SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI)

POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

GOBERNACIÓN DEL ATLÁNTICO

2023

CONTROL DE DOCUMENTOS

Fecha	Autor	Versión	Referencia de Cambios
30-07- 2018	Secretaría De Tecnologías	1	Creación del documento
05-09-2023	Network Security Team	2	Actualización del documento

Revisado por :

Fecha	Nombre	Dependencia
15-09-2023	Grupo de Gestión de TI	Secretaría General.

POLITICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Contenido

0. INTRODUCCIÓN

La dirección de la GOBERNACIÓN DEL ATLÁNTICO, entendiendo la importancia de una adecuada gestión de la información, se ha comprometido con la implementación de un sistema de gestión de seguridad de la información buscando establecer un marco de confianza en el ejercicio de sus deberes con el Estado y los ciudadanos, todo enmarcado en el estricto cumplimiento de las leyes y en concordancia con la misión y visión de la entidad.
Para la GOBERNACIÓN DEL ATLÁNTICO, la protección de la información busca la disminución del impacto generado sobre sus activos, por los riesgos identificados de manera sistemática con objeto de mantener un nivel de exposición que permita responder por la integridad, confidencialidad y la disponibilidad de la misma, acorde con las necesidades de los diferentes grupos de interés identificados.

De acuerdo con lo anterior, esta política aplica a la Entidad según como se defina en el alcance, sus funcionarios, terceros, aprendices, practicantes, proveedores y la ciudadanía en general, teniendo en cuenta que los principios sobre los que se basa el desarrollo de las acciones o toma de decisiones alrededor del SGSI estarán determinadas por las siguientes premisas:

- ✓ Minimizar el riesgo en las funciones más importantes de la entidad.
- ✓ Cumplir con los principios de seguridad de la información.
- ✓ Cumplir con los principios de la función administrativa.
- ✓ Mantener la confianza de sus clientes, socios y empleados.
- ✓ Apoyar la innovación tecnológica.
- ✓ Proteger los activos tecnológicos.
- ✓ Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.
- ✓ Fortalecer la cultura de seguridad de la información en los funcionarios, terceros, aprendices, practicantes y clientes de la GOBERNACIÓN DEL ATLÁNTICO
- ✓ Garantizar la continuidad del negocio frente a incidentes.
- ✓ La GOBERNACIÓN DEL ATLÁNTICO ha decidido definir, implementar, operar y mejorar de forma continua un Sistema de Gestión de Seguridad de la Información, soportado en lineamientos claros alineados a las necesidades del negocio, y a los requerimientos regulatorios.

1. ALCANCE

Las políticas de Seguridad de la Información establecen las directrices requeridas para la implementación de un Sistema de Gestión de Seguridad de la Información confiable y flexible, y definen el marco básico que guiará la implantación de cualquier requisito, proceso, procedimiento, y/o acción, relacionados con la Seguridad de la Información.

Estas políticas aplican a todos los funcionarios, contratistas y terceros que tengan acceso a los servicios de red, aplicaciones y sistemas de información de la GOBERNACIÓN DEL ATLÁNTICO, y a las partes interesadas que accedan o hagan uso de cualquier activo de información independientemente de su ubicación, medio o formato; definen quiénes deben mantener la debida confidencialidad sobre la información de la Entidad por el tiempo que se estipule en los acuerdos establecidos.

Adicionalmente, las políticas aplican a todos los activos de información que se encuentren relacionados directa o indirectamente con el manejo de información creada, procesada o utilizada en el soporte y desarrollo de los procesos de la Entidad.

