de baja o donados a terceros según sea el caso y el proceso definido por el área encargada.

8.2 Clasificación de la Información

Objetivo: Asegurar que la información recibe un nivel apropiado de protección, de acuerdo con su importancia para la Entidad.

8.2.1 Clasificación de la información

Control: La información se debe clasificar en función de los requisitos legales, valor, criticidad y susceptibilidad a divulgación o a modificación no autorizada.

- El dueño de los activos de información debe clasificar estos activos dependiendo del nivel de confidencialidad, integridad y disponibilidad que se requiera para su protección, teniendo en cuenta la I-E-GET-02 Metodología para la identificación, gestión y clasificación de activos de información.
- El servidor público, contratista, proveedor y/o tercero responsable del activo de información debe asegurarse de que el activo está inventariado en la F-E-GET-18 Matriz inventario de Activos de Información Ministerio de Ambiente y Desarrollo Sostenible – AMBIENTE o informar a la OTIC para su debido registro.

.

8.2.2 Etiquetado de la información

Control: Se debe desarrollar e implementar un conjunto adecuado de procedimientos para el etiquetado de la información, de acuerdo con el esquema de clasificación de información adoptado por la Entidad.

- El dueño de los activos de información debe etiquetar los activos teniendo en cuenta el procedimiento I-E-GET-02 Metodología para la identificación, gestión y clasificación de activos de información.
- Cada activo debe contar con un etiquetado donde se identifique el nivel de clasificación asignado. El etiquetado debe aplicarse a toda la información contenida en medios físicos, electrónicos y digitales, de acuerdo con los lineamientos relacionados con la clasificación y rotulación de la información.

8.2.3 Manejo de activos

Control: Se debe desarrollar e implementar procedimientos para el manejo de activos, de acuerdo con el esquema de clasificación de información adoptado por la Entidad.

Para el uso, tratamiento, procesamiento, almacenamiento y comunicación de la información se deben considerar los niveles de clasificación establecidos en la documentación relacionada con la Clasificación y rotulación de la información.

La eliminación y destrucción de la información deben realizarse de acuerdo con su nivel de clasificación y siguiendo los lineamientos establecidos en la documentación pertinente sobre la clasificación y rotulación de la información

Se deben acatar los lineamientos de la I-E-GET-02 Metodología para la identificación, gestión y clasificación de activos de información, considerando lo siguiente:

Teniendo en cuenta que la Integridad es un principio fundamental de la seguridad de la información, se debe cumplir con:

- En lo que respecta a todas las aplicaciones de la Entidad, se deben implementar mecanismos destinados a garantizar la integridad de los activos de información, basándose en el nivel de clasificación y el nivel de evaluación del riesgo identificado.
- La Oficina de Tecnologías de la Información y Comunicación - OTIC de la Entidad será la única dependencia autorizada para realizar copias de seguridad del software original.
- Con el fin de asegurar el cumplimiento de las normativas de propiedad intelectual y protección de la información la OTIC realizará supervisiones periódicas para validar que el software proporcionado por la Entidad no sea copiado ni suministrado a terceros.

8.3 Manejo de Medios

Objetivo: Evitar la divulgación, la modificación, el retiro o la destrucción no autorizados de información almacenada en los medios.

8.3.1 Gestión de medios removibles

Control: Se debe implementar procedimientos para la gestión de medios removibles, de acuerdo con el esquema de clasificación adoptado por la Entidad.

- Se debe acatar el documento G-A-GTI-04 BORRADO SEGURO de la Entidad, que brinda lineamientos sobre como borrar o eliminar toda información que no se requiera o no sea útil en los medios de almacenamiento, de tal forma que no pueda ser recuperada, restaurada o reconstruida posteriormente.
- Cualquier dispositivo de almacenamiento de información de propiedad de la Entidad, se considera un activo de información, por lo tanto, su ingreso, uso, movilización y salida, debe ser previamente autorizado por el Grupo de Servicios Administrativos y del proceso responsable del activo.
- La Subdirección Administrativa debe mantener un inventario actualizado de los dispositivos de almacenamiento de información removible de la entidad, tales como cintas de backups, discos duros externos, USB, GPS, entre otros. Este inventario debe incluir la identificación de cada dispositivo y los datos de sus respectivos responsables y/o propietarios.
- Los propietarios y custodios de los medios removibles deben asegurarse de que estos no queden desatendidos, ya que pueden ser susceptibles a pérdida o robo.
- La protección a los medios debe hacerse de acuerdo con el nivel de clasificación de la información definida por la entidad.

- Todos los medios de almacenamiento removibles deben ser almacenados en un ambiente seguro, conforme a las especificaciones proporcionadas por los fabricantes.
- En caso de que la información contenida en los medios removibles de la Entidad ya no sea requerida, se debe solicitar y aplicar técnicas de borrado seguro para que estos puedan ser reutilizados, de acuerdo con la guía G-A-GTI-04 BORRADO SEGURO.
- La OTIC realizará el control de los dispositivos removibles a través de la consola de antivirus u otras herramientas disponibles.

8.3.2 Disposición de los medios

Control: Se debe disponer en forma segura de los medios cuando ya no se requieran, utilizando procedimientos formales.

- La Entidad cuenta con el documento G-A-GTI-04 BORRADO SEGURO, que proporciona lineamientos sobre como borrar o eliminar de manera adecuada toda información que no sea requerida o que no sea útil en los medios de almacenamiento.
- Todo funcionario, contratista, proveedor o tercero que tenga acceso a la información debe seguir el proceso establecido de solicitud de borrado, a través de la plataforma de Mesa de Asistencia, donde deberá presentar una solicitud formal especificando el objeto de la misma.
- La OTIC debe validar que, una vez terminado el ciclo de vida útil de un medio de almacenamiento determinado, la información en él sea eliminada de forma segura, posteriormente a la generación del backup de dicha información.
- Se deben tener en cuenta los lineamientos establecidos en la documentación actualizada para la disposición de dispositivos tecnológicos RAEE, en relación con los equipos y medios de almacenamiento que se den de baja.

8.3.3 Transferencia de medios físicos

Control: Los medios que contienen información, se debe proteger contra acceso no autorizado, uso indebido o corrupción durante el transporte.

- El servidor público, contratista, proveedor y/o tercero debe acatar el instructivo I-E-GET-06 Cifrado de Archivos Confidenciales de Acceso Restringido, el cual ha sido documentado, aprobado e implementado por la OTIC. La Entidad contará con servicios de transporte de los medios de almacenamiento, los cuales deberán definirse y gestionarse de acuerdo con la clasificación de la información contenida en ellos, para ello se deberá:
    - Utilizar servicios de mensajería confiables.
    - Verificar los tipos de monitoreo para la transferencia de medios físicos. Verificar si se realizan técnicas de embalaje.
    - Llevar un registro correspondiente de los medios físicos que son transportados.

- Tener en cuenta que la Entidad tiene un contrato de transporte y servicios de mensajería con la empresa 4/72.

9 CONTROL DE ACCESO

9.1 Requisitos del Negocio para Control de Acceso

Objetivo: Limitar el acceso a información y a instalaciones de procesamiento de información.

9.1.1 Política de control de acceso

Control: Se debe establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de seguridad de la información.

- La Entidad debe definir una política que determine los criterios para establecer quien accede a la información de la Entidad, así como la implementación de los controles necesarios para el acceso a la infraestructura tecnológica como son: redes, correo, internet, sistemas de información, información digital o física y de esta manera proteger la confidencialidad, integridad y disponibilidad de la información.
- La Entidad debe suministrar y garantizar el cambio de contraseña a los usuarios, las credenciales para el acceso a los servicios de red y sistemas de información a los que hayan sido autorizados, según su perfil y rol, las credenciales de acceso son de uso personal e intransferible.
- La Entidad debe establecer medidas de control de acceso físico y lógico para los servidores públicos, contratistas y proveedores y partes interesadas a través de mecanismos de identificación, autenticación y autorización de acceso, a nivel de red, sistemas de información, bases de datos y servicios de tecnologías de información de acuerdo con los perfiles y cargos establecidos en la Entidad.
- La gestión de contraseñas de usuarios privilegiados o super usuarios (Administrador), se debe realizar de acuerdo con lo establecido en el Manual General de Operaciones de Infraestructura de TI (Anexo 17). Documento confidencial de Seguridad OTIC
- Todas las contraseñas de usuarios privilegiados o super usuarios (Administrador) de los servicios tecnológicos, se deben proteger y almacenar de acuerdo con lo establecido en Manual General de Operaciones de Infraestructura de TI (Anexo 17). Documento confidencial de seguridad OTIC
- El Grupo de Talento Humano y el Grupo de Contratos, deben informar a través de la herramienta de mesa de asistencia GEMA, lo referente a novedades o situaciones administrativas que concluyan en la separación, temporal o definitivas del cargo de,

funcionarios, contratistas y partes interesadas, lo anterior con el objeto de que dichos usuarios sean deshabilitados o suspendidos oportunamente, según fuere el caso.

9.1.2 Acceso a redes y a servicios en red

Control: Solo se debe permitir acceso de los usuarios a la red y a los servicios de red para los que hayan sido autorizados específicamente por el jefe inmediato o supervisor del contrato.

- La OTIC debe establecer una segregación de las redes, separando los entornos de red de usuarios de los entornos de red de servidores y servicios publicados. Manual General de Operaciones de Infraestructura de TI (Anexo 1.) Documento confidencial de seguridad OTIC
- La OTIC debe establecer los protocolos de autorización para determinar a quién se permite el acceso a qué redes y servicios de red. **G-A-GTI-05** Guía del Uso de la Red e Internet, Directorio Activo, F2A, MFA para algunos sistemas de información.
- La Entidad debe establecer medidas para evitar la conexión o instalación, tanto, de manera cableada como inalámbrica a la red LAN de la Entidad, cualquier dispositivo fijo o móvil que no sean autorizados por La OTIC de acuerdo con lo establecido en el Manual General de Operaciones de Infraestructura de TI (Anexo 2). Documento confidencial de seguridad OTIC
- La conexión remota a la red de área local de la Entidad debe establecerse a través de una conexión VPN, la cual debe ser aprobada, registrada y monitoreada por La OTIC. Manual General de Operaciones de Infraestructura de TI (Anexo 2). Documento confidencial de seguridad OTIC
- La OTIC debe otorgar a los usuarios, únicamente los accesos solicitados y autorizados por el jefe inmediato, supervisor del contrato o un jefe de mayor jerarquía de conformidad con lo estipulado en el Manual General de Operaciones de Infraestructura de TI (Anexo 14). Documento confidencial de seguridad OTIC
- La OTIC debe establecer los requisitos de autenticación de usuarios para acceder a diversos servicios de red. **G-A-GTI-05** Guía del Uso de la Red e Internet, Directorio Activo, F2A, MFA para algunos sistemas de información.

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.

9.2.1 Registro y cancelación del registro de usuarios

Control: Se debe implementar un proceso formal de registro y de cancelación de registro de usuarios, para posibilitar la asignación de los derechos de acceso.

- La OTIC debe definir y documentar los lineamientos para la gestión de usuarios donde se contemple la creación, actualización, activación e inactivación de dichas cuentas, así como el control de acceso lógico. Manual General de Operaciones de Infraestructura de TI (Anexo 14). Documento confidencial de seguridad OTIC
- La OTIC debe identificar y eliminar o deshabilitar periódicamente las identificaciones de usuario redundantes. Manual General de Operaciones de Infraestructura de TI (Anexo 14). Documento confidencial de seguridad OTIC
- La OTIC debe verificar, controlar y restringir los accesos físicos y lógicos de los servidores públicos, contratistas o terceros que de alguna manera terminan la vinculación laboral con la Entidad; y deben diligenciar en su totalidad el formato **F-A-ATH-06** Legalización Retiro del Servicio.
- La OTIC debe suspender el acceso a los sistemas de todo funcionario o colaborador de la Entidad que se encuentre en alguna situación administrativa que implique ausencia temporal, como licencia, permisos o vacaciones. Excepcionalmente y si hay funciones que se deban reasignar para garantizar la continuidad durante dichas ausencias, los jefes o delegados deben solicitar el acceso necesario para los colaboradores que ejecutarán las actividades. Una vez cumplido el plazo, se debe solicitar el retiro de los permisos. Manual General de Operaciones de Infraestructura de TI (Anexo 14). Documento confidencial de seguridad OTIC

9.2.2 Suministro de acceso de usuarios

Control: Se debe implementar un proceso de suministro de acceso formal de usuarios para asignar o revocar los derechos de acceso para todo tipo de usuarios para todos los sistemas y servicios.

- La OTIC debe establecer los privilegios para el control de acceso lógico de cada usuario o grupo de usuarios a los recursos y servicios tecnológicos y los sistemas de información. Así mismo, velará porque los servidores públicos, contratistas, proveedores y partes interesadas tengan acceso únicamente a la información necesaria para el desarrollo de sus labores y porque la asignación de los derechos de acceso esté regulada con procedimientos establecidos para tal fin. Manual General de Operaciones de Infraestructura de TI (Anexo 14). Documento confidencial de seguridad OTIC
- La OTIC debe asignar los privilegios a los usuarios de acuerdo con los roles y responsabilidades, según lo establecido en el formato asignación o modificación de usuarios. La vigencia de estos privilegios podrá ser modificada solo cuando sea necesario y debe contar con autorización del jefe inmediato o Supervisor del Contrato. Manual General de Operaciones de Infraestructura de TI (Anexo 14). Documento confidencial de seguridad OTIC
- La OTIC debe establecer identificaciones únicas para los usuarios, que les permita estar vinculados a sus acciones y mantener la responsabilidad por ellas; el uso de identificaciones compartidas solo se debe permitir cuando sea necesario por razones operativas o del negocio, y se aprueban y documentan. Manual General de Operaciones de Infraestructura de TI (Anexo 14). Documento confidencial de seguridad OTIC

- La OTIC debe mediante la información que suministra el proceso de talento humano sobre el perfil del funcionario o contratista, realizar el registro y creación de los usuarios para los distintos sistemas de información, esto se hará mediante la Herramienta GEMA.

9.2.3 Gestión de derechos de acceso privilegiado

Control: Se debe restringir y controlar la asignación y uso de derechos de acceso privilegiado.

- La OTIC debe mantener un listado actualizado con las cuentas que administren todos los recursos tecnológicos. La asignación de privilegios está ligada al perfil de cargo del funcionario, contratista o tercero.
- La OTIC debe otorgar los privilegios para administración de recursos tecnológicos, servicios de red y sistemas de información sólo a aquellos funcionarios y contratistas designados para dichas labores, entregando cuentas personalizadas y/o genéricas a cada uno de los administradores.
- La OTIC debe, definir los requisitos para la expiración de los derechos de acceso privilegiado para el en el caso de los contratistas las cuentas del Directorio Activo se configuran desde su creación para su bloqueo con la fecha de finalización del contrato.
- La OTIC debe definir, documentar y registrar la autorización de todos los privilegios asignados. Sólo se suministran los derechos de acceso cuando el proceso de autorización esté completo. Adicional a lo anterior, se deben definir los requisitos para la expiración de los derechos de acceso privilegiado.
- Para el acceso a los activos de TI (infraestructura), la Entidad debe gestionar acuerdos de confidencialidad para los roles de DBA, Redes y Servidores.

9.2.4 Gestión de información de autenticación secreta de usuarios.

Control: La asignación de información de autenticación secreta se debe controlar por medio de un proceso de gestión formal.

- Los servidores públicos y contratistas deben mantener estricto control y confidencialidad de la información secreta de sus credenciales (contraseñas de las cuentas de usuario y accesos a sistemas de información). Manual General de Operaciones de Infraestructura de TI (Anexo 14). Documento confidencial de seguridad OTIC

9.2.5 Revisión de los derechos de acceso de usuarios

Control: Los propietarios de los activos debe revisar los derechos de acceso de los usuarios, a intervalos regulares.

- La OTIC debe administrar de los perfiles de usuario y cuya responsabilidad es responsabilidad de los administradores de cada aplicación o sistema.

- Los funcionarios, contratistas, proveedores y partes interesadas de la Entidad deben reportar cualquier sospecha de que una persona esté utilizando una contraseña o un usuario que no le pertenece en la herramienta de la Mesa de servicios como incidente de Seguridad de Información.
- La OTIC debe definir los requisitos para la expiración de los derechos de acceso de los contratistas. Estos requisitos deben asegurar que las cuentas del Directorio Activo se bloqueen automáticamente cuando finalice el contrato. Así se evita el acceso no autorizado a los recursos de la organización. Manual General de Operaciones de Infraestructura de TI (Anexo 14). Documento confidencial de seguridad OTIC
- La OTIC debe otorgar a los servidores públicos, contratistas, proveedores y partes interesadas solamente el acceso a los servicios de red y a los sistemas de información que hayan sido autorizados y que sean necesarios para el desarrollo de sus funciones, obligaciones o actividades.
- La OTIC debe revisar los derechos de acceso de los usuarios a intervalos regulares y después de cualquier cambio, promoción, cambio a un cargo a un nivel inferior, o terminación del empleo.
- El jefe de área o dependencia debe definir los permisos que correspondan a cada perfil y será responsable por el otorgamiento de los permisos de acceso a los recursos de la plataforma tecnológica, servicios de red, los sistemas de información y áreas seguras.
- Se deben establecer controles de acceso a los ambientes de desarrollo, pruebas y producción de los sistemas de información y garantizar que solo el personal autorizado tenga los privilegios necesarios para el acceso tanto a los ambientes como a la información.

9.2.6 Retiro o ajuste de los derechos de acceso

Control: Los derechos de acceso de todos los empleados y de usuarios externos a la información y a las instalaciones de procesamiento de información se debe retirar al terminar su empleo, contrato o acuerdo, o se debe ajustar cuando se hagan cambios.

- La Entidad debe revisar los derechos de acceso, que tiene cada funcionario, contratista o tercero, ya sean lógicos o físicos, y actualizarlos según corresponda cuando se produzca algunas de las siguientes situaciones: cambio de cargo, traslado de dependencia o área, cambios de puesto de trabajo dentro de la misma Entidad o cambio en la modalidad de empleo.
- La OTIC debe revocar los derechos de acceso, físicos y lógicos, de cualquier funcionario, contratista o tercero que se separe de la entidad. Esta acción se realiza mediante el formato **F-A-ATH-06** Control de Retiro del Servicio.

9.3 Responsabilidades de los Usuarios

Objetivo: Hacer que los usuarios rindan cuentas por la salvaguarda de su información de autenticación.

9.3.1 Uso de información secreta para la autenticación.

Control Se debe exigir a los usuarios que cumplan las prácticas de la Entidad para el uso de información secreta para la autenticación.

- La OTIC debe impedir que los colaboradores y contratistas usen contraseñas predecibles o fáciles de deducir, como palabras de diccionario, derivados de sus identificadores, secuencias comunes de caracteres, detalles personales o partes gramaticales. Manual General de Operaciones de Infraestructura de TI (Anexo 14.) Documento confidencial de seguridad OTIC
- La OTIC debe asegurar que los funcionarios, contratistas o terceros no compartan o divulguen sus contraseñas. Para ello, deben cumplir con las siguientes medidas: exigir el cambio de contraseña inicial, las contraseñas deben ser lo suficientemente complejas, exigir que las contraseñas se cambien con regularidad, prohibir compartir contraseñas y evitar escribir las contraseñas en lugares visibles. Manual General de Operaciones de Infraestructura de TI (Anexo 14). Documento confidencial de seguridad OTIC
- Todos los servidores públicos, contratistas y partes interesadas bajo ningún motivo deben prestar su usuario y contraseña para acceder al equipo y/o aplicaciones de la Entidad. Manual General de Operaciones de Infraestructura de TI (Anexo 14). Documento confidencial de seguridad OTIC
- La OTIC debe cambiar la contraseña de los distintos usuarios en donde se descubra una amenaza: La contraseña debe cambiarse inmediatamente ante la sospecha de una amenaza de seguridad, como un ataque de fuerza bruta o un acceso no autorizado a la cuenta.
- La OTIC debe almacenar las contraseñas de forma segura, ya sea en memoria o en un archivo.
- Las acciones que se realicen con una cuenta usuario en los sistemas de información serán total responsabilidad del usuario.
- Después de (3) tres intentos fallidos al ingresar los datos de acceso, la cuenta debe quedar bloqueada, y sólo podrá ser desbloqueada por los responsables de soporte tecnológico de la OTIC.
- Se debe implementar mecanismos de múltiple factor de autenticación en los servicios de TI que lo permitan.

9.4 Control de Acceso a Sistemas y Aplicaciones

Objetivo: Evitar el acceso no autorizado a sistemas y aplicaciones.

9.4.1 Restricción de acceso a la información

Control: El acceso a la información y a la funcionalidad de las aplicaciones se debe restringir de acuerdo con la política de control de acceso.

- Se debe contar con mecanismos de control de acceso para las áreas seguras (centro de cómputo, centro de cableado, y oficinas que almacenen información reservada); tales como cámaras, puertas de seguridad, sistemas de control con lectores biométricos, sistema de alarmas, llaves, entre otras, que la Entidad considere pertinentes.
- La OTIC debe aplicar mecanismos de control de acceso basado en roles, considerando los siguientes aspectos: definición de roles, asignación de derechos de acceso, administración de derechos de acceso, separación de funciones, autorización formal, revisión periódica y retiro de derechos de acceso. Asimismo, debe aplicar controles específicos para los roles de acceso privilegiado, como requisitos de aprobación adicionales y revisiones periódicas a dichos accesos.
- La OTIC o los terceros que desarrollen sistemas de información o servicios tecnológicos para la Entidad deben garantizar que el acceso a estos sea restringido y controlado mediante el uso de usuario y contraseña de dominio. Así mismo, el acceso debe estar limitado a las tareas, funciones, responsabilidades u obligaciones que correspondan a los funcionarios, contratistas y terceros de la entidad.
- Las puertas de acceso al centro de cómputo, centros de cableado u otras áreas que alberguen información crítica, deben permanecer siempre cerradas y aseguradas. De igual manera, los gabinetes y puertas de los equipos que se encuentran en las áreas mencionadas deben permanecer cerrados.
- La OTIC debe solicitar y garantizar que los Sistemas de Información y Aplicaciones de la Entidad, tenga establecidos “Time Out”, es decir que después de determinados minutos de inactividad previamente establecidos, se cierren. Esto debe estar tanto para las Aplicaciones locales y web

  La OTIC debe asegurar que los sistemas de información y aplicaciones de la Entidad cuenten con menús que regulen el acceso a la información como a las diferentes funciones, de acuerdo con las necesidades y roles de cada usuario. De esta forma, se garantiza que los usuarios solo puedan realizar las tareas que les corresponden y solo puedan ver los menús y funciones a los que tienen autorización.

9.4.2 Procedimiento de ingreso seguro

Control: Cuando lo requiere la política de control de acceso, el acceso a sistemas y aplicaciones se debe controlar mediante un proceso de ingreso seguro.

- Toda solicitud de acceso a sistemas y aplicaciones debe hacerse mediante el procedimiento a través de la plataforma GEMA.

- Los sistemas de información, y las aplicaciones que los integran, deberán disponer de la autenticación multifactor (F2A por sus siglas en inglés).
- La OTIC debe registrar todos los intentos de acceso al directorio activo, tanto exitosos como fallidos, para medir la eficacia del control.
- Cuando se cambien las contraseñas, los sistemas de información o aplicaciones integrados al único punto de autenticación deben cerrar automáticamente todas las sesiones activas.
- Los sistemas de información o aplicaciones que se integren al SSO debe registrar y monitorear los eventos de autenticación y autorización para detectar y responder a las actividades sospechosas de manera oportuna, mediante el cual se pueda identificar los intentos de acceso no autorizado y proporcionar información útil para las investigaciones de seguridad.

9.4.3 Sistema de gestión de contraseñas

Control: Los sistemas de gestión de contraseñas debe ser interactivos y debe asegurar la calidad de las contraseñas.

- La OTIC debe establecer y documentar los lineamientos para implementar los controles para la gestión de contraseñas, requisitos de longitud y complejidad, de cambio periódico de uso de contraseñas únicas, de bloqueo, de recordatorio de cambio de contraseña.
- Las contraseñas que se utilizan en la infraestructura de la OTIC deben ser creadas de acuerdo con las normas y políticas fijadas por La Entidad. Para ello, se aplicarán controles y herramientas como generadores de contraseñas que permitan asegurar el cumplimiento mínimo de seguridad, según lo establecido en el Manual General de Operaciones de Infraestructura (Anexo 17). Documento confidencial de seguridad OTIC
- La información correspondiente a la autenticación de los usuarios es de uso personal e intransferible, por tal motivo es responsabilidad de cada funcionario, contratista o externo dar el uso adecuado a la misma.

9.4.4 Uso de programas utilitarios privilegiados

Control: Se debe restringir y controlar estrictamente el uso de programas utilitarios que podrían tener capacidad de anular el sistema y los controles de las aplicaciones.

- Los servidores públicos y los contratistas deben abstenerse de usar programas utilitarios que puedan alterar el funcionamiento del sistema o sus controles, así como software o aplicaciones que no cuenten con la autorización previa de la OTIC y el jefe de la dependencia o el supervisor del contrato.
- El uso de herramientas o utilitarios propios de los sistemas operativos debe ser limitado a personal autorizado y su uso está restringido en casos específicos y debe disponerse de la

trazabilidad de las operaciones realizadas en los casos que son autorizados. (GEMA y Consola Antivirus).

9.4.5 Control de acceso a códigos fuente de programas

Control: Se debe restringir el acceso a los códigos fuente de los programas.

- La OTIC debe definir y documentar los criterios que determinen quién puede acceder al código fuente, cómo se administra el acceso y qué acciones están permitidas. Además, se debe garantizar un control de acceso físico y lógico, una segmentación de redes que aísle el entorno donde se almacena el código fuente y una auditoría o seguimiento periódico a la gestión de cambios, que incluya revisión y aprobación. M-E-GET-04 Manual de Políticas Específicas de Seguridad y Privacidad de la Información.
- El código fuente debe estar protegido con acceso restringido mediante el uso de librerías fuente. El código fuente no debería protegerse con aplicaciones de red.

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.

10.1.1 Política sobre el uso de controles criptográficos

Control: Se debe desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información.

- La dependencia encargada debe buscar mecanismos y herramientas para la trasmisión de la información considerada como reservada o de acceso restringido mediante técnicas de cifrado con el propósito de proteger su confidencialidad e integridad para esto implementará sistemas de cifrado como aplicativos que permitan llevar a cabo el procedimiento para el manejo de la información al igual que establecer estándares y normas de controles criptográficos.
- Se debe documentar los pasos necesarios para el registro, generación, distribución, almacenamiento, recuperación, renovación, revocación y destrucción de las claves criptográficas y debe mantener un registro de actividad que evidencie su cumplimiento y permita su posterior revisión o auditoría.

- Los aspectos importantes que se debe tener en cuenta para el uso de los controles criptográficos son:
    - Para la Información clasificada (confidencial) y/o Reservada (altamente confidencial) de la Entidad.
    - Para las líneas de comunicación por donde se almacena, procesa y transmite la información Clasificada y/o reservada.
    - Las herramientas y mecanismos de cifrado definidas por la Entidad.
    - Para cumplimiento de los Requisitos legales.

Para los tokens de Seguridad suministrados a los servidores y/o colaboradores, para realizar consulta, modificación, trasmisión de información, pagos, entre otros fines:

- Se debe guardar en un lugar seguro bajo llave, libre de acceso al mismo por personal no autorizado.
- No se debe dejar desatendido cuando el usuario se encuentre ausente del puesto de trabajo.
- No se puede prestar el token ni suministrar la clave bajo ninguna circunstancia.
- No se debe utilizar fuera de las instalaciones de la Entidad.
- No se debe utilizar en horario no laboral sin previa autorización escrita del jefe o supervisor de contrato.
- Si el token se bloquea por intentos fallidos por el uso del mismo se debe solicitar el desbloqueo a la Entidad "Administradora" del mismo, previo a solicitud a través de la mesa de asistencia.

10.1.2 Gestión de llaves

Control: Se debe desarrollar e implementar una política sobre el uso, protección y tiempo de vida de las llaves criptográficas durante todo su ciclo de vida.

- Las llaves públicas de encriptación debe considerar la política de gestión de contraseñas para su generación; esta se hará aplicando procesos de expiración acorde a los criterios establecidos para cada herramienta de encriptación y desencriptación, en los cuales se debe configurar tiempo para la expiración de la llave no superior a los 90 días y esta debe ser reemplazada cada vez que las personas dueñas del proceso sean sustituidos del cargo o al momento de efectuar controles de cambios en las configuraciones de las herramientas.
- Se debe contar con el M-E-GET-04 Manual de Políticas Específicas de Seguridad y Privacidad de la Información.

11 SEGURIDAD FÍSICA 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 Entidad.

11.1.1 Perímetro de seguridad física

Control: Se debe definir perímetros de seguridad, y usarlos para proteger áreas que contengan información sensible o crítica, e instalaciones de manejo de información. Para la Entidad se definen las siguientes áreas seguras:

- **Datacenter**: corresponde al centro de procesamiento de datos en donde se albergan los sistemas de información (aplicaciones, bases de datos), los componentes de telecomunicaciones y los sistemas de almacenamiento (servidores físicos y virtuales).
- **Centros de Cableado**: áreas de unión central que se usan para conectar los dispositivos de la red del área local (LAN) el cual alberga paneles de conexión, Hubs de cableado, Switches, Router, Puentes, entre otros.
- **Cuartos de Suministro**: áreas en donde se ubican los servicios de suministro como las UPS y la planta eléctrica.
- **Archivo Físico Central**: áreas en MinAmbiente donde se administran, custodian y conservan los documentos físicos con valor administrativo, legal, permanente, histórico, entre otros, que son transferidos por las diferentes oficinas.
- **Archivo Físico de Gestión**: Hace referencia a aquella documentación todavía en trámite que conservan las oficinas, así como a aquella que aún después de finalizado el procedimiento administrativo, está sometida a uso continuo y consulta administrativa por las mismas oficinas, o los que aún no han podido ser trasladados al archivo central, aplicando para ello lo dispuesto en las tablas de retención documental.
- **Oficinas**: todas aquellas dependencias y áreas de la Entidad, que por sus competencias funcionales manejan información Clasificada (confidencial) y/o Reservada (altamente confidencial), serán consideradas “Áreas Seguras”, para lo cual debe adoptarse los mecanismos tendientes para asegurar dicha información. Por todo lo expuesto, se debe adoptar por lo menos los controles definidos en el “Numeral 11.1.2. Controles de Acceso Físico”, según su nivel de riesgo y capacidades institucionales.
- Se debe contar con mecanismos de control de acceso para las áreas seguras (centro de cómputo, centro de cableado, y oficinas que almacenen información reservada), tales como cámaras, puertas de seguridad, sistemas de control con lectores biométricos, torniquetes en acceso peatonal y registro en las entradas vehiculares.
- Se deben seguir los lineamientos definidos en el documento: G-A-GSA-03 Protocolo de Seguridad Ministerio de Ambiente y Desarrollo Sostenible.

- En cada piso de la Entidad se deberá contar con un recurso de la compañía de vigilancia encargado de llevar un registro del personal que ingrese al mismo.

11.1.2 Controles de acceso físicos

Control: Las áreas seguras se debe proteger mediante controles de acceso apropiados para asegurar que solo se permite el ingreso a personal autorizado.

- La OTIC debe aprobar de previamente las solicitudes de acceso al centro de cómputo, a las áreas consideradas como seguras, así como a la administración de infraestructura a los centros de cableado; además es necesario que los visitantes sean acompañados permanentemente durante su estancia en estas áreas.
- Los visitantes deben registrarse en una bitácora, ya sea manual o sistematizada, proporcionada por el personal de la empresa de seguridad.
- El personal de la empresa de seguridad encargado de la vigilancia de las instalaciones debe contar con un procedimiento que permita a las áreas informar y autorizar la entrada de visitantes. Este procedimiento debe incluir la identificación de la persona responsable del visitante, la necesidad de acompañamiento, el motivo de la visita, así como la fecha y la hora de ingreso y salida.
- Las áreas seguras, según su nivel de criticidad, deben contar con barreras, puertas o elementos que restrinjan el acceso a personal no autorizado, implementando mecanismos de autenticación e incluso un segundo factor de autenticación cuando sea necesario.
- Los sistemas biométricos y las tarjetas de acceso deben ser verificados y depurados al menos una vez al año por el área responsable de su administración.
- Se deben seguir los lineamientos definidos en los documentos: G-A-GSA-03 Protocolo de Seguridad Ministerio de Ambiente y Desarrollo Sostenible y M-E-GET-04 Manual de Políticas Específicas de Seguridad y Privacidad de la Información.