2. OBJETIVOS

2.1 Objetivo General

Establecer lineamientos de seguridad de alto nivel que permitan que los activos de información de propiedad de la GOBERNACIÓN DEL ATLÁNTICO, sean accedidos sólo por las personas autorizadas que tienen necesidad legítima para la realización de las funciones propias de la Entidad (confidencialidad), que no se realicen modificaciones sin autorización y se salvaguarde su exactitud y completitud (integridad), y que sean accesibles y utilizables cuando éstos se requieran para el desarrollo de las actividades propias de la Entidad (disponibilidad); alineados con la misión, visión, objetivos estratégicos y valores corporativos de la GOBERNACIÓN DEL ATLÁNTICO.

2.2 Objetivos Específicos

Los objetivos específicos de las políticas de Seguridad de la Información en la GOBERNACIÓN DEL ATLÁNTICO son:

a) Definir los fundamentos para el Sistema de Gestión de Seguridad de la Información (SGSI).
b) Proteger la imagen, los intereses y el buen nombre de la GOBERNACIÓN DEL ATLÁNTICO.
c) Reducir el nivel de riesgo en Seguridad de la Información, gracias a la definición, implementación y ejecución efectiva de controles.
d) Promover una cultura organizacional orientada a la Seguridad de la Información, manteniendo una comunicación asertiva entre la Alta Dirección y los funcionarios, contratistas y terceros de la Entidad.
e) Establecer y comunicar la responsabilidad en el uso de los activos de información, que soportan los procesos y sistemas de la Entidad.
f) Asegurar la continuidad en los procesos de la GOBERNACIÓN DEL ATLÁNTICO permitiendo el cumplimiento de los objetivos estratégicos de la Entidad.
g) Cumplir con la legislación colombiana en los temas referentes a la seguridad de la información y a los requerimientos relacionados con la protección de datos personales.
h) Buscar la mejora continua en los procesos asociados a la seguridad de la información.

3. COMPROMISO DE LA ALTA DIRECCIÓN

La Gobernadora como muestra de su apoyo a la seguridad de la información, demuestra su compromiso a través de:

a) La autorización para la implementación de políticas de Seguridad de la Información en la GOBERNACIÓN DEL ATLÁNTICO.
b) La revisión y aprobación de las políticas de Seguridad de la Información.
c) El suministro de los recursos necesarios para una adecuada implementación de políticas de Seguridad de la Información en el marco de la implementación del Sistema de Gestión de Seguridad de la Información.
d) La divulgación sobre la importancia en el cumplimiento de las políticas de Seguridad de la Información para el logro de los objetivos de seguridad.

El compromiso de la Alta Dirección asegura la identificación, evaluación, tratamiento, monitoreo y control de los riesgos que puedan afectar la seguridad de la Información, mediante la destinación de los recursos físicos, humanos y económicos necesarios para el establecimiento, la implementación, el mantenimiento y la mejora continua del Sistema de Gestión de Seguridad de la Información en los procesos productivos, misionales y administrativos.

4. POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN

La Gobernación del Atlántico establecerá un esquema de seguridad de la información en donde existan roles y responsabilidades definidos que consideren actividades de administración, operación y gestión de la seguridad de la información.

La Alta Dirección de la GOBERNACIÓN DEL ATLÁNTICO, deduciendo la importancia de una adecuada gestión de la información, se ha comprometido con la implementación de un Sistema de Gestión de Seguridad de la Información, buscando establecer un marco de confianza en el ejercicio de sus deberes con el Estado y los ciudadanos; alineado con el ordenamiento jurídico y normativo en concordancia con la misión, visión, objetivos estratégicos y valores de la Entidad.

Para la GOBERNACIÓN DEL ATLÁNTICO, la protección de la información busca la disminución del impacto generado sobre los activos de información por los riesgos identificados de manera sistemática; con el propósito de mantener un nivel aceptable de exposición que permita responder por la confidencialidad, disponibilidad e integridad de la información, acorde con las necesidades de los diferentes grupos de interés identificados.

4.1 Objetivo General del SGSI

Definir en la Entidad lineamientos de acuerdo con lo establecido en el alcance; teniendo en cuenta los principios sobre los que se basa el desarrollo de las acciones o toma de decisiones alrededor del SGSI determinadas por las siguientes premisas:

a. Minimizar el riesgo a niveles aceptables definidos por la Entidad.
b. Establecer las políticas, procedimientos e instructivos en materia de Seguridad de la Información.
c. Cumplir con los principios de Seguridad de la Información: confidencialidad, disponibilidad e integridad.
d. Implementar el sistema de gestión de seguridad de la información.
e. Proteger los activos de información de la Entidad.
f. Fortalecer la cultura de Seguridad de la Información en los funcionarios, usuarios, terceros y contratistas de la GOBERNACIÓN DEL ATLÁNTICO.
g. Asegurar la continuidad del negocio en la Entidad frente a incidentes de seguridad de la información.
h. Apoyar la innovación tecnológica.
i. Mantener la confianza de los funcionarios, contratistas y terceros.
j. Garantizar la continuidad del negocio.
k. Cumplir con los principios de la función administrativa.

La GOBERNACIÓN DEL ATLÁNTICO ha decidido definir, implementar, operar y mejorar de forma continua un SGSI, soportado en lineamientos claros alineados a las necesidades de la Entidad y sus requerimientos regulatorios.

4.2 Alcance y Aplicabilidad

Las políticas de seguridad de la información aplican a todos los aspectos administrativos y de control y deben ser cumplidas por toda la entidad, sus funcionarios, contratistas y/o terceros de la GOBERNACIÓN DEL ATLÁNTICO y la ciudadanía en general que interactué con los sistemas de información de la entidad.

4.3 Sanciones

El cumplimiento de las Políticas de Seguridad de la Información es de carácter obligatorio, cada uno de los funcionarios, contratistas y/o terceros debe comprender su rol y asumir su responsabilidad respecto a los riesgos en Seguridad de la Información y la protección de los activos de información de la Entidad.

El incumplimiento de las políticas de Seguridad de la Información, que conlleve a comprometer la confidencialidad, disponibilidad y/o integridad de la información puede resultar en una acción disciplinaria o en acciones legales que apliquen a la normatividad del Gobierno Nacional y Territorial.

Las políticas de seguridad de información de la GOBERNACIÓN DEL ATLÁNTICO están desarrolladas para ajustarse o exceder, sin contravenir, las medidas de protección establecidas en la normatividad vigente. Si algún funcionario, contratista y/o tercero de la Entidad considera que alguna política de seguridad de información está en conflicto con las leyes y regulaciones existentes, lo debe reportar en forma inmediata al personal encargado de la seguridad de la información de la Entidad.

4.4 Términos y Definiciones

Las expresiones utilizadas en este documento deben ser entendidas con el significado que a continuación se indica. Los términos definidos son aplicados en singular y en plural de acuerdo como lo requiera el contexto en el cual son considerados. Y aquellos que no se encuentren definidos a continuación, deben entenderse con su significado natural.

Los Términos y Definiciones mostrados a continuación fueron tomados de las referencias listadas al final del documento.

Activo de Información: En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de esta (sistemas, soportes, edificios, personas, entre otros) que tenga valor para la organización. [1]

Amenaza: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. [2]

Antimalware: [Definición modificada tomando como base la definición de Antivirus de MinTIC]. Antimalware es una categoría de software de seguridad que protege un equipo de malware, normalmente a través de la detección en tiempo real y también mediante análisis del sistema, que pone en cuarentena y elimina los softwares maliciosos. El antimalware debe ser parte de una estrategia de seguridad estándar de múltiples niveles. [3]

Archivo: Es el 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, 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. [4]

Autenticidad: Propiedad de que una entidad es lo que afirma ser. [2]

Autorización: Consentimiento previo, expreso e informado del Titular para llevar a cabo el tratamiento de datos personales. [5]