11.1.3 Seguridad de oficinas, recintos e instalaciones

Control: Con el propósito de mantener la Confidencialidad, Integridad y Disponibilidad de la Información en las Oficinas, recintos e instalaciones, es necesario establecer y dar cumplimiento a las siguientes directrices de Seguridad.

Los suministros de papelería no deben almacenarse en áreas seguras como el datacenter, centros de cableado, cuarto de suministro, archivo físico central y archivo físico de gestión.

Las áreas seguras como: datacenter, centros de cableado, cuarto de suministro, archivo físico central y archivo físico de gestión, no deben ser utilizados como bodega de almacenamiento de otros elementos no relacionados con su fin específico.

Las salidas de emergencia deben estar identificadas, señalizadas y socializadas conforme lo indica en plan de emergencia.

- Se deben proteger las áreas de centro de cómputo y los centros de cableado con instalaciones de seguridad físicas robustas.
- Para el acceso a los centros de cableado, se debe diligenciar la bitácora de ingreso y salida. Esto medida aplicará para los servidores públicos, contratistas, proveedores y partes interesadas de la entidad.
- Todos los servidores públicos, contratistas, y partes interesadas deben presentar su carné o documento de identificación, según corresponda, para el ingreso a las instalaciones de la entidad.
- Se debe Implementar el uso de chapas de seguridad en las puertas de las áreas seguras para garantizar que permanezcan cerradas.
- La Entidad cuenta con los documentos **G-A-GSA-03** Protocolo de Seguridad Ministerio de Ambiente y Desarrollo Sostenible, **DS-E-GET-37** Política General de Seguridad de la Información y el **M-E-GET-04** Manual de Políticas Específicas de Seguridad y Privacidad de la Información, cuyos lineamientos deben ser acatados por los servidores públicos, contratistas, y partes interesadas.
- Se debe garantizar de manera anónima la confidencialidad de las áreas físicas en donde se procesa información sensible.
- Todas las oficinas, áreas o dependencias de la Entidad que procesen, almacenen y/o gestionen información clasificada y/o reservada deben implementar y adoptar las medidas tendientes a asegurar dicha información.

11.1.4 Protección contra amenazas externas y ambientales

Control: Se debe diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes. Se debe contar con soluciones de control de incendios, sistemas de precisión ambiental.

- La Entidad debe proporcionar las condiciones físicas y medio ambientales necesarias para garantizar la protección de las personas y a la seguridad de la información, ante posibles eventos como incendios, inundaciones, terremotos, explosiones, ataques maliciosos, entre otros. Por lo tanto, se debe dar cumplimiento a los siguientes lineamientos:
- El Grupo de Servicios Administrativos y el Grupo de Talento Humano por medio del área de Seguridad y Salud en el Trabajo debe hacer una revisión periódica de las condiciones físicas de las áreas seguras y de procesamiento de información, generando las recomendaciones para el cumplimiento normativo correspondiente.
- La OTIC debe garantizar la seguridad del datacenter y centros de cableado que estén bajo su custodia, asegurándose que estén separados de áreas que contengan líquidos inflamables o que presenten riesgo de inundaciones e incendios.
- En el datacenter, centros de cableado y archivos documentales deben existir sistemas de control ambiental de temperatura, sistemas de detección y extinción de incendios, sistemas

de descarga eléctrica, sistemas de vigilancia, monitoreo, y alarmas en caso de detectarse condiciones ambientales inapropiadas. Estos sistemas se deben monitorear de manera permanente.

- El propietario del activo de información debe velar porque la información se almacene en un ambiente protegido y seguro.
- El Grupo de Servicios Administrativos y el Grupo de Talento Humano deben definir un plan de emergencias, el cual debe ser probado anualmente para garantizar la protección contra amenazas externas.

11.1.5 Trabajo en áreas seguras

Control: Se debe diseñar y aplicar procedimientos para trabajo en áreas seguras.

- Los servidores públicos, contratistas y proveedores solo deben conocer de la existencia de un área segura o de actividades dentro de la misma, con base en las necesidades de sus responsabilidades.
- Las actividades ejecutadas en las áreas seguras solamente deben ser conocidas por los servidores públicos, contratistas, proveedores y partes interesadas autorizadas que las ejecutan o supervisan de acuerdo con su rol.
- Todas las actividades ejecutadas al interior de un área segura deben ser supervisadas por el responsable de esta o por quien asigne la jefatura de la OTIC.
- Las áreas seguras vacías deben estar cerradas con llave y deben ser revisadas periódicamente por el personal de la empresa de vigilancia.
- No se debe permitir equipo fotográfico, de video, audio u otro equipo de grabación, tales como cámaras en dispositivos móviles al interior de las áreas seguras, a menos que se cuente con autorización para ello.

11.1.6 Áreas de despacho y carga

Control: Se debe controlar los puntos de acceso tales como áreas de despacho y de carga, y otros puntos en donde pueden entrar personas no autorizadas, y si es posible, aislarlos de las instalaciones de procesamiento de información para evitar el acceso no autorizado.

- El área de carga y despacho debe estar previamente señalizada y definida de manera clara.
- La recepción y despacho de carga deben ser controlados por el grupo de servicios administrativos y la empresa de vigilancia de la Entidad, dentro de los horarios establecidos para la realización de estas actividades, y en ningún caso deben llevarse a cabo cerca de las áreas consideradas como seguras.
- Si la puerta de acceso al área de despacho y carga está al interior de la Entidad, ésta deberá permanecer cerrada y con control de acceso restringido.
- Las puertas externas deben permanecen cerradas mientras se efectúa el cargue o despacho.

- Se debe restringir los accesos al área de carga y descarga desde fuera de las instalaciones y permitir su acceso solamente al personal autorizado y debidamente identificado.
- Las áreas de entrega de reciclaje deben ser monitoreadas y custodiadas por el personal de vigilancia, junto con un delegado del Grupo de Servicios Administrativos y del área interesada, durante el proceso de entrega.

11.2 Equipos

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

11.2.1 Ubicación y protección de los equipos

Control: Los equipos deben estar ubicados y protegidos para reducir los riesgos de amenazas y peligros del entorno, y las posibilidades de acceso no autorizado.

- Los equipos de procesamiento de información como servidores, equipos de comunicaciones deben ser ubicados en áreas seguras.
- Los computadores portátiles y de escritorio tipo “todo en uno” asignados a los servidores públicos y contratistas deben ser entregados con guaya de seguridad, según disponibilidad, para permitir su anclaje en el puesto de trabajo, con el fin de mitigar el riesgo de pérdida o robo de este.
- Los equipos que contengan o manejen información clasificada (confidencial) o reservada (altamente confidencial), deben estar ubicados en áreas donde el acceso sea restringido.
- Las condiciones ambientales en las instalaciones donde se encuentran los servidores (datacenter) y equipos activos, como switches, enrutadores, entre otros, deben ser adecuadas y contar con aire acondicionado, detector de humo y alarma contra incendios.
- Está prohibido el consumo de bebidas y alimentos en las instalaciones de procesamiento de información.
- Está prohibido fumar dentro de las instalaciones de la Entidad.
- Las impresoras, fotocopiadoras, scanners y/o multifuncionales que procesen información interna, confidencial (clasificada) y/o altamente confidencial (reservada) deben ubicarse en áreas seguras para prevenir accesos y transmisiones no autorizadas o duplicación de documentos.

11.2.2 Servicios de suministro

Control: Los equipos se deben proteger contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro.

- Se debe cumplir con las especificaciones de los fabricantes de equipos de soporte ambiental y eléctrico, así como los requisitos legales locales.
- Los servicios de suministro como, electricidad, agua, alcantarillado, aire acondicionado, ventilación/calefacción deben ser inspeccionados regularmente por el Grupo de Servicios Administrativos o por un tercero, para garantizar su correcto funcionamiento.
- Frente a posibles fallas en el suministro de energía para los equipos de la Entidad, especialmente aquellos que soportan las operaciones críticas para la continuidad de las actividades y servicios, se deben implementar sistemas de suministro eléctrico respaldado por fuentes de energía interrumpible, como UPS.

    Se debe monitorear periódicamente, en articulación entre la OTIC y el Grupo de Servicios Administrativos el funcionamiento de los equipos de soporte, verificando que cumplan con requisitos de configuración y capacidad recomendados por el fabricante, por ejemplo, en el caso de UPS, aire acondicionado, planta eléctrica, entre otros. El mantenimiento de las plantas eléctricas es responsabilidad del Grupo de Servicios Administrativos.

11.2.3 Seguridad del cableado

Control: El cableado de energía eléctrica y de telecomunicaciones que porta datos o brinda soporte a los servicios de información debe estar protegido contra interceptación, interferencia o daño.

- Se debe contar con cableado estructurado, canaletas de fin específico y un sistema eléctrico regulado.
- El Grupo de Servicios Administrativos y la OTIC, deben garantizar que, dentro de la infraestructura física de la Entidad, el cableado de energía eléctrica y de telecomunicaciones que transporta datos o soporta los servicios de información estén protegidos para evitar daños o manipulaciones indebidas.
- Las áreas de distribución de redes (eléctricas y comunicaciones) deben estar físicamente aseguradas para prevenir modificaciones o accesos no autorizados a las mismas.
- Se debe contar con un sistema eléctrico regulado para la conexión de todos los activos tecnológicos.

11.2.4 Mantenimiento de equipos

Control: Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.

- La Entidad debe contar con planes de mantenimiento que incluyan las condiciones definidas por las aseguradoras, requisitos técnicos de los equipos, definiciones de ventanas de tiempo, entre otros, para todos los equipos que soporten los procesos de la Entidad.

- La instalación de cualquier tipo de software en los equipos de la Entidad es responsabilidad de la OTIC, que es la única autorizada para realizar y/o autorizar esta labor, la cual se llevará a cabo con el usuario administrador del equipo local.
- Los usuarios no deben realizar cambios en los equipos de la Entidad incluyendo la configuración del equipo, las conexiones de red, el papel tapiz, el protector y fondo de pantalla y la plantilla del correo institucional definidos por la Entidad. Estos cambios solo pueden ser realizados por el personal de la Mesa de Asistencia, designado por el administrador de la herramienta GEMA y deben ser solicitados a través de un ticket previamente autorizado.

11.2.5 Retiro de activos

Control: Los equipos, información o software no se debe retirar de su sitio sin autorización previa.

- Todos los servidores públicos, contratistas, colaboradores y partes externas deben estar debidamente autorizados para el retiro o traslado de activos desde el lugar donde se encuentran.
- Para los servidores públicos, contratistas, proveedores y terceros se requiere autorización para la salida del equipo aprobada por el jefe de área donde está ubicado el equipo y/o la persona a quien está asignado. Además, se debe contar con el visto bueno del jefe de la OTIC y el Coordinador del Grupo de Servicios Administrativos. Esta información debe registrarse de acuerdo con lo establecido por la empresa de seguridad encargada de la seguridad física de las instalaciones, de acuerdo con el formato **F-A-GSA-19** Autorización Salida de Elementos.
- Se debe tener como marco de referencia la siguiente documentación: F-A-GSA-02 Movimiento de elementos devolutivos, **G-A-GTI-08** Guía de Apoyo en el Servicio de Backup para usuarios, **G-A-GTI-07** Guía para la Administración de Usuarios en Sistemas de Información, **M-E-GET-04** Manual de Políticas Específicas de Seguridad y Privacidad de la Información.

11.2.6 Seguridad de equipos y activos fuera de las instalaciones

Control: Se debe aplicar medidas de seguridad a los activos que se encuentran fuera de las instalaciones de la Entidad, teniendo en cuenta los diferentes riesgos de trabajar fuera de dichas instalaciones.

Los servidores públicos, contratistas, proveedores y partes interesadas que retiren equipos o medios removibles de las instalaciones del Ministerio deben seguir las siguientes directrices:

- En ninguna circunstancia se deben dejar desatendidos los equipos de cómputo en lugares públicos o a la vista, especialmente si están siendo transportados en un vehículo.

- Las personas autorizadas para retirar cualquier equipo o activo de información de las instalaciones de la Entidad son responsables directos de su protección.
- En caso de presentarse alguna situación que comprometa la confidencialidad, integridad y disponibilidad de la información, como robo, daño, acceso no autorizado, entre otros, se debe reportar la situación como un incidente de seguridad de la información, el cual será tratado de acuerdo con la documentación vigente.
- La Entidad cuenta con el M-A-GSA-01 Manual para el manejo de bienes.

11.2.7 Disposición segura o reutilización de equipos

Control: Se debe verificar todos los elementos de equipos que contengan medios de almacenamiento, para asegurar que cualquier dato sensible o software licenciado haya sido retirado o sobrescrito en forma segura antes de su disposición o reúso.

- Para los equipos que contengan información de carácter confidencial (clasificada) y/o altamente confidencial (reservada), deben aplicarse mecanismos de borrado seguro antes de su disposición o reutilización, con el fin de prevenir el riesgo de acceso no autorizado. Esta actividad se realizará en colaboración entre el área propietaria del activo de información y la Mesa de Asistencia, asegurando que se realice, previamente una copia de seguridad (backup) de la información.
- Antes de cualquier venta, subasta, transferencia o donación, todos los medios de almacenamiento deben ser borrados de acuerdo con los mecanismos de eliminación o borrado seguro de información establecidos por la Entidad, previa generación del backup de la información almacenada.
- Desde la OTIC se deberá contar con la política GPO (Objeto de Política de Grupo) para el bloqueo de equipos.

11.2.8 Equipos de usuario desatendidos

Control: Los usuarios debe asegurarse de que a los equipos desatendidos se les da protección apropiada.

- Todo servidor público, contratista, proveedor o visitante debe asegurarse de no dejar la sesión abierta al ausentarse de su puesto o lugar de trabajo.
- Todo servidor público, contratista, proveedor o visitante antes de alejarse y dejar desatendido el computador o portátil debe bloquear su equipo utilizando las combinaciones de teclas: “Botón de windows + la tecla L” o “Ctrl + ALT+ SUPR + ENTER”.
- Todo servidor público, contratista, proveedor o visitante debe bloquear la sesión y/o cerrar la sesión de usuario al finalizar sus tareas. No es suficiente con simplemente apagar la pantalla o el equipo sin haber cerrado la sesión previamente.

- Los equipos que se encuentren bloqueados deben contar con protector de pantalla establecido por la Entidad, de acuerdo con el tiempo límite de inactividad definida por el administrador.
- Los equipos portátiles y los de escritorio tipo "todo en uno ", deben estar asegurados mediante el uso de una guaya como mecanismo de seguridad física.
- Los dispositivos móviles corporativos y/o personales, a través de los cuales se accede a información de la Entidad de tipo confidencial o interna, deben contar con controles de bloqueo o acceso para evitar el riesgo de fuga de información por parte de personas no autorizadas.
- Como parte del desarrollo del plan de sensibilización y capacitación en temas de seguridad de la información se deberán llevar a cabo charlas relacionadas con esta política.

11.2.9 Política de escritorio y pantalla limpios

Control: Se debe adoptar una política de escritorio limpio para documentos y medios de almacenamiento removibles, así como una política de pantalla limpia en las instalaciones de procesamiento de información.

- Todos los servidores públicos y contratistas deben mantener su escritorio libre de información propiedad de la Entidad que pueda ser accesible, copiada o utilizada por terceros o personal no autorizado. Al retirarse de sus puestos de trabajo se deben contemplar los siguientes lineamientos:
- Es responsabilidad de todos los servidores públicos y contratistas proteger la información cada vez que se alejen de su puesto de trabajo.
- Durante la jornada laboral o al finalizarla, no se deben dejar documentos con información clasificada o reservada al alcance de personal no autorizado. Si se maneja este tipo de información en formato físico, debe guardarse bajo llave y la llave debe ser resguardada en un lugar seguro por un responsable asignado.
- La impresión de documentos con información interna, confidencial (clasificada) y/o altamente confidencial (reservada) de la Entidad debe realizarse a través del mecanismo de control establecido (código o pin). La información debe ser retirada de las impresoras de inmediato por el propietario o la persona autorizada.
- Está prohibido consumir alimentos o bebidas en el puesto de trabajo.
- Como parte del plan de sensibilización y capacitación en temas de seguridad de la información se deberán llevar a cabo charlas relacionadas con esta política.

12. SEGURIDAD DE LAS OPERACIONES

12.1 Procedimientos Operacionales y Responsabilidades

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

12.1.1 Procedimientos de operación documentados

Control: Los procedimientos de operación se debe documentar y poner a disposición de todos los usuarios que los necesitan.

Se debe definir un procedimiento de operación que contemple la operación y administración del centro de cómputo y centros de cableado en donde se documenten las configuraciones e instalaciones de equipos, el manejo de la información manual y automática, y otras condiciones de cumplimiento para la operación adecuada de estos sitios, como la recuperación de sistemas, equipos y aplicaciones. Se cuenta con los siguientes documentos los cuales deben se acatados:

- **G-A-GTI-04** Borrado Seguro.
- Manual General de Operaciones de Infraestructura de TI - Confidencial
- **P-A-GTI-11** Gestión de la Operación de Servicios Tecnológicos.

- Los procedimientos operativos deben ser documentados y estar disponibles para los funcionarios, colaboradores y partes interesadas que los necesiten para la ejecución de sus funciones, teniendo en cuenta el nivel de clasificación (público, interno, confidencial y/o altamente confidencial.
- El acceso a las instalaciones de centro de cómputo y cableado debe ser restringido al personal no autorizado. Cualquier acceso debe realizarse en compañía del responsable de la infraestructura tecnológica, siendo identificado y controlado mediante un documento de soporte, así como con conocimiento y constancia del servicio de vigilancia.
- Las instalaciones de procesamiento de información ya sean internas o externas deben mantener las condiciones físicas y ambientales necesarias para garantizar la correcta ejecución de los servicios.
- Se deben establecer Acuerdos de Nivel de Servicio (ANS) tanto internos como con los proveedores de servicios en la nube, aplicables a los modelos de software como servicio (SaaS), infraestructura como servicio (IaaS) o plataforma como servicio (PaaS), para garantizar el adecuado funcionamiento de los servicios y la infraestructura tecnológica de la entidad.
- Los Acuerdos de Nivel de Servicio (ANS) establecidos deben ser monitoreados y revisados regularmente para asegurar su efectividad y cumplimiento.

- Se deben considerar y aplicar los Acuerdos Marco Vigentes de Colombia Compra Eficiente, para los modelos de Software como servicio (SaaS), Plataforma como servicio (PaaS) e Infraestructura como servicio (IaaS).
- Deben incluirse las instrucciones para el manejo de errores u otras condiciones excepcionales que puedan surgir durante la ejecución del trabajo, así como las restricciones sobre el uso de utilidades del sistema.
- Se deben seguir los lineamientos del proceso documentado para el cifrado de información de la Entidad, el cual se encuentra detallado en el siguiente documento: I-E-GET-06 Cifrado de archivos confidenciales de acceso restringido.

12.1.2 Gestión de cambios

Control: Se debe controlar los cambios en la Entidad, en los procesos de negocio, en las instalaciones y en los sistemas de procesamiento de información que afectan la seguridad de la información.

- La Entidad debe definir procesos documentados para la gestión de cambios en los procesos de negocio, instalaciones y los sistemas de procesamiento de información en los cuales se requiera realizar cambios, diligenciando el formato **F-A-GTI-01** Gestión de Cambio**.**
- El procedimiento de gestión de cambios debe contemplar entre otros los siguientes aspectos:
  - La identificación y registro de cambios significativos.
  - La planificación y puesta a prueba de los cambios.
  - La valoración de los impactos potenciales, incluidos los impactos de los cambios en relación con la seguridad de la información.
  - El procedimiento de aprobación formal de los cambios propuestos. La comunicación de todos los detalles del cambio a las personas pertinentes.
- Se deben realizar reuniones para informar y aprobar los cambios que se requieran realizar en la infraestructura tecnológica de la Entidad, en los cuales se pueda afectar la normal prestación de los servicios tecnológicos. En dichas reuniones deben participar como mínimo, los responsables de desarrollo, bases de datos, infraestructura seguridad de la información. Posteriormente se deberá informar al jefe de la OTIC, para su respectiva aprobación y ejecución.
- Se deben llevar a cabo y salvaguardar los registros soporte de la gestión de cambios realizada.

12.1.3 Gestión de capacidad

Control: Se debe hacer seguimiento al uso de recursos, hacer los ajustes, y hacer proyecciones de los requisitos de capacidad futura, para asegurar el desempeño requerido del sistema.

- La OTIC debe llevar a cabo actividades relacionadas con la gestión de la capacidad, que incluyan análisis y proyecciones para el procesamiento y almacenamiento de la información. Se debe tener en cuenta entre otros los siguientes aspectos: Nuevos requerimientos de Servicios tecnológicos.

- Cambios Tecnológicos.
- El crecimiento de los sistemas actuales de procesamiento de la información.
- Crecimiento o proyección institucional.
- Se deben aplicar controles de detección que identifiquen los problemas oportunamente.

- Se debe monitorear la capacidad de los sistemas y su infraestructura para garantizar la disponibilidad y proyectar nuevos requisitos del negocio.

12.1.4 Separación de los ambientes de desarrollo, pruebas y producción

Control: Se debe separar los ambientes de desarrollo, prueba y producción, para reducir los riesgos de acceso o cambios no autorizados al ambiente de producción.

- La OTIC debe separar los ambientes de desarrollo, pruebas y producción para reducir los riesgos de accesos o cambios no autorizados a los sistemas en producción, así como posibles inconvenientes en su operación.
- Los usuarios que por su rol tienen acceso a los ambientes de desarrollo, pruebas o producción deben aplicar los controles establecidos en la gestión de cambios, garantizando la continuidad de la operación sin comprometer la disponibilidad de los servicios tecnológicos asociados a dichos cambios.
- La OTIC debe asegurar que los ambientes de desarrollo, prueba y producción estén separados de manera lógica, estableciendo reglas claras de transferencia del software entre estos ambientes hasta su implementación en ambiente de producción.

.

12.2 Protección Contra Códigos Maliciosos

Objetivo: Asegurarse de que la información y las instalaciones de procesamiento de información estén protegidas contra códigos maliciosos.

12.2.1 Controles contra códigos maliciosos

Control: Se debe implementar controles de detección, de prevención y de recuperación, combinados con la toma de conciencia apropiada de los usuarios, para proteger contra códigos maliciosos.

- La OTIC debe proveer herramientas tales como antivirus, antimalware, antispam, antispyware, entre otras, para reducir el riesgo de infección por software malicioso y proteger la seguridad de la información contenida y administrada en la plataforma tecnológica de la Entidad y los servicios que se ejecutan en ella.
- La OTIC debe garantizar que el software de antivirus, antimalware, antispam y antispyware cuente con las licencias de uso requeridas, asegurando así su autenticidad y acceso a actualizaciones, para mitigar las vulnerabilidades de la plataforma tecnológica.

12.3 Copias de Respaldo

Objetivo: Proteger contra la pérdida de datos.

12.3.1 Respaldo de la información

Control: Se debe hacer copias de respaldo de la información, software e imágenes de los sistemas, y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo acordadas.

- La OTIC debe definir un procedimiento para las actividades de respaldo (Backups) de la Información de la Entidad, considerándola criticidad y las necesidades de disponibilidad de los datos. Este procedimiento debe estar debidamente documentado para su seguimiento y control.
- Los dueños de los activos del proceso son las personas autorizadas para solicitar o consultar copias de respaldo de los sistemas de información relacionados con sus procesos.
- Es responsabilidad de los administradores de cada sistema de información solicitar la copia a los administradores de Backup, validar y asegurarse que su sistema de información esté incluido en el cronograma de copias de seguridad, y realizar seguimientos regulares a la ejecución de esta actividad.
- Se deben seguir los lineamientos definidos en los siguientes documentos: **I-A-GTI-02** Instructivo para la Generación de Copias de Respaldo BACK-UP y **G-A-GTI-08** Guía de Apoyo en el Servicio de Backup para Usuarios.

12.4 Registro (Logging) y Seguimiento

Objetivo: Registrar eventos y generar evidencia.

12.4.1 Registro de eventos

Control: Se debe elaborar, conservar y revisar regularmente los registros acerca de actividades del usuario, excepciones, fallas y eventos de seguridad de la información.

- La Entidad debe disponer de registros (logs de eventos), que permitan llevar un control y seguimiento de las actividades realizadas en los sistemas de información, que garanticen la trazabilidad y detección oportuna de incidentes o irregularidades.
- Se deben generar, mantener y revisar regularmente (2 veces al año) los registros de auditoría de las actividades de los usuarios, excepciones y eventos de seguridad de la información. Estos registros deben respaldar futuras investigaciones y revisiones regulares del control de acceso, registros de actividad en el directorio activo, red, antivirus y seguridad perimetral.

- La Entidad debe contar con procedimientos de operación establecidos para la gestión de capacidad, respaldos (Backups), administración de casos de soporte, entre otros, que aseguren la continuidad y eficiencia de los servicios.
- Los registros de eventos deben generarse de manera que no afecten el desempeño ni la disponibilidad de los servicios tecnológicos, tanto en la nube como en instalaciones locales (on-premise), teniendo en cuenta las capacidades institucionales. Estos registros deben considerar los siguientes aspectos:

    - Identificación de usuarios;
    - Actividades del sistema;
    - Fechas, horas y detalles de los eventos clave, como entradas y salidas;
    - Identidad del dispositivo o ubicación, e identificador del sistema cuando sea posible;
    - Registros de intentos de acceso al sistema exitosos y rechazados;
    - Registros de acceso a datos exitosos y rechazados, así como otros intentos de acceso a recursos;
    - Cambios a la configuración del sistema;
    - Uso de privilegios;
    - Uso de utilidades y aplicaciones del sistema;
    - Archivos a los que se accedió y el tipo de acceso;
    - Direcciones y protocolos de red utilizados;
    - Alarmas activadas por el sistema de control de acceso;
    - Activación y desactivación de sistemas de protección, como antivirus y sistemas de detección de intrusiones.
    - Registros de las transacciones ejecutadas por los usuarios en las aplicaciones.

12.4.2 Protección de la información de registro.

Control: Los sistemas de gestión de registros y la información de registro se debe proteger contra alteración y acceso no autorizado.

- Deben tenerse en cuenta los lineamientos definidos en el procedimiento **P-A-GTI-11** Gestión de la Operación de Servicios Tecnológicos.
- Limitar los privilegios de administrador y aplicar el principio de privilegio mínimo para evitar que usuarios no autorizados realicen cambios en los sistemas de registro.

12.4.3 Registros (Logs) del administrador y del operador

Control: Las actividades del administrador y del operador del sistema se debe registrar (Logged), y los registros (Logs) se debe proteger y revisar con regularidad.

- Todas las evidencias que se recolecten como resultado de las auditorías practicadas deben reposar en un lugar para el almacenamiento de los registros y monitoreo de los eventos de seguridad.
- Deben tenerse en cuenta los lineamientos definidos en el procedimiento **P-A-GTI-11** Gestión de la Operación de Servicios Tecnológicos

12.4.4 Sincronización de relojes

Control: Los relojes de todos los sistemas de procesamiento de información pertinentes dentro de una Entidad o ámbito de seguridad se debe sincronizar con una única fuente de referencia de tiempo.

- La Entidad debe contar con un mecanismo de sincronización de relojes para todos los equipos de cómputo, servidores, dispositivos de red, sistemas operativos, bases de datos, sistemas de información y demás elementos de infraestructura utilizados. Este mecanismo debe utilizar como referencia la hora oficial de Colombia (Instituto Nacional de Metrología) a través de horalegal.inm.gov.co, que garantice la adecuada correlación de eventos y facilite la investigación efectiva de incidentes.
- Se debe utilizar como referencia la hora legal colombiana, y no está permitida la desactivación del sistema de sincronización o la manipulación manual de la hora. Los relojes de todos los servicios tecnológicos on-premise de la Entidad deben estar sincronizados con la fuente oficial.
- La Entidad cuenta con los siguientes documentos cuyos lineamientos deben ser observados:

12.5 Control de Software Operacional

Objetivo: Asegurar la integridad de los sistemas operativos.

12.5.1 Instalación de software en sistemas operativos.

Control: Se debe implementar procedimientos para controlar la instalación de software en sistemas operativos.

Se deben establecer los siguientes controles:

- Deben ser implementadas políticas GPO desde el directorio activo para restringir la instalación y desinstalación de software no autorizado.
- Implementar actualizaciones automáticas para los sistemas operativos, garantizando que los equipos mantengan las versiones y parches de seguridad más recientes.
- Realización de Backups antes de realizar cualquier cambio de versión.

12.6 Gestión de la Vulnerabilidad Técnica

Objetivo: Prevenir el aprovechamiento de las vulnerabilidades técnicas

12.6.1 Gestión de las vulnerabilidades técnicas

Control: Se debe obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se usen; evaluar la exposición de la Entidad a estas vulnerabilidades y tomar las medidas apropiadas para tratar el riesgo asociado.

- Se deben tener como marco de referencia los siguientes documentos relacionados a la gestión y remediación de vulnerabilidades: **P-A-GTI-11** Gestión de la Operación de Servicios Tecnológicos y **F-A-GTI-11** Registro de Pruebas y Remediación de Vulnerabilidades Técnicas.
- La Entidad debe realizar análisis periódicos de vulnerabilidades a sus activos de información. Actualmente se cuenta con la herramienta Tenable IO para la ejecución de estos análisis. El análisis de vulnerabilidades tiene como fin identificar las brechas de seguridad en los sistemas de información y en la infraestructura tecnológica. Por lo tanto, dicha actividad implica:
  - Contar con personal debidamente capacitado para la administración de esta herramienta.
  - Documentar los resultados, priorizar las vulnerabilidades, elaborar un plan de remediación para corregir o mitigar, según sea el caso, las brechas identificadas y comunicar los resultados de las pruebas a cada uno de los responsables de los sistemas de información e infraestructura tecnológica, quienes serán los responsables de definir y aplicar dicho plan.
- La OTIC debe revisar periódicamente la aparición de nuevas vulnerabilidades técnicas y reportarlas a los administradores de la plataforma tecnológica con el fin de prevenir la exposición a riesgos.
- La OTIC a través de sus servidores públicos, contratistas, proveedores y partes interesadas, debe generar, ejecutar y hacer seguimiento a los planes de acción para mitigar las vulnerabilidades técnicas detectadas en la plataforma tecnológica.

12.6.2 Restricciones sobre la instalación de software

Control: Se debe establecer e implementar las reglas para la instalación de software por parte de los usuarios.

- La OTIC debe implementar los controles necesarios para prevenir la instalación de software no autorizado por parte de servidores públicos, contratistas, proveedores y partes interesadas, con el fin de mitigar posibles las vulnerabilidades técnicas que puedan derivarse de dichas instalaciones.

- La Entidad debe contar con políticas de grupo (GPO) configuradas y gestionadas a través del directorio activo, que fortalezcan la seguridad y el control de los sistemas, al facilitar la implementación centralizada de restricciones y configuraciones.

12.7 Consideraciones Sobre Auditorías de Sistemas de Información

Objetivo: Minimizar el impacto de las actividades de auditoría sobre los sistemas operativos.

12.7.1 Controles sobre auditorías de sistemas de información

Control: Los requisitos y actividades de auditoría que involucran la verificación de los sistemas operativos se debe planificar y acordar cuidadosamente para minimizar las interrupciones en los procesos del negocio.

- Las auditorías que involucren acceso a los sistemas de información deben ser planificadas y acordadas para minimizar las interrupciones en los procesos de la entidad.

Durante el desarrollo de las auditorias, se debe tener en cuenta los siguientes aspectos:

- Los requisitos de auditoría para acceso a sistemas y datos deben ser acordados con el área auditada.
- La entidad debe contar con configuraciones de auditoria en los sistemas de información y dispositivos (appliance) que faciliten el registro y monitoreo de las actividades realizadas, contribuyendo así al cumplimiento de dicha tarea.