Ciberseguridad: Preservación de la confidencialidad, la integridad y la disponibilidad de la información y/o de los sistemas de información a través del medio cibernético. Asimismo, pueden estar involucradas otras propiedades, tales como la autenticidad, la trazabilidad, el no repudio y la confiabilidad.[2]

Cifrado: Proceso para convertir información en un formato ilegible, a excepción de los titulares de una clave criptográfica específica. El cifrado se utiliza para proteger la información entre el proceso de cifrado y el proceso de descifrado (lo contrario del cifrado) de la divulgación no autorizada. [6]

Confidencialidad: Propiedad según la cual la información no está disponible para personas, entidades, procesos o sistemas no autorizados, ni se da a conocer a personas, entidades, procesos o sistemas no autorizados. [2]

Contraseña: Forma de autentificación de un usuario, a través de una clave secreta,
para controlar el acceso a algún recurso o herramienta. En caso de que no se proporcione la clave correcta no se permitirá el acceso a dichos elementos. [13]

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. [3]

Correo Electrónico Institucional: Es el servicio de correo electrónico que provee y administra directamente la GOBERNACIÓN DEL ATLÁNTICO a sus funcionarios, como herramienta de apoyo a las funciones y responsabilidades de estos. [13]

Disponibilidad: Propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada, cuando ésta así lo requiera. [2]

Dispositivo Móvil: Un dispositivo móvil se puede definir como un aparato de pequeño tamaño, con algunas capacidades de procesamiento, con conexión permanente o intermitente a una red, con memoria limitada, que ha sido diseñado específicamente para una función, pero que puede llevar a cabo otras funciones más generales. [7]

Evaluación de Riesgo: Proceso de comparación de los resultados del análisis del riesgo con los criterios de riesgo para determinar si el riesgo y/o su magnitud son aceptables o tolerables. [6]

Firma Digital: Datos añadidos o transformación criptográfica de una unidad de datos que prueba al receptor de dicha información la fuente y/o integridad de los datos contra posibles falsificaciones. Es un mecanismo de seguridad, e incluye el proceso de firmado y el de verificación de la firma. [6]

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. [2]

Gestión Documental: Es el conjunto de actividades administrativas y técnicas tendientes a la planificación, procesamiento, manejo y organización de la documentación producida y recibida por los sujetos obligados, desde su origen hasta su destino final, con el objeto de facilitar su utilización y conservación. [4]

Incidente de Seguridad de la Información: Evento singular o serie de eventos de seguridad de la información, inesperados o no deseados, que tienen una probabilidad significativa de comprometer las operaciones del negocio y de amenazar la seguridad de la información [2]

Información: Se refiere a un conjunto organizado de datos contenido en cualquier documento que los sujetos obligados generen, obtengan, adquieran, transformen o controlen. [4]

Información Pública: Es toda información que un sujeto obligado genere, obtenga, adquiera, o controle en su calidad de tal. [4]

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. [4]

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 de esta ley. [4]

Integridad: propiedad exactitud y completitud. [2]

Inventario de Activos: Lista de todos aquellos recursos (físicos, de información, software, documentos, servicios, personas, intangibles, etc.) dentro del alcance del SGSI, que tengan valor para la organización y necesiten por tanto ser protegidos de potenciales riesgos. [2]

Malware: El malware es la descripción general de un programa informático que tiene efectos no deseados o maliciosos. Incluye virus, gusanos, troyanos y puertas traseras. El malware a menudo utiliza herramientas de comunicación populares, como el correo electrónico y la mensajería instantánea, y medios magnéticos extraíbles, como dispositivos USB, para difundirse. También se propaga a través de descargas inadvertidas y ataques a las vulnerabilidades de seguridad en el software. La mayoría del malware peligroso actualmente busca robar información personal que pueda ser utilizada por los atacantes para cometer acciones delictivas. [8]

Repudio: Denegación, por una de las entidades implicadas en un a comunicación, de haber participado en la totalidad o en parte de dicha comunicación [6]