13 SEGURIDAD EN LAS TELECOMUNICACIONES

13.1 Gestión de la Seguridad de las Redes

Objetivo: Asegurar la protección de la información en las redes, y sus instalaciones de procesamiento de información de soporte.

13.1.1 Controles de redes

Control: Las redes se debe gestionar y controlar para proteger la información en sistemas y aplicaciones.

La OTIC debe establecer y documentar los lineamientos para:

- Se deben implementar controles de acceso a la red para restringir el acceso de personas no autorizadas, incluyendo el uso de mecanismos de autenticación.
- Se deben implementar controles de seguridad específicos para los dispositivos de red, como routers, switches, firewalls y demás dispositivos con los que cuente la Entidad, incluyendo configuraciones adecuadas de estos dispositivos, la actualización de firmware, la protección de accesos no autorizados y la segmentación de la red.
- Se deben implementar controles de seguridad para las comunicaciones de red como el uso de protocolos seguros (HTTPS, SSL/TLS, entre otros) para garantizar que los datos trasmitidos a través de la red estén cifrados y protegidos contra interceptaciones o ataques.
- Se deben implementar controles de seguridad para los servicios de red, como los servicios de correo electrónico, los servicios web y los servicios de almacenamiento en la nube, entre otros.
- Se deben implementar controles de supervisión y control de la red para monitorear el tráfico de red y detectar amenazas.

  Lo anterior se encuentra contenido en el Manual General de Operaciones de Infraestructura (Anexo 1 Documento confidencial).

- El acceso a los sistemas de la red se debe hacer a través de usuarios autorizados, de acuerdo con los roles definidos en el manual del sistema de gestión de seguridad de la información y aplicar los privilegios de manera puntual para cada servicio tecnológico según las condiciones definidas por el dueño del proceso y la OTIC.

13.1.2 Seguridad de los servicios de red

Control: Se debe identificar los mecanismos de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de red, e incluirlos en los acuerdos de servicios de red, ya sea que los servicios se presten internamente o se contraten externamente.

- La Oficina TIC debe disponer de mecanismos robustos de monitoreo del canal de internet, que permitan detectar y mitigar de manera oportuna cualquier incidente o ataque que se presente mediante este medio. Manual General de Operaciones de Infraestructura (Anexo 1, Documento confidencial).
- La OTIC, como responsable de las redes de datos y de los recursos de red de la Entidad (internos y externos), debe propender porque dichas redes estén debidamente protegidas contra accesos no autorizados, mediante la implementación de controles de acceso lógico, tales como sistemas de autenticación, firewalls, entre otros.
- En los acuerdos establecidos con proveedores, se debe identificar e incluir acuerdos de niveles de Servicio (ANS) como mecanismos de seguridad, además, debe garantizarse el derecho a realizar y auditorias regulares a los proveedores.

- La OTIC debe identificar los mecanismos de seguridad, los niveles de servicio (ANS) y los requisitos de gestión de todos los servicios de red, estableciendo los siguientes controles:
    - Se debe identificar y documentar los servicios de red que son necesarios para el funcionamiento de la organización, así como los requisitos de seguridad asociados a cada uno de ellos. Manual General de Operaciones de Infraestructura (Anexo 1, Documento confidencial).
    - Se debe implementar y mantener una política de seguridad de red que defina las reglas y responsabilidades para el uso, acceso, configuración, monitoreo y protección de los servicios de red, esta política debe ser comunicada y aplicada a todos los niveles de la entidad, Manual General de Operaciones de Infraestructura (Anexo 1, Documento confidencial).
    - Todos los servicios de red deben contar con mecanismos de autenticación, autorización, cifrado y no repudio, según el nivel de confidencialidad, disponibilidad e integridad de la información que transmiten o procesen.
    - Se debe controlar y registrar el acceso a los servicios de red por parte de los usuarios y dispositivos autorizados, el acceso debe ser restringido o bloqueado en caso de detectar alguna actividad sospechosa o no autorizada.
    - Se debe supervisar y auditar el funcionamiento y el rendimiento de los servicios de red de manera continua, a través de sistemas de monitoreo que permitan la detección temprana de cualquier incidente o anomalía que puedan comprometer la seguridad de la red, cualquier incidente debe ser reportado de inmediato y gestionado según lo establecido en el procedimiento **P-A-GTI-11** Gestión de la Operación de Servicios Tecnológicos.

13.1.3 Separación en las redes

Control: Los grupos de servicios de información, usuarios y sistemas de información se debe separar en las redes.

- La OTIC, debe implementar mecanismos de control de acceso a través de la segmentación de las redes, de acuerdo con los grupos de servicios, usuarios, sistemas de información y físicas, esto garantizará una protección más efectiva de los activos críticos.
- La OTIC debe proveer los mecanismos, controles y recursos necesarios para establecer niveles adecuados de separación física y lógica, con el fin de reducir el acceso no autorizado y prevenir el uso o cambios inadecuados en los servicios de T.I. (servicios de red, acceso a sistemas de información, servicios de internet).
- Se debe segmentar las conexiones de los elementos de red físicos, tanto físicos como lógicos, así como de los usuarios, diferenciándolas de las de terceros y de los servicios de internet. Esto se hace por medio de una infraestructura de seguridad perimetral robusta.

- La OTIC debe diseñar una arquitectura de red que separe los segmentos de acuerdo con el nivel de seguridad requerido. Esto implica el uso de dispositivos de red, como routers, firewalls, switches o VLANs, que faciliten dicha separación.
- La OTIC debe Implementar mecanismos de control de acceso que impidan el tráfico no autorizado entre los segmentos. A través de las listas de control de acceso, reglas de firewall y mecanismos de autenticación.
- La OTIC debe establecer y documentar los lineamientos para la gestión de la red, incluyendo la asignación de roles y responsabilidades, la monitorización del tráfico, la detección y respuesta a incidentes, así como la revisión periódica de la configuración y el cumplimiento de las políticas de seguridad.
- La OTIC debe documentar y mantener actualizada la información relacionada con la estructura y funcionamiento de la red. Esto incluye diagramas, inventarios, especificaciones técnicas y registros de actividad, asegurando una referencia clara para la gestión y mantenimiento de la infraestructura.

13.2 Transferencia de Información

Objetivo: Mantener la seguridad de la información transferida dentro de la Entidad y con cualquier Entidad externa.

13.2.1 Políticas y procedimientos de transferencia de información

Control: Se debe contar con políticas, procedimientos y controles de transferencia formales para proteger la transferencia de información mediante el uso de todo tipo de instalaciones de comunicación.

- La Entidad debe contar con la identificación y clasificación de la información que se va a transferir, esta clasificación debe estar alineada con las políticas de seguridad de la información y establecer los niveles de confidencialidad, integridad y disponibilidad que aplican a cada tipo de información, incluyendo los datos sensibles o críticos. Asimismo, se debe identificar claramente a los destinatarios autorizados y los medios de transferencia que se utilizarán, asegurando que estos últimos sean apropiados y seguros.
- La OTIC debe establecer los requisitos específicos de seguridad para la transferencia de información. Estos incluyen, el uso de mecanismos de protección como el cifrado para garantizar la confidencialidad, la firma digital, el control de acceso, el registro y la verificación.
- La Entidad debe definir las responsabilidades y autorizaciones asociadas con la transferencia de información, así como de los procesos de aprobación, notificación y seguimiento.
- La Entidad debe definir las medidas de protección física y lógica para los medios de transferencia, esto incluye el uso de sobres o contenedores sellados, el borrado o la

destrucción seguros de medios físicos (discos duros, USB, medios ópticos, entre otros) de los medios después del uso, Además, se debe garantizar la integridad de la información durante el transporte y prevenir accesos no autorizados o modificaciones.

- Los usuarios deben hacer uso únicamente de los canales de comunicación establecidos por la entidad para la transferencia de información aprobados y controlados por la entidad. Cualquier otro canal de transferencia no especificado se considerará como no autorizado.

13.2.2 Acuerdos sobre transferencia de información

Control: Los acuerdos debe tratar la transferencia segura de información del negocio entre la Entidad y las partes externas.

- Cuando se trate de intercambios periódicos de información, se debe priorizar la transmisión de datos a través de vías seguras, con los cuales se establecen convenios o acuerdos formales, garantizando que las partes involucradas cumplan con los requisitos de seguridad y confidencialidad.
- La Entidad debe identificar los requisitos legales, reglamentarios y contractuales que apliquen a la transferencia de información, así como las responsabilidades de las partes interesadas involucradas en el proceso, para asegurar su cumplimiento.
- La Entidad debe definir los métodos y formatos adecuados para la transferencia de información, teniendo en cuenta los niveles de confidencialidad, integridad y disponibilidad requeridos, además se deben considerar los riesgos asociados a la pérdida, alteración o divulgación no autorizada de la información.
- La OTIC debe establecer los mecanismos de protección de la información durante su trasmisión y recepción, tales como el cifrado, autenticación, firma digital y otros controles que sean necesarios para proteger la información y la integridad de los datos transferidos.

13.2.3 Mensajería electrónica

Control: Se debe proteger adecuadamente la información incluida en la mensajería electrónica.

- La Entidad debe contar con un sistema de correo electrónico y suite ofimática en la nube, accesible mediante autenticación "single sign-on" (SSO) para garantizar un acceso seguro y controlado, de acuerdo al I-A-GTI-09 Instructivo de Integración de Sistemas de Información al Single Sign On
- Todos los mensajes enviados desde la cuenta institucional de la Entidad deben cumplir con los estándares de formato e imagen corporativa de la Entidad.
- La OTIC debe definir las condiciones sobre el uso aceptables de la mensajería electrónica, incluyendo los tipos de información que se pueden ser trasmitidos, las restricciones de acceso, el uso de cifrado, la firma digital y el etiquetado de la información confidencial.
- Se deben establecer e implementar mecanismos de autenticación, autorización y registro para los usuarios y dispositivos que acceden al servicio de mensajería electrónica.

- Se deben implementar medidas de seguridad para prevenir, detectar y responder a incidentes relacionados con la mensajería electrónica, tales como el malware, el phishing, el spam, la suplantación de identidad y la fuga de información.
- La OTIC debe realizar copias de seguridad periódicas de los mensajes y archivos adjuntos almacenados en los servidores, y garantizar su recuperación en caso de pérdida, daño o incidente de seguridad.
- La OTIC debe sensibilizar y concienciar a los usuarios sobre los riesgos asociados al uso de la mensajería electrónica y promover las mejores prácticas de seguridad en el uso de la mensajería electrónica.
- El uso indebido del correo electrónico, como el envío de cadenas de mensajes o correos masivos que no estén relacionados con la misión de la Entidad, afecta negativamente el rendimiento del servicio de correo y consume recursos tecnológicos. Se debe evitar la distribución de correos masivos o reenviarlos sin un propósito justificado y relevante.

13.2.4 Acuerdos de confidencialidad o de no divulgación

Control: Se debe identificar, revisar regularmente y documentar los requisitos para los acuerdos de confidencialidad o no divulgación que reflejen las necesidades de la Entidad para la protección de la información.

- Se debe informar a todos los servidores públicos, contratistas, proveedores y partes interesadas o quien por su rol estén vinculados con la Entidad, sobre el compromiso frente a la no divulgación de la información relacionada con las funciones y/o obligaciones contractuales que desempeñen, Este compromiso abarca tanto al personal interno como externo que tenga acceso a dicha información.
- Todos los servidores públicos, contratistas, proveedores y partes interesadas o quien por su rol estén vinculados con la Entidad, deben firmar la cláusula y/o acuerdos de confidencialidad definidos, estos acuerdos deben ser parte integral de los expedientes laborales o de los contratos celebrados. Este requerimiento también se aplicará para los casos de contratación de personal temporal o aquellos casos cuando se permita el acceso a la información y/o a los recursos de la Entidad a personas o entidades externas.
- Todos los servidores públicos, contratistas, proveedores y partes interesadas de la Entidad, deben guardar absoluta reserva sobre cualquier información a la que tenga acceso con ocasión de la ejecución de las funciones y/o obligaciones, Este deber de reserva se mantendrá incluso después de la finalización de sus actividades o relación contractual, durante el tiempo que establezca la legislación vigente y aplicable en cada caso.

14 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS

14.1 Requisitos de Seguridad de 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 sobre redes públicas.

14.1.1 Análisis y especificación de requisitos de seguridad de la información

Control: Los requisitos relacionados con seguridad de la información se debe incluir en los requisitos para nuevos sistemas de información o para mejoras a los sistemas de información existentes.

- En todos los proyectos de desarrollo y adquisición de sistemas de información, ya sean propios o de terceros, se deben incluir requisitos de seguridad de la información desde la fase de diseño aplicables a todo el ciclo de vida del sistema. Esto asegura que la seguridad esté integrada en cada fase, desde la planificación hasta la operación y el mantenimiento.
- La OTIC debe definir los requisitos de seguridad de la información para los nuevos sistemas de información, así como para las mejoras de los sistemas existentes, ya sea que se contraten externamente o se desarrollen internamente. Los propietarios de los activos de información deben autorizar los accesos a sus sistemas de información o aplicativos, de acuerdo con los perfiles establecidos, las necesidades de uso y la clasificación de la información definida por la Entidad.
- Las dependencias o procesos que contraten el desarrollo de software o adquieran software de terceros, deben apoyarse en la OTIC para definir los requisitos necesarios de seguridad de la información.
- En cuanto a los requisitos de los sistemas de información, se debe definir lo siguiente:
    - El nivel de confianza requerido con relación a la identificación declarada de los usuarios, para obtener los requisitos de autenticación de usuario
    - Los procesos de suministro de acceso y de autorización para usuarios, al igual que para usuarios privilegiados o técnicos
    - Las necesidades de protección de activos de información involucrados, en términos de disponibilidad, confidencialidad e integridad.
    - Los requisitos derivados de los procesos del negocio, tales como ingreso, seguimiento, no repudio, autenticación de formularios mediante HTTPS, cifrado de contraseñas almacenadas y uso de firmas digitales. Los requisitos de trazabilidad (registro de eventos) de las actividades de los usuarios.
    - La necesidad de implementar metodologías de desarrollo seguro.

14.1.2 Seguridad de servicios de las aplicaciones en redes públicas

Control: La información involucrada en los servicios de aplicaciones que pasan sobre redes públicas se debe proteger de actividades fraudulentas, disputas contractuales y divulgación y modificación no autorizadas.

- Se debe evitar, en la medida de lo posible, el uso de redes públicas (como las de aeropuertos, hoteles, centros comerciales, cafés internet, entre otros) para acceder a los servicios y/o sistemas de información de la Entidad. Estas redes son inherentemente menos seguras y más propensas a ataques. Para las redes domésticas que pueden ser accedidas, se debe aplicar entre otras las siguientes recomendaciones:
    - Cambiar la contraseña periódicamente y asegurarse de utilizar contraseñas seguras, como mínimo con 12 caracteres de longitud.
    - El nombre de la red no debe incluir información que permitan identificar al propietario de la red o la contraseña.
    - Utilizar el método de seguridad más avanzado que su dispositivo permita.
- Las aplicaciones que se conectan a redes públicas deben contar con mecanismos de protección de la información sensible.
- Se deben definir e implementar mecanismos técnicos que mitiguen las amenazas de fraude y manipulación de la información publicada en las redes.

14.1.3 Protección de transacciones de los servicios de las aplicaciones

Control: La información involucrada en las transacciones de los servicios de las aplicaciones se debe proteger para evitar la transmisión incompleta, el enrutamiento errado, la alteración no autorizada de mensajes, la divulgación no autorizada, y la duplicación o reproducción de mensajes no autorizada.

- Quienes ejecuten el rol de Administrador del control de acceso lógico, deben asegurar de que los usuarios utilicen diferentes perfiles diferenciados para los ambientes de desarrollo, pruebas y producción.
- Los administradores de control de acceso lógico deben garantizar que los desarrolladores, tanto internos como externos, que tengan acceso limitado y estrictamente controlado a los datos y archivos en los entornos de producción, minimizando los riesgos de alteración o fuga de información crítica. Se debe implementar autenticación secreta de usuario en todos los servicios de transacciones con los bancos.
- Se deben cumplir los lineamientos establecidos para la seguridad lógica, seguridad física, seguridad de red, seguimiento y control en las terminales de áreas financieras de las entidades públicas de acuerdo con el documento **"**Guía 18 Lineamientos: Terminales de áreas financieras Entidades públicas "del MSPI.

14.2 Seguridad en los Procesos de Desarrollo y de Soporte

Objetivo: Asegurar que la seguridad de la información esté diseñada e implementada dentro del ciclo de vida de desarrollo de los sistemas de información.

14.2.1 Política de desarrollo seguro

Control: Se debe establecer y aplicar reglas para el desarrollo de software y de sistemas, a los desarrollos dentro de la Entidad.

- La Entidad velará por que el desarrollo, ya sea interno o externo de aplicaciones y sistemas de información cumpla con los requisitos de seguridad establecidos, con las mejores prácticas de desarrollo seguro, así como la metodología para la realización de pruebas de aceptación y seguridad del software desarrollado.
- Se debe verificar que los desarrollos estén debidamente documentados, incluyendo las especificaciones técnicas, cambios realizados y versiones del software. Además, todas las versiones del desarrollo deben ser almacenadas en varios medios, y se debe mantener una copia de respaldo en un sitio externo para asegurar la recuperación en caso de incidentes.
- Para el desarrollo de software y de sistemas que se implementen en la infraestructura tecnológica de la Entidad o que consuman sus servicios, se debe tener en cuenta la integración con el único punto de autenticación por medio de Keycloak. Las aplicaciones deben ser capaces de integrarse con Keycloak para la debida autenticación y la autorización.
- Los propietarios de los sistemas de información son responsables de realizar las pruebas para asegurar que cumplen con los requerimientos de seguridad establecidos antes del paso a producción de los sistemas, utilizando metodologías establecidas para este fin, documentado las pruebas realizadas y aprobando los pasos a producción. Estas pruebas deben realizarse por entrega de funcionalidades nuevas, por ajustes de funcionalidad o por cambios sobre la plataforma tecnológica en la cual funcionan los aplicativos.

14.2.2 Procedimientos de control de cambios en sistemas

Control: Los cambios a los sistemas dentro del ciclo de vida de desarrollo se debe controlar mediante el uso de procedimientos formales de control de cambios.

- La OTIC, es la responsable de planificar, desarrollar y llevar a cabo las actividades relacionadas con los desarrollos, actualizaciones e instalaciones de software. Asimismo, debe coordinar y ejecutar pruebas funcionales y de seguridad de los sistemas nuevos o modificados, asegurándose de que se realicen antes de su implementación en los servidores de producción.
- El control de cambios debe llevarse a cabo conforme a los lineamientos y requerimientos de seguridad establecidos, asegurando que todas las modificaciones sean previamente aprobadas por las partes interesadas.

14.2.3 Revisión técnica de las aplicaciones después de cambios en la plataforma de operación

Control: Cuando se cambian las plataformas de operación, se debe revisar las aplicaciones críticas del negocio, y someter a prueba para asegurar que no haya impacto adverso en las operaciones o seguridad de la Entidad.

- Se debe realizar una verificación de los cambios en las plataformas de operación y en las aplicaciones, para identificar cualquier posible impacto en el funcionamiento del sistema y asegurar que se cumplan los lineamientos de seguridad de la información de la Entidad.

Los cambios en los sistemas operativos y aplicaciones deben ser probados en un entorno de pruebas antes de su implementación en los ambientes de producción. Esto asegura que se detecten y solucionen posibles problemas o vulnerabilidades sin comprometer los sistemas críticos.

14.2.4 Restricciones en los cambios a los paquetes de software

Control: Se debe desalentar las modificaciones a los paquetes de software, los cuales se debe limitar a los cambios necesarios, y todos los cambios se debe controlar estrictamente.

- Solo se deben utilizar paquetes de software con licencias válidas, adquiridos a través de proveedores autorizados. Esto incluye la instalación de actualizaciones y parches necesarios para mantener la seguridad y estabilidad de las aplicaciones. Se debe definir y documentar las reglas para la transferencia de software desde el ambiente de pruebas al ambiente de producción. Estas reglas deben garantizar que los cambios sean controlados y aprobados adecuadamente antes de ser implementados.
- Cualquier tipo de modificación que se realice, debe ser puesta a prueba y ser validada antes de su implementación.

14.2.5 Principios de construcción de sistemas seguros

Control: Se debe establecer, documentar y mantener principios para la construcción de sistemas seguros, y aplicarlos a cualquier actividad de implementación de sistemas de información.

- La Entidad debe documentar y exigir el cumplimiento de una arquitectura de diseño seguro en la construcción de sistemas de información, que abarque capas de negocio, datos, aplicaciones y tecnología, y que se actualice regularmente para hacer frente a nuevas amenazas potenciales. La OTIC debe incluir requisitos de seguridad en la definición de requerimientos y garantizar que estos se verifiquen plenamente durante las pruebas de los desarrollos del software.
- En los nuevos desarrollos, deben realizarse un análisis de gestión de riesgos de seguridad, y revisar en función de patrones de ataque conocidos.

14.2.6 Ambiente de desarrollo seguro

Control: Las organizaciones deben establecer y proteger adecuadamente los ambientes de desarrollo seguros para las actividades de desarrollo e integración de sistemas que comprendan todo el ciclo de vida de desarrollo de sistemas.

- Los usuarios deben utilizar perfiles diferenciados para los ambientes de producción y s de pruebas, y los menús debe mostrar mensajes de identificación apropiados para reducir el riesgo de errores.

14.2.7 Desarrollo contratado externamente

Control: La Entidad debe supervisar y hacer seguimiento de la actividad de desarrollo de sistemas contratados externamente.

- La Entidad cuenta con el documento: M-E-GET-04 Manual de Políticas Específicas de Seguridad y Privacidad de la Información.
- La OTIC verificará el cumplimiento con los requerimientos del sistema, incluyendo los de seguridad, asegurando su implementación en todas las etapas del ciclo de vida del sistema.
- El software que adquirido a través de los proyectos o programas debe registrarse a nombre del Ministerio de Ambiente y Desarrollo Sostenible.

14.2.8 Pruebas de seguridad de sistemas

Control: Durante el desarrollo se debe llevar a cabo pruebas de funcionalidad de la seguridad.

- La OTIC debe llevar a cabo pruebas de seguridad exhaustivas en los sistemas de información para validar su resistencia a vulnerabilidades y amenazas potenciales. Las pruebas no se deben llevar a cabo en el ambiente de producción.

14.2.9 Prueba de aceptación de sistemas

Control: Para los sistemas de información nuevos, actualizaciones y nuevas versiones, se debe establecer programas de prueba para aceptación y criterios de aceptación relacionados.

- Se adquirió una herramienta para realizar análisis de vulnerabilidades, permitiendo la identificación y gestión de riesgos de seguridad de manera efectiva, se debe contar con recurso humano para llevar a cabo la administración de dicha herramienta.
- Se debe establecer un procedimiento, para llevar a cabo la gestión de vulnerabilidades.
- La OTIC debe aplicar los documentos relacionas con el Ciclo de vida de Desarrollo, definidos en el Numeral: 14.2.5 de esta Política. Estos documentos deben incluir directrices sobre la

incorporación de pruebas de seguridad y controles de calidad en cada etapa del ciclo de vida del desarrollo, desde la planificación y diseño hasta la implementación y mantenimiento.

14.3 Datos de Prueba

Objetivo: Asegurar la protección de los datos usados para pruebas.

14.3.1 Protección de datos de prueba

Control: Los datos de prueba se debe seleccionar, proteger y controlar cuidadosamente.

- Los datos de carácter clasificados y/o reservados no deben copiarse en el ambiente de pruebas, a menos que se implementen controles equivalentes a los del ambiente de producción.
- La OTIC debe establecer un proceso para la selección y anonimización de datos de prueba, asegurando que la información sensible sea reemplazada o enmascarada para prevenir la exposición de datos reales en entornos no seguros.

15 RELACIONES CON LOS PROVEEDORES

15.1 Seguridad de la Información en las Relaciones con los Proveedores

Objetivo: Asegurar la protección de los activos de la Entidad que sean accesibles a los proveedores.

15.1.1 Política de seguridad de la información para las relaciones con proveedores

Control: Los requisitos de seguridad de la información para mitigar los riesgos asociados con el acceso de proveedores a los activos de la Entidad se debe acordar con estos y se debe documentar.

- Durante la fase precontractual, y desde la construcción de los estudios previos, el área solicitante de la contratación, con el apoyo de la OTIC, debe identificar y evaluar los riesgos de seguridad de la información. los cuales debe ser parte de la estimación y cobertura de los riesgos dentro del proceso de contratación.
  De acuerdo con lo anterior, el análisis de riesgos de seguridad de la información debe incluir la identificación de estos en la respectiva contratación, su clasificación, probabilidad de ocurrencia estimada, su impacto, la determinación de la parte que debe asumirlos, el

tratamiento que se les debe dar para eliminarlos o mitigarlos y las características del monitoreo más adecuado para administrarlos.

- En la etapa contractual, deben incluirse cláusulas, se seguridad de la información especificas asignando responsables y tratamiento: de confidencialidad, de protección de datos, derechos de autor, las políticas de seguridad y privacidad de la información definida por la Entidad, estos aspectos deben ser claros y obligatorios para los proveedores.
- Los documentos relacionados con la seguridad y privacidad de la información definidos por la Entidad deben ser conocidos y aceptados por los proveedores, antes de la firma del contrato, asegurando así el cumplimiento de los lineamientos de seguridad para el perfeccionamiento del contrato.
- Se deben suscribir los acuerdos (ANS) formales donde se establecen y acuerdan los requisitos de seguridad de la información, y el compromiso de cumplimiento por parte de los proveedores.

15.1.2 Tratamiento de la seguridad dentro de los acuerdos con proveedores

Control: Se debe establecer y acordar todos los requisitos de seguridad de la información pertinentes con cada proveedor que pueda tener acceso, procesar, almacenar, comunicar o suministrar componentes de infraestructura de TI para la información de la Entidad.

- En cada contrato se debe especificar el tipo de información al que tendrá acceso el proveedor según el objeto del contrato. Además, el supervisor del contrato será responsable de verificar el cumplimiento de las obligaciones relacionadas con la seguridad y privacidad de la información.
- La obligación de los proveedores de entregar periódicamente un informe independiente sobre la eficacia de los controles y un acuerdo sobre la corrección oportuna de los asuntos pertinentes presentados en el informe.
- Las obligaciones de los proveedores relativas al cumplimiento de los requisitos de seguridad de la organización.

15.1.3 Cadena de suministro de tecnología de información y comunicación.

Control: Los acuerdos con proveedores debe incluir requisitos para tratar los riesgos de seguridad de la información asociados con la cadena de suministro de productos y servicios de tecnología de información y comunicación.

- Para los servicios contratados externamente, se debe exigir que los proveedores conozcan, adopten y comuniquen los requisitos y prácticas de seguridad y privacidad de la información de la Entidad a lo largo de la cadena de suministros.
- Para la contratación de servicios o componentes de la Infraestructura de TI y/o Áreas Seguras, se debe exigir a los proveedores la presentación de los planes de contingencia que aseguren la disponibilidad de la Información, suministrada y procesada entre las partes.

- Se debe definir acuerdos de niveles de servicios con todos los proveedores que tengan acceso o no a información confidencial o altamente confidencial, estos acuerdos deben estar monitoreados permanentemente por el supervisor del contrato.

15.2 Gestión de la Prestación 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.

15.2.1 Seguimiento y revisión de los servicios de los proveedores

Control: Las organizaciones debe hacer seguimiento, revisar y auditar con regularidad la prestación de servicios de los proveedores.

- Se debe asegurar que el proveedor mantenga la capacidad de servicio suficiente para mantener los niveles de continuidad del servicio acordados, después de fallas considerables en el servicio, o después de un desastre.
- Se deben definir acuerdos de niveles de servicios con todos los proveedores que tengan acceso o no a información confidencial o altamente confidencial, estos acuerdos deben estar monitoreados permanentemente por el supervisor del contrato.
- La OTIC debe monitorear la asignación de permisos de acceso de los proveedores a los sistemas de información de la entidad, lo anterior, teniendo en cuenta las condiciones que éstos deben cumplir en cuanto a la gestión de usuarios y contraseñas definidos en este manual.
- Se debe hacer un seguimiento al servicio y desempeño de los proveedores con base en los acuerdos de nivel de servicios establecido para validar los niveles de seguridad de la información acordados.

15.2.2 Gestión de cambios en los servicios de los proveedores

Control: Se debe gestionar los cambios en el suministro de servicios por parte de los proveedores, incluido el mantenimiento y la mejora de las políticas, procedimientos y controles de seguridad de la información existentes, teniendo en cuenta la criticidad de la información, sistemas y procesos del negocio involucrados, y la revaloración de los riesgos.

- En los servicios establecidos con los proveedores se debe gestionar todos los cambios siguiendo el procedimiento definido por La Entidad teniendo en cuenta los cambios en los acuerdos con el proveedor, los cambios requeridos por la Entidad y los cambios en los servicios del proveedor a implementar.
- Toda gestión del proveedor que represente una modificación, mantenimiento, revisión al Servicio de Tecnología de la Información, Comunicaciones o Equipos de Suministros, debe

cumplir con los lineamientos de gestión de cambios definidos por la entidad, donde se contemplen entre otros: cambios en los acuerdos con los proveedores, cambios hechos por la Entidad para implementar las mejoras a los servicios ofrecidos en la actualidad, desarrollo de nuevas aplicaciones y sistemas, modificaciones o actualizaciones a las políticas y procedimientos de la Entidad, controles nuevos o modificados para resolver incidentes de seguridad de la información y mejorar la seguridad.

- Los cambios en los servicios de los proveedores para implementar cambios y mejoras en las redes, el uso de nuevas tecnologías, la adopción de nuevos productos o versiones/ediciones más recientes, nuevas herramientas y ambientes de desarrollo, cambios en las ubicaciones físicas de las instalaciones de servicio, cambio de proveedores y/o contratación externa de otros proveedores.

16 GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

16.1 Gestión de Incidentes y Mejoras en la Seguridad de la Información

Objetivo: Asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación sobre eventos de seguridad y debilidades.

16.1.1 Responsabilidades y procedimientos

Control: Se debe establecer las responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.

- La OTIC promoverá entre los servidores públicos, contratistas, proveedores y partes interesadas, el deber de reportar los incidentes relacionados con la seguridad de la información.
- Los propietarios de los Activos de Información deben informar a la OTIC, a través de la Mesa de asistencia, los eventos e incidentes de seguridad de la información que identifiquen o que reconozcan ante su posibilidad de materialización.
- La Entidad en cabeza de la OTIC gestionará el incidente de seguridad y se apoyará con las áreas afectadas para el tratamiento de los incidentes de seguridad de la información, quienes tendrán la responsabilidad de investigarlo y solucionarlo, tomando las medidas necesarias para evitar su reincidencia.
- La OTIC ha implementado los siguientes controles: La gestión de incidentes de seguridad debe estar basada en los lineamientos del ProcedimientoP-A-GTI-11 Gestión de la operación de servicios tecnológicos, donde se debe establecer como mínimo: quiénes debe reportar, los canales de comunicación, tipo de situaciones que se debe reportar, decisiones sobre las

situaciones reportadas, respuesta a incidentes, aprendizaje de estos y recolección de evidencias digitales.

- Cualquier incumplimiento identificado debe remitirse a la OTIC - Seguridad de la información, quien debe determinar si el evento se considera como incidente de seguridad de la información, teniendo en cuenta las categorías y criterios de clasificación definidos M-A-GTI-03 Manual para la gestión de incidentes de seguridad y privacidad de la información.

16.1.2 Reporte de eventos de seguridad de la información

Control: Los eventos de seguridad de la información se debe informar a través de los canales de gestión apropiados, tan pronto como sea posible.