Proceso: Conjunto de actividades interrelacionadas o interactuantes que transforman unas entradas en salidas. [2]

Propietario de Activo de Información: Persona responsable de la integridad, confidencialidad y disponibilidad de una cierta información. Debe tener autoridad para especificar y exigir las medidas de seguridad necesarias para cumplir con sus responsabilidades, pudiendo delegar los aspectos operacionales en responsables de seguridad. [6]

Proveedor de Redes y Servicios: Persona jurídica responsable de la operación de redes y/o de la provisión de servicios de telecomunicaciones a terceros. [3]

Publicar o Divulgar: Significa poner a disposición en una forma de acceso general a los miembros del público e incluye la impresión, emisión y las formas electrónicas de difusión. [4]

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. [2]

Seguridad de la Información: Preservación de la confidencialidad, integridad y disponibilidad de la información. [2]

Sistema de Gestión de Seguridad de la Información SGSI: Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión y de mejora continua. [2]

Spam: También conocido como correo basura, el spam es correo electrónico que involucra mensajes casi idénticos enviados a numerosos destinatarios. Un sinónimo común de spam es correo electrónico comercial no solicitado (UCE). El malware se utiliza a menudo para propagar mensajes de spam al infectar un equipo, buscar direcciones de correo electrónico y luego utilizar esa máquina para enviar mensajes de spam. Los mensajes de spam generalmente se utilizan como un método de propagación de los ataques de phishing. [3]

Sujetos Obligados: Se refiere a cualquier persona natural o jurídica, pública o privada incluida en el artículo 5 de la Ley 1712 de 2014. [4]

Teletrabajo: Es una forma de organización laboral, que consiste en el desempeño

de actividades remuneradas o prestación de servicios a terceros utilizando como soporte las tecnologías de la información y la comunicación – TIC para el contacto entre el trabajador y la empresa, sin requerirse la presencia física del trabajador en un sitio específico de trabajo. [9]

Teletrabajador: Persona que desempeña actividades laborales a través de tecnologías de la información y la comunicación por fuera de la empresa a la que presta sus servicios. [9]

Trabajo en Casa: El trabajo en casa permite que los empleadores autoricen a sus trabajadores ante una situación ocasional temporal y excepcional a realizar sus labores desde su lugar de residencia como alternativa para el desarrollo de actividades. [10]

Transferencia de Datos: La transferencia de datos tiene lugar cuando el responsable y/o Encargado del Tratamiento de datos personales, ubicado en Colombia, envía la información o los datos personales a un receptor, que a su vez es Responsable del Tratamiento y se encuentra dentro o fuera del país. [11]

Tratamiento de Datos Personales: Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión. [5]

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. [2]

Usuario: Es la persona natural, nacional o extranjera titular de cédula de extranjería, o la persona jurídica, de naturaleza pública o privada, que haga uso de los servicios ciudadanos digitales. [12] En la GOBERNACIÓN DEL ATLÁNTICO se refiere a directivos, funcionarios, contratistas, terceros y otros colaboradores, debidamente autorizados para usar equipos, sistemas o aplicativos informáticos disponibles en la red de la Entidad y a quienes se les otorga un nombre de usuario y una contraseña.

VPN: Una red privada virtual, también conocida por sus siglas VPN (Virtual Private Network) es una tecnología de red que permite una extensión segura de una red local (LAN) sobre una red pública o no controlada como Internet. [6]

Vulnerabilidad: Debilidad de un activo o control que pueda ser explotado por una o más amenazas. [2]

4.5 Principios de Seguridad

A continuación, se establecen los principios de seguridad que soportan el SGSI de la GOBERNACIÓN DEL ATLÁNTICO:

- ✓ Las responsabilidades frente a la seguridad de la información serán definidas, compartidas, publicadas y aceptadas por cada uno de los empleados, proveedores, socios de negocio o terceros.
- ✓ La GOBERNACIÓN DEL ATLÁNTICO protegerá la información generada, procesada o resguardada por los procesos de negocio, su infraestructura tecnológica y activos del riesgo que se genera de los accesos otorgados a terceros (ej.: proveedores o clientes), o como resultado de un servicio interno en outsourcing.
- ✓ La GOBERNACIÓN DEL ATLÁNTICO protegerá la información creada, procesada, transmitida o resguardada por sus procesos de negocio, con el fin de minimizar impactos financieros, operativos o legales debido a un uso incorrecto de esta. Para ello es fundamental la aplicación de controles de acuerdo con la clasificación de la información de su propiedad o en custodia.
- ✓ La GOBERNACIÓN DEL ATLÁNTICO protegerá su información de las amenazas originadas por parte del personal.
- ✓ La GOBERNACIÓN DEL ATLÁNTICO protegerá las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos.
- ✓ La GOBERNACIÓN DEL ATLÁNTICO controlará la operación de sus procesos de negocio garantizando la seguridad de los recursos tecnológicos y las redes de datos.
- ✓ La GOBERNACIÓN DEL ATLÁNTICO implementará control de acceso a la información, sistemas y recursos de red.
- ✓ La GOBERNACIÓN DEL ATLÁNTICO garantizará que la seguridad sea parte integral del ciclo de vida de los sistemas de información.
- ✓ La GOBERNACIÓN DEL ATLÁNTICO garantizará a través de una adecuada gestión de los eventos de seguridad y las debilidades asociadas con los sistemas de información una mejora efectiva de su modelo de seguridad.
- ✓ La GOBERNACIÓN DEL ATLÁNTICO garantizará la disponibilidad de sus procesos de negocio y la continuidad de su operación basada en el impacto que pueden generar los eventos.
- ✓ La GOBERNACIÓN DEL ATLÁNTICO garantizará el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas.

El incumplimiento a la política de Seguridad y Privacidad de la Información traerá consigo, las consecuencias legales que apliquen a la normativa de la Entidad, incluyendo lo establecido en las normas que competen al Gobierno nacional y territorial en cuanto a Seguridad y Privacidad de la Información se refiere.

5 POLÍTICAS ESPECÍFICAS A CONTROLES ORGANIZACIONALES

La GOBERNACIÓN DEL ATLÁNTICO considera la información como un activo fundamental, razón por la cual es necesario establecer un marco normativo para asegurar que la información es protegida, independientemente de la forma en que ésta sea generada, manejada, procesada, transportada o almacenada. Así mismo, en la Entidad se reconoce la importancia de la implementación de Políticas de Seguridad de la Información, con el fin de mantener y mejorar continuamente el Sistema de Gestión de Seguridad de la Información y asegurar la confidencialidad, disponibilidad e integridad de la información.

Las políticas específicas de Seguridad de la Información, constituyen un eje fundamental del Sistema de Gestión de Seguridad de la Información de la Entidad, se consideran la base para la implementación de los controles, procedimientos y estándares definidos y serán revisadas periódicamente, para que en caso de cambios relevantes en la Entidad que incidan en la Seguridad de la Información, sigan siendo adecuadas y ajustadas a las recomendaciones de la Guía de Seguridad y Privacidad de la Información establecida por MINTIC y la Norma NTC- ISO-IEC 27001:2022.

5.1 Roles y responsabilidades de seguridad de la información

La Gobernación del Atlántico establecerá un esquema de seguridad de la información en donde existan roles y responsabilidades definidos que consideren las actividades de administración, operación y gestión de la seguridad de la información.

5.1.1 Alta Dirección

La Alta Dirección de la Gobernación del Atlántico debe definir, establecer e informar los roles y responsabilidades relacionados con la seguridad de la información en niveles directivo y operativo.

La Alta Dirección deberá definir y establecer el procedimiento de contacto con las autoridades, y establecer cuando y que autoridades se deben contactar para diferentes escenarios, además de definir el responsable para establecer dicho contacto.