- Todos los servidores públicos, contratistas, proveedores y partes interesadas, que tengan acceso a información interna, confidencial (clasificada) y/o altamente confidencial (reservada), independiente de su medio de conservación física o digital, deben:
    - Reportar de manera oportuna y a través de los medios establecidos por la entidad, los eventos o incidentes de seguridad de la información técnicos y no técnicos, donde se puedan ver comprometidos la confidencialidad, integridad y disponibilidad de los activos de información. Lo anterior siguiendo los lineamientos del procedimiento de Gestión de Incidentes de seguridad P-A-GTI-11 Gestión de la operación de servicios tecnológicos.
- Para el reporte de eventos o incidentes de seguridad de la información se debe tener en cuenta entre otras las siguientes situaciones:
    - Al presentarse un evento asociado con la seguridad de la información tales como un control de seguridad ineficaz; violación de la integridad, confidencialidad o expectativas de disponibilidad de la información, errores humanos, violaciones de seguridad física, cambios no controlados en el sistema, mal funcionamiento en el software o hardware, violaciones de acceso, entre otros, se deben notificar inmediatamente a la OTIC a través de la herramienta de mesa de asistencia.

16.1.3 Reporte de debilidades de seguridad de la información

Control: Se debe exigir a todos los servidores públicos, contratistas, proveedores o terceros que usan los servicios y sistemas de información de la Entidad, que observen y reporten cualquier debilidad de seguridad de la información observada o sospechada en los sistemas o servicios.

- Todos los servidores públicos, contratistas, proveedores o terceros deben reportar a través de los canales definidos cualquier situación que se pueda considerar como una debilidad en la seguridad de la información.
- Los servidores públicos, contratistas, proveedores o terceros de la Entidad, que hagan uso de la infraestructura tecnológica de la Entidad debe informar a través de los canales oficiales

establecidos por La Entidad y de acuerdo con el procedimiento de Gestión de incidentes de seguridad de la información, aquellas debilidades que puedan comprometer los activos de información.

- La OTIC tiene documentado e implementado como control, el P-A-GTI-11 Gestión de la operación de servicios tecnológicos, M-A-GTI-03 Manual para la gestión de incidentes de seguridad y privacidad de la información.

16.1.4 Evaluación de eventos de seguridad de la información y decisiones sobre ellos

Control: Los eventos de seguridad de la información se debe evaluar y se debe decidir si se van a clasificar como incidentes de seguridad de la información.

- Con base en la información reportada, la OTIC – Seguridad de la Información debe realizar el respectivo análisis para establecer la ocurrencia de un incidente de seguridad de la información y la respectiva gestión de éste por parte del personal responsable del activo afectado.

16.1.5 Respuesta a incidentes de seguridad de la información

Control: Se debe dar respuesta a los incidentes de seguridad de la información de acuerdo con procedimientos documentados.

- La Entidad, debe designar personal calificado, para gestionar adecuadamente los incidentes de seguridad de la información reportados, siguiendo los lineamientos del procedimiento Gestión de incidentes de seguridad de la información, para garantizar la seguridad y la continuidad de los servicios comprometidos.
- La respuesta a incidentes de seguridad de la información debe contemplar entre otras las siguientes condiciones:
    - Recolectar la evidencia lo más pronto posible después de que ocurra el incidente;
    - Llevar a cabo análisis forense de seguridad de la información, según se requiera;
    - Llevar el asunto a una instancia superior (escalar), según se requiera.
    - Tratar las debilidades de seguridad de información que se encontraron que causan o contribuyen al incidente.
    - Una vez que el incidente se haya tratado exitosamente, cerrarlo formalmente y hacer un registro de esto.
- La Entidad cuenta con los siguientes documentos y herramienta:
    - Procedimiento y manual de gestión de Incidentes P-A-GTI-11 Gestión de la operación de servicios tecnológicos, M-A-GTI-03 Manual para la gestión de incidentes de seguridad y privacidad de la información
    - M-E-GET-04 Manual de Políticas Específicas de Seguridad y Privacidad de la Información.

- Herramienta de Gestión GEMA.

.

16.1.6 Aprendizaje obtenido de los incidentes de seguridad de la información

Control: El conocimiento adquirido al analizar y resolver incidentes de seguridad de la información se debe usar para reducir la posibilidad o el impacto de incidentes futuros.

- Se debe documentar en la mesa de asistencia todo el manejo y gestión de incidentes con el fin de gestionar las lecciones aprendidas y así fortalecer los controles y lineamientos asociados.

16.1.7 Recolección de evidencia

Control: La Entidad debe definir y aplicar procedimientos para la identificación, recolección, adquisición y preservación de información que pueda servir como evidencia.

- La Entidad incluye en el procedimiento Gestión de incidentes de seguridad de la información actividades para la identificación, recolección, adquisición y preservación de información que pueda servir como evidencia con propósitos de acciones legales y/o disciplinarias**.**
- La identificación, es el proceso que involucra la búsqueda, reconocimiento y documentación de evidencia potencial.
- Recolección, es el proceso de reunir elementos físicos que pueden contener evidencia potencial.

17 ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE CONTINUIDAD DE NEGOCIO

17.1 Continuidad de Seguridad de la Información

Objetivo: La continuidad de seguridad de la información se debe incluir en los sistemas de gestión de la continuidad de negocio de la Entidad.

17.1.1 Planificación de la continuidad de la seguridad de la información

Control: La Entidad debe determinar sus requisitos para la seguridad de la información y la continuidad de la gestión de la seguridad de la información en situaciones adversas, por ejemplo, durante una crisis o desastre.

- La Entidad debe realizar el diagnóstico del estado de la continuidad de la seguridad de la información, definir el plan (costo-beneficio) para cerrar las brechas identificadas y proveer los recursos suficientes para proporcionar una respuesta efectiva de sus funcionarios, colaboradores y procesos en caso de contingencia o eventos catastróficos que afecten la continuidad de la operación de la entidad. Este plan debe contener al menos los siguientes elementos:
    - La Entidad debe realizar un análisis de impacto del negocio identificando los procesos claves y los tiempos de recuperación. Especificaciones de TI, comunicaciones, sistemas, personal interno y contactos de emergencia.
    - La Entidad debe diseñar una estrategia de continuidad que salvaguarde la información crítica (indispensable para la operación de la entidad) donde incluyan contención, Backup y recuperación, sitio alterno, cubrimiento de seguros entre otros.

17.1.2 Implementación de la continuidad de la seguridad de la información

Control: la Entidad debe establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel de continuidad requerido para la seguridad de la información durante una situación adversa.

- La OTIC debe elaborar el plan de recuperación ante desastres (DRP) y retorno a la normalidad, para cada uno de los Servicios y Sistemas de Información que tengan un impacto alto en los procesos de la Entidad.
- La Entidad debe establecer, documentar, aprobar, implementar y mantener planes, procesos, procedimientos y controles para asegurar el nivel de continuidad de TI requerido para la seguridad de la información durante una situación adversa.

17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información

Control: La Entidad debe verificar a intervalos regulares los controles de continuidad de la seguridad de la información establecidos e implementados, con el fin de asegurar que son válidos y eficaces durante situaciones adversas.

- La Entidad, debe asegurar la realización de pruebas periódicas del Plan de Recuperación Ante Desastres (DRP) y/o Continuidad de Negocio, verificando la Seguridad de la Información durante su realización y la documentación de dichas pruebas.
- La Entidad, debe verificar a intervalos regulares los controles de Continuidad de la Seguridad de la Información, implementados con el fin de asegurar que son válidos y eficaces durante situaciones adversas.

17.2 Redundancias

Objetivo: Asegurar la disponibilidad de instalaciones de procesamiento de información.

17.2.1 Disponibilidad de instalaciones de procesamiento de información

Control: Las instalaciones de procesamiento de información se debe implementar con redundancia suficiente para cumplir los requisitos de disponibilidad.

La OTIC ha implementado los siguientes controles:

- La OTIC debe asegurar la disponibilidad de instalaciones de Procesamiento de Información de la Entidad y propender por la existencia de una Plataforma Tecnológica redundante que satisfaga los requerimientos de disponibilidad aceptables, de acuerdo con los niveles de servicio establecidos por La Entidad.
- La OTIC debe evaluar y probar soluciones de redundancia tecnológica y seleccionar la solución que mejor cumple los requerimientos de la Entidad.
- La OTIC, debe analizar y establecer los requerimientos de redundancia para los Sistemas de Información esenciales para la Entidad y la plataforma tecnológica que los apoya.
- La OTIC debe implementar una arquitectura con orientación a nube (responsables de infraestructura).
- La OTIC debe administrar las soluciones de redundancia tecnológica y realizar pruebas periódicas sobre dichas soluciones, para asegurar el cumplimiento de los requerimientos de disponibilidad de la Entidad.

18 CUMPLIMIENTO

18.1 Cumplimiento de Requisitos Legales y Contractuales

Objetivo: Evitar el incumplimiento de las obligaciones legales, estatutarias, de reglamentación o contractuales relacionadas con seguridad de la información, y de cualquier requisito de seguridad.

18.1.1 Identificación de la legislación aplicable y de los requisitos contractuales

Control: Se debe realizar la identificación y seguimiento de todos los requisitos normativos y contractuales aplicables a la seguridad de la información, así como la definición de las actividades que garanticen su debido cumplimiento.

- La Entidad debe identificar, documentar y actualizar las leyes, decretos, resoluciones y demás aplicables asociadas a la seguridad de la información, dentro del normograma de la entidad https://madsigestion.minambiente.gov.co/portal/normograma.php.
- Todos los servidores públicos, contratistas, proveedores y terceros de la Entidad deben dar cumplimiento las políticas de seguridad de la información establecidas dentro del presente documento de acuerdo con su aplicabilidad.

18.1.2 Derechos de propiedad intelectual

Control: Se debe implementar procedimientos apropiados para asegurar el cumplimiento de los requisitos legislativos, de reglamentación y contractuales relacionados con los derechos de propiedad intelectual y el uso de productos de software patentados.

- Se debe realizar el seguimiento y control de la instalación de software licenciado en cada uno de los recursos de la plataforma tecnológica.
- El Grupo de Servicios Administrativos debe realizar la gestión y seguimiento del inventario para el control del software adquirido por la entidad.
- El Grupo de Contratos debe incluir las cláusulas de propiedad intelectual y derechos de autor en contratos, que protejan el software, documentos, derechos de diseño, marcas registradas, patentes y códigos fuente en los casos requeridos.

.

18.1.3 Protección de registros

Control: los registros se deben proteger contra pérdida, destrucción, falsificación, acceso no autorizado y liberación no autorizada, de acuerdo con los requisitos legislativos, de reglamentación, contractuales y de negocio.

- La Entidad se obliga a proteger todos los registros que muestren evidencia del cumplimiento de los requisitos normativos, legales o regulatorios contra la pérdida de Confidencialidad, Integridad y Disponibilidad, siguiendo las directrices de inventario de Activos. (I-E-GET-02 Metodología para la identificación gestión y clasificación de activos de información).
- Se deben clasificar e identificar los registros de información y aplicar los respectivos controles para evitar su perdida, falsificación o acceso no autorizado (I-E-GET-02 Metodología para la identificación gestión y clasificación de activos de información).
- El grupo de Gestión Documental debe realizar la gestión de las tablas de retención documental para la identificación y periodos de tiempos que deben retenerse los registros.
- Todos los líderes de procesos deben mantener actualizado el inventario de activos de información identificando sus registros críticos.

18.1.4 Privacidad y protección de información de datos personales

Control: Se debe asegurar la privacidad y la protección de la información de datos personales, como se exige en la legislación y la reglamentación pertinentes, cuando sea aplicable.

- La entidad debe contar con una Política de protección de datos personales, la cual debe ser revisada, actualizada y socializada con cada una de las partes interesadas.
- Se deben identificar las bases de datos personales en cada una de las dependencias y realizar el respectivo tratamiento de acuerdo con los lineamientos establecidos. (I-E-GET-02 Metodología para la identificación gestión y clasificación de activos de información).
- Las dependencias que tratan datos personales deben asegurar que tendrán acceso únicamente las personas autorizadas por una necesidad laboral legitima, así como también debe identificarse la finalidad de recolección de los datos personales.
- La Entidad debe registrar las bases de datos personales en el Registro Nacional de Base de Datos de acuerdo con los lineamientos establecidos por la Superintendencia de Industria y Comercio.
- El grupo de contratos debe garantizar la suscripción de los acuerdos de confidencialidad con los proveedores de servicios y contratistas. (F-A-CTR-36 Acta de compromiso de confidencialidad) que garantice la confidencialidad de los datos personales recolectados en caso de que aplique.

18.1.5 Reglamentación de controles criptográficos

Control: Se debe usar controles criptográficos, en cumplimiento de todos los acuerdos, legislación y reglamentación pertinentes. La Entidad, se regirá por la Ley 527 de 1999 (acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las Entidades de certificación y otras disposiciones) y sus decretos reglamentarios, según aplique.

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

Control: El enfoque de la Entidad para la gestión de la seguridad de la información y su implementación (es decir, los objetivos de control, los controles, las políticas, los procesos y los procedimientos para seguridad de la información) se debe revisar independientemente a intervalos planificados o cuando ocurran cambios significativos.

- La Entidad debe gestionar la ejecución de auditorías internas y seguimiento, el cual incluye la revisión del SGSI de forma transversal.
- Se deben gestionar seguimientos a los controles documentados y establecidos en cada uno de los procesos de la entidad respecto a la seguridad de la información, que permitan analizar y evaluar su aplicabilidad y eficacia.
- Se debe realizar la revisión de las políticas de seguridad de la información por lo menos una vez al año.

18.2.2 Cumplimiento con las políticas y normas de seguridad

Control: Revisar con regularidad el cumplimiento del procesamiento y procedimientos de información dentro de su área de responsabilidad, con las políticas y normas de seguridad apropiadas, y cualquier otro requisito de seguridad.

- Es fundamental garantizar que todos los procedimientos de seguridad de la información se ejecuten correctamente, asegurando el cumplimiento de las políticas y estándares de seguridad establecidos, en alineación con los compromisos asumidos en los comités de gestión y desempeño.
- Se debe realizar una revisión periódica para verificar el cumplimiento de las políticas y normas de seguridad aplicables al centro de cómputo, identificando posibles desviaciones.
- En caso de detectar incumplimientos o violaciones a las políticas de seguridad de la información, estos deben ser reportados por la persona conocedora o parte interesada a través de la herramienta de gestión de servicios de TI, adjuntando las evidencias correspondientes para su oportuna gestión.

18.2.3 Revisión del cumplimiento técnico

Control: Los sistemas de información se deben revisar periódicamente para determinar el cumplimiento con las políticas y normas de seguridad de la información.

- Es necesario realizar validaciones periódicas de la configuración de las reglas y políticas establecidas en los sistemas de información de la Entidad, con el fin de identificar y gestionar posibles fallos que puedan surgir.
- Se deben llevar a cabo pruebas de vulnerabilidades en los sistemas de información, con el objetivo de detectar posibles debilidades en materia de seguridad y tomar las medidas correctivas necesarias.