La Alta Dirección debe revisar y aprobar las Políticas de Seguridad de la Información contenidas en este documento.

La Alta Dirección debe exigir a todo el personal de la entidad que aplique las políticas y procedimientos de seguridad de la información.

La Alta Dirección debe promover activamente una cultura de concienciación relacionada con seguridad de la información.

La Alta Dirección debe facilitar la divulgación de las Políticas de Seguridad de la Información a todos los funcionarios, contratistas y personal provisto por terceras partes que desarrollen actividades en la Gobernación del Atlántico.

La Alta Dirección debe incluir dentro de los ejes y objetivos estratégicos acciones que garanticen el cumplimiento de política y asignar los recursos adecuados, de infraestructura física, lógica y de personal con las habilidades necesarias para la gestión de la seguridad de la información.

5.1.2 Grupo de Gestión de TI

El Grupo de Gestión de TI de la Secretaría General debe actualizar y presentar ante la Alta Dirección las Políticas de Seguridad de la Información, la metodología para el análisis de riesgos de seguridad y el instructivo para la clasificación de la información, según lo considere pertinente.

El Grupo de Gestión de TI de la Secretaría General debe analizar los incidentes de seguridad que le son escalados y activar el procedimiento de contacto con las autoridades, cuando lo estime necesario.

El Grupo de Gestión de TI de la Secretaría General debe verificar el cumplimiento de las políticas de seguridad de la información aquí mencionadas.

El Grupo de gestión de TI debe liderar la generación de lineamientos para gestionar la seguridad de la información de la Gobernación del Atlántico y el establecimiento de controles técnicos, físicos y administrativos derivados de análisis de riesgos de seguridad.

El Grupo de Gestión de TI de la Secretaría General debe validar y monitorear de manera periódica la implantación de los controles de seguridad establecidos.

El Grupo de Gestión de TI de la Secretaría General debe asignar las funciones, roles y responsabilidades, a sus funcionarios para la operación y administración de la plataforma tecnológica de la Gobernación. Dichas funciones, roles y responsabilidades deben encontrarse documentadas y apropiadamente segregadas.

El Grupo de Gestión de TI de la Secretaría General debe establecer y mantener contacto permanente con grupos de interés especial relacionados con seguridad de la información o seguridad informática como los CSIRT de gobierno buscando un flujo adecuado de información relevante y actualizada que permita tomar acciones preventivas referentes a nuevas tecnologías, amenazas o vulnerabilidades; además de servir como punto de enlace en la gestión de incidentes de seguridad de la información.

5.1.3 Grupo Interno de Trabajo de Gestión Documental

El grupo interno de Gestión Documental deberá establecer dentro de Programa de gestión documental todas las medidas necesarias para salvaguardar la confidencialidad, integridad y disponibilidad de la información creada, procesada, transportada y almacenada en los documentos físicos producidos o recibidos por la entidad

En el procedimiento de Planeación Documental, se deben determinar su permanencia y medidas de seguridad en las diferentes fases del archivo y determinar cómo su disposición final no permite la recuperación de la información de forma no autorizada.

5.1.4. Secretaría de Control Interno

La Secretaría de Control Interno debe planear y ejecutar las auditorías internas al Sistema de Gestión de Seguridad de la Información, a fin de determinar si las políticas, procesos, procedimientos y controles establecidos están conformes con los requerimientos institucionales, requerimientos de seguridad y regulaciones aplicables.

La Secretaría de Control Interno debe ejecutar revisiones totales o parciales de los procesos o áreas que hacen parte del alcance del Sistema de Gestión de Seguridad de la Información, con el fin de verificar la eficacia de las acciones correctivas cuando sean identificadas no conformidades.

La Secretaría de Control Interno debe informar a las áreas responsables los hallazgos de las auditorías.