REFERENCIAS

- Incibe_. (s.f.). *CONTRASEÑAS*. Obtenido de Instituto Nacional De Ciberseguridad: https://www.incibe.es/sites/default/files/contenidos/politicas/documentos/contrasenas.pdf
- Incibe_. (s.f.). *Copias De Seguridad*. Obtenido de Instituto Nacional De CiberSeguridad: https://www.incibe.es/sites/default/files/contenidos/guias/guia-copias-de-seguridad.pdf
- Incibe_. (s.f.). *Guía sobre borrado seguro de la información*. Obtenido de Instituto Nacional De Ciberseguridad: https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_ciberseguridad_borrado_seguro_metad.pdf
- Incibe_. (s.f.). *PROTECCIÓN DEL PUESTO DE TRABAJO*. Obtenido de Instituto Nacional De Ciberseguridad: https://www.incibe.es/sites/default/files/contenidos/politicas/documentos/proteccion-puesto-trabajo.pdf
- MinTic. (29 de Julio de 2016). *Modelo de Seguridad y Privacidad de la Información*. Obtenido dehttps://www.mintic.gov.co/gestionti/615/articles-5482_Modelo_de_Seguridad_Privacidad.pdf
- Pinzón Serrano, L. C. (s.f.). *Política de escritorio limpio y pantalla limpia*. Obtenido de MinTIC: https://www.mineducacion.gov.co/1780/articles-407695_galeria_02.pdf.
- Serrano, P. C. (s.f.). *Política sobre el uso de controles criptográficos*. Obtenido de MinTIC: https://www.mineducacion.gov.co/1759/articles-407695_galeria_07.pdf
- De Gestión, D., & Desempeño, I. (s/f). *Guía para la Administración del Riesgo y el diseño de controles en entidades públicas Versión 6*. Gov.co. Recuperado el 26 de septiembre de 2023, de https://www.funcionpublica.gov.co/documents/34645357/34702994/Guia-externa-administracion-riesgo-direccinamiento-estrategico-v6.pdf/0330fa64-0a6a-4772-887f-27aae325afa5?t=1685979801107
- *LEY 527 DE 1999*. (s/f). Gov.co. Recuperado el 26 de septiembre de 2023, de https://www.suin-juriscol.gov.co/viewDocument.asp?id=1662013
- *LEY 1273 DE 2009*. (s/f). Gov.co. Recuperado el 26 de septiembre de 2023, de https://www.suin-juriscol.gov.co/viewDocument.asp?ruta=Leyes/1676699
- *No title*. (s/f). Leyex.info. Recuperado el 26 de septiembre de 2023, de https://www.leyex.info/documents/leyes/601be1dc32bb1a2ee789f230cc6048df.htm
- NORMA TÉCNICA NTC-ISO/IEC COLOMBIANA 27001. (s/f). Gov.co. Recuperado el 26 de septiembre de 2023, de https://serviciocivil.gov.co/sites/default/files/marco-legal/2006_03_22_NTC-ISO-IEC%2027001.pdf
- Política, N., & De Confianza, Y. (s/f). *CONSEJO NACIONAL DE POLÍTICA ECONÓMICA Y SOCIAL REPÚBLICA DE COLOMBIA DEPARTAMENTO NACIONAL DE PLANEACIÓN*. Gov.co. Recuperado el 26 de septiembre de 2023, de https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3995.pdf
- *Preguntas Frecuentes*. (s/f). Gov.co. Recuperado el 26 de septiembre de 2023, de https://www.sic.gov.co/preguntas-frecuentes-pdp

- *RESOLUCION 1519 DE 2020*. (s/f). Gov.co. Recuperado el 26 de septiembre de 2023, de https://www.suin-juriscol.gov.co/viewDocument.asp?ruta=Resolucion/30044657
- (S/f-a). Gov.co. Recuperado el 26 de septiembre de 2023, de https://gobiernodigital.mintic.gov.co/692/articles-162625_recurso_2.pdf.
- (S/f-b). Gov.co. Recuperado el 26 de septiembre de 2023, de https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854.pdf
- (S/f-c). Gov.co. Recuperado el 26 de septiembre de 2023, de https://www.mintic.gov.co/gestionti/615/articles-5482_Modelo_de_Seguridad_Privacidad.pdf
- Resolución 500 de 202 https://gobiernodigital.mintic.gov.co/692/articles-162625_recurso_2.pdf.
- Directiva Presidencial 02 Del 24 De febrero De 2022;

MINISTERIO DE AMBIENTE Y DESARROLLO SOSTENIBLE

MATRIZ DE ROLES Y RESPONSABILIDADES EN EL SGSI

Matriz RACI para la implementación del proyecto ISO 27001

Tabla RASCI asocia roles en la organización con las secciones de ISO / IEC 27002.

Los roles se identifican como R, A, S, C o I, lo que significa entonces:

Responsable: Este rol tiene la responsabilidad principal de realizar las actividades en esta sección/componente del sistema.

Aprobador: Este rol será llamado a rendir cuentas si los riesgos se materializan (generalmente porque fallan los controles preventivos): generalmente es el responsable del proceso/presupuesto.

Apoyo: Esta función ayuda activamente con el diseño, la implementación o la gestión de las actividades de esta sección o componente del sitema.

Consultado: Esta es una función de no intervención, que ofrece orientación y dirección a quienes participan más activamente.

Informado: Esta función tiene interés en el estado de los riesgos en esta sección/componente y debe mantenerse en contacto con la situación.

Esta es una herramienta para ayudar a descubrir y describir quién hace qué en relación con el Sistema de Gestión de Seguridad de la Información.

Ilustración 1: ilustracion xxxxx

MINISTERIO DE AMBIENTE Y DESARROLLO SOSTENIBLE

Norma ISO/IEC 27002

R = Responsible A = Accountable S = Supportive C = Consulted I = Informed
R = Responsable A = Aprobador S = Apoyo C = Consultao I = Informado

		Propietarios de Activos de información	Funcionarios de la Entidad	Dirección de la Entidad - Despacho del Ministro	Director de TIC	Comité Sectorial de gestión y desempeño	Oficial de Seguridad de la Información - OSI	Equipo de seguridad de operaciones de SI	Director de Talento Humano	Secretaria General - Presupuesto	Director Jurídico área legal y de Cumplimiento	Director de Finanzas	Responsable de Gestión de Instalaciones Físicas	Responsable de Infraestructura de TI	Responsable de I+ D+ I	Oficina jefes de área o grupos de trabajo	Otras Direcciones ajenas a la Organización	Proveedores
5	**Políticas de seguridad e la Información**																	
5.1.1	Políticas para la seguridad de la información	C	I	C	R	A	R	S	C	S	C	C	C	S	C	C	C	R
5.1.2	Revisión de las políticas para la seguridad de la información	C	I	S	A	R	S	C	S	S	S	S	C	S	S	I	I	I
6	**Organización de la Seguridad de la Información**																	
6.1.1	Roles y Responsabilidades de la Seguridad de la Información	A		C	R	S	C		C		C			C	C			
6.1.2	Segregación de tareas	A	I		C	R	C	S						C				
6.1.3	Contacto con autoridades	A			C	S	S	S			R							
6.1.4	Contacto con grupos especiales de interés	A			C	C	R	S			S			S				
6.1.5	Seguridad de la información en gestión de proyectos	A			C	R	S	S						S				
6.2.1	Política para dispositivos móviles	A	I		C	R	S	C						C				I
6.2.2	Teletrabajo	A	I		R	S	C	C						C				I
7	**Seguridad de los Recursos Humanos**																	
7.1.1	Verificación de antecedentes	A				S	S		R									
7.1.2	Términos y condiciones para el empleo	A	I			S			S		R							
7.2.1	Responsabilidades de la dirección	A	I	C	R	S			S									
7.2.2	Toma de conciencia, educación y entrenamiento en seguridad de la información	A	I		S	R	S	S	S		C							
7.2.3	Procesos disciplinarios	A	I		S				R									
7.3.1	Terminación o cambio en las responsabilidades del empleo	A	I			S			S		R			S				
8	**Gestión de activos**																	
8.1.1	Inventario de activos	A				S	S	S		R					C			
8.1.2	Propiedad de los activos	R			R	S	A					S	S	C				
8.1.3	Uso aceptable de los activos	A	I			R	S	C	S	C			S					I
8.1.4	Devolución de activos	A	I		R	C	A	S	S	S		C	S	S				I
8.2.1	Clasificación de la información	A	I		S	R	C	S										
8.2.2	Etiquetado de la información	A	I			S	R	S	C	C	C	C	S	S				
8.2.3	Manejo de activos	A	I			C	S					C	S	R				
8.3.1	Gestión de medios removibles	A	I			S	S	C					S	R				
8.3.2	Eliminación de medios	A	I			S	A	S				C		R				
8.3.3	Transferencia de medios físicos	A	I			S	C	C						R				I

Control de acceso																				
9.1.1	Política de control de acceso	A			S	R	S	S	C	C				S				I		
9.1.2	Acceso a redes y servicios de red	A	I			S	C	S						R				I		
9.2.1	Registro y de-registro de usuarios	A				S	C		R					S						
9.2.2	Suministro de acceso a usuarios	A				S	C		S					S						
9.2.3	Gestión de derechos de acceso removibles	A				S								R				I		
9.2.4	Gestión de información secreta de autenticación de usuarios	A				S	C	C						R						
9.2.5	Revisión de derechos de acceso de los usuarios	A			C	S	R	S	C					S						
9.2.6	Remoción o ajuste de derechos de acceso	A				S	S	C						R						
9.3.1	Uso de información secreta de autenticación	A	I			S		S						R						
9.4.1	Restricción de acceso a la información	A	I			S	C							R						
9.4.2	Procedimientos seguros de inicio de sesión	A				S	C							R				I		
9.4.3	Gestión de contraseñas	A				S	C	S						R						
9.4.4	Uso de privilegios de programas utilitarios	A	I			S	C	S						R				I		
9.4.5	Control de acceso al código fuente de las aplicaciones	A	I			S	C	S						R				I		
10 Criptografía																				
10.1.1	Política de uso de controles Criptográficos	A	I			S	R	S						S						
10.1.2	Gestión de claves	A				S	R							S						
11 Seguridad Física y Ambiental																				
11.1.1	Perímetro de seguridad física	A	I			S	C	S					R	C						
11.1.2	Controles físicos de entrada	A	I			S	C	S					R	C						
11.1.3	Aseguramiento de oficinas, áreas e instalaciones	A	I			S	C	S					R	C						
11.1.4	Protección contra amenazas externas y ambientales	A	I			S	C	S					R	C						
11.1.5	Trabajo en áreas seguras	A	I			S	C	S					R					I		
11.1.6	Áreas de entrada y carga	A	I			S	C	S					R							
11.2.1	Emplazamiento y protección de equipos	A	I			S	C	S					R					I		
11.2.2	Servicios de soporte	A				S	C	S					R	C						
11.2.3	Seguridad en cableado	A				S	C	S					S	R						
11.2.4	mantenimiento de equipos	A				S	C	S					R							
11.2.5	Remoción de activos	A	I			S	C	S					R							
11.2.6	Seguridad de equipos y activos fuera de sitio	A	I			S	C	S					C	R						
11.2.7	Eliminación segura o reúso de equipos	A	I			S	C	S					S	R						
11.2.8	Equipo de usuario desatendido	A	I			S	C	S					S	R						
11.2.9	Política de escritorio y pantalla limpia	A	I			S	C	S					S	R				I		
12 Seguridad en las Operaciones																				
12.1.1	Procedimientos operativos de Operación	A					C	S						R				I		
12.1.2	Manejo del cambio	A	I		S	R	S			S				S	C					
12.1.3	Gestión de la capacidad	A			S	R				S			C	S	C					
12.1.4	Separación de ambientes de prueba y producción.	A			S	R	C	S						S						
12.2.1	Controles antimalware	A			S		C	S		C				R	C			I		
12.3.1	Copia de respaldo de la Información. Backup	A			R	S	C			S				S						
12.4.1	Registro de eventos	A			S	S	C	S		S				R						
12.4.2	Protección de la información de registros (Logs)	A			S	S	R	C		S				S						
12.4.3	Registro (Logs) del Administrador y el operador	A				S	R	S						S						
12.4.4	Sincronización de relojes	A					C	S						R						
12.5.1	Instalación de software en sistemas en producción.	A	I			S	C			C				R						
12.6.1	Gestión de las vulnerabilidades técnicas	A				S	S	S						R						
12.6.2	Restricciones en la instalación de software	A	I			S	S	S						R						
12.7.1	Controles de auditoria en sistemas de información	A			S	S	R	S						S	C					
13 Seguridad en comunicaciones																				
13.1.1	Controles de red	A				S	C	S						R				I		
13.1.2	Seguridad en servicios de red.	A				S	C							R				I		
13.1.3	Segregación en las redes.	A				S	C							R	S					
13.2.1	Políticas y procedimientos para transferencia de información.	A	I			S	R							S				I		
13.2.2	Acuerdos de transferencia de información.	A			S	R	S							S						
13.2.3	Mensajería electrónica	A	I		S	S	C				C			R				I		
13.2.4	Acuerdos de confidencialidad y no divulgación.	A			S	S	S		S		R	S		S				R		
14 Adquisición, desarrollo y mantenimiento de sistemas.																				
14.1.1	Análisis y especificación de requisitos en seguridad de la información.	A			C	S	R			C				C	C	I	I			
14.1.2	Aseguramiento de servicios de aplicaciones en redes públicas.	A			C	R	S	S						S	C					
14.1.3	Protección de transacciones en servicios y aplicaciones.	A				S	C	S						R						
14.2.1	Política de desarrollo seguro.	A			C	S	S							S	R	I	I	I		
14.2.2	Procedimiento de control de cambio en sistemas	A			C	S	R			C				S	C					
14.2.3	Revisión técnica de aplicaciones luego de cambios en plataformas de producción.	A				S	R							S						
14.2.4	Restricciones en cambios los paquetes de software.	A				S	S	S						R	C			I		
14.2.5	Principios de la ingeniería en sistemas seguros	A				R	S							S	S					
14.2.6	Ambiente de desarrollo seguro	A				S	S							S	R			R		
14.2.7	Desarrollo tercerizado.	A				S	S	C						S	R					
14.2.8	Prueba de seguridad en los sistemas	A				S	R	S						S	S					
14.2.9	Pruebas de aceptación de los sistemas	A	C			S	S							S	R					
14.3.1	Protección de datos de prueba	A				R	S	S						S	S			I		
15 Relación con los proveedores																				
15.1.1	Política de seguridad de la información para relaciones con los proveedores	A			C	R	S	S								I	I	I		
15.1.2	Incorporación de la seguridad en los acuerdos con los proveedores.				A	S	R				S			S				R		
15.1.3	Cadena de suministro para las tecnologías de la información y las comunicaciones				A	S	R							S						
15.2.1	Supervisión y revisión en los servicios con proveedores	A					S	C						R						
15.2.2	Gestión de cambios a servicios de proveedores	A				S	S							R						
16 Gestión de incidentes de seguridad de la información.																				
16.1.1	Responsabilidades y procedimientos	A				R	S		S		C		S	S						
16.1.2	Reporte de eventos de seguridad de la información	A	I			S	R	S					S	S		I	I	I		
16.1.3	Reporte de debilidades en la seguridad de la información	A	I			S	R	S					S	S		I	I	I		
16.1.4	Evaluación y decisiones en eventos de seguridad de la información	A				R	S	S			C		S	S						
16.1.5	Respuesta a incidentes de seguridad de la información	A		C		S	R	S			C		S	S						
16.1.6	Aprendizaje de los incidentes en seguridad de la información	A				R	S	C	C			C	C	C	C					
16.1.7	Recolección de evidencia	A					R	S			C		S	S				S		
17 Aspectos de seguridad de la información en la gestión de la continuidad del negocio.																				
17.1.1	Planeación de la continuidad de la seguridad de la información	A				S	R						S	S		R	R	I		
17.1.2	Implementar la continuidad de la seguridad de la información.				S	S	R						S	S		R	R	R		
17.1.3	Verificar, revisar y evaluar la continuidad de la seguridad de la información.						A	R					S	S				R		
17.2.1	Disponibilidad en las instalaciones de procesamiento de información.				S	S	A						R	S				R		
18 Cumplimiento																				
18.1.1	Identificar requisitos legales y contractuales aplicables.	A	I	C	S	S	S				S		S	S				I		
18.1.2	Derechos de propiedad intelectual	A	I	C	R	S	S				C			S				I		
18.1.3	Protección de registros	A	I	C	R	S	S							S				I		
18.1.4	Privacidad y protección de la información identificable como personal.	A	I	C	S	S	S				R			S				I		
18.1.5	Regulación de controles criptográficos.	A				R					C			S						
18.2.1	Revisión independiente de la seguridad de la información	A			R	S								C						
18.2.2	Cumplimiento con políticas de seguridad y estándares	A	I	C	S	R					C			S		I	I	I		
18.2.3	Revisión de cumplimiento técnico	A			S	R					C			S						
	Número de responsabilidades	1	0	0	10	22	22	1	3	1	5	0	11	34	4	2	2	7	125	RESPONSABLE
	Número de responsabilidades	106	0	0	3	1	5	0	0	0	0	0	0	0	0	0	0	0	115	APTOBADOR
	Número de controles soportados	0	0	1	20	81	35	55	10	8	4	3	20	52	5	0	0	1	295	APOYO
	Número de controles sobre los que se consultó	2	1	9	11	3	41	12	6	7	13	6	5	14	11	1	1	0	143	COSULTADO
	Número de controles de los que se informó	0	48	0	0	0	0	0	0	0	0	0	0	0	0	7	7	33	95	INFORMADO