5.1.5 Comité de seguridad de la información

Actualizar anualmente las políticas de seguridad de la Información de la institución.

Coordinar las decisiones de seguridad de la información, nuevas políticas, normas, análisis de riesgos, planes de continuidad del negocio, recuperación de incidentes,

etc.

Aprobar las medidas de seguridad de la información, incluyendo planes de continuidad del negocio, análisis de riesgos, actualización de controles, normas y cambios en las políticas de seguridad.

Coordinar los esfuerzos de todos los grupos internos con responsabilidades sobre la seguridad de la información.

Aprobar los acuerdos de confidencialidad que deben realizarse con proveedores de servicios, servicios de outsourcing y demás terceros.

Coordinar todos los proyectos de mejora respecto a la seguridad de la información dentro de la organización.

Promover auditorias periódicas de seguridad de la información con el fin de identificar desviaciones y subsanarlas.

Apoyar al oficial de seguridad en la coordinación de las actividades de capacitación y sensibilización al personal de la entidad

5.1.6. Todos los Usuarios

Los funcionarios, contratistas y personal provisto por terceras partes que realice labores en o para la Gobernación del Atlántico, tienen la responsabilidad de cumplir con las políticas, normas, procedimientos y estándares referentes a la seguridad de la información.

5.2 Política de segregación de funciones

El Grupo de Gestión de TI de la Secretaría General, junto con la Secretaría de Control Interno deben determinar la separación de deberes y áreas de responsabilidad con el objetivo de separar deberes en conflicto para así evitar o al menor reducir el riesgo de que un individuo ejecute tareas potencialmente conflictivas por su cuenta.

En el proceso de desarrollo de software del Grupo de Gestión de TI se debe separar en diferentes roles las tareas de diseñar, implementar, revisar y administrar los diferentes sistemas de producción incluidas las aplicaciones de uso propietario de la entidad.

En ocasiones y después buscar implementar en la medida de lo posible la segregación, es difícil lograr la segregación total de funciones en un proceso, por lo cual se deberán

considerar otros controles mitigantes como las pistas de auditoria o seguimiento de actividades, que permitan realizar claramente trazabilidad de los participantes, líneas de tiempo, actividades, sistemas de información y cualquier otra información que se considere relevante en caso de una investigación.

5.3 Política de Inteligencia de amenazas

Con el propósito de lograr conciencia sobre el entorno de amenazas externas e internas de la entidad referentes a seguridad de la información, se hace necesario recopilar y analizar información sobre amenazas existentes o emergentes.

Por lo cual la GOBERNACIÓN DEL ATLÁNTICO establece que se realice inteligencia de amenazas estratégicas y tácticas donde se consideren aspectos que puedan afectar la seguridad de la información.

Para lo anterior deberá considerarse múltiples fuentes de información de preferencia un conjunto de fuentes internas y externas. El análisis de esta información se podrá realizar junto con el análisis de riesgos que se realice por proceso en la entidad.

El resultado del análisis se deberá comunicar en el comité de seguridad de la información o a las personas relevantes en la toma de decisiones.

5.4 Política de Clasificación, Etiquetado y Gestión de Activos de Información

La Gobernación del Atlántico como propietario y/o custodio de la información física y lógica, generada, procesada, almacenada y transmitida con su plataforma tecnológica y su archivo físico, otorgará responsabilidad a los funcionarios, contratistas y terceros autorizados, para cumplir con la misión de la organización; sobre sus activos de información, asegurando el cumplimiento de las directrices que regulen el uso adecuado de la misma.

Esta política establece los criterios con los cuales la GOBERNACIÓN DEL ATLÁNTICO identifica los activos de información y asigna valor a los mismos; de igual forma, proporciona a los funcionarios indicaciones sobre el uso apropiado de los activos de información con el propósito de proteger a la Entidad y sus activos de información.

El Grupo de Gestión de TI, en conjunto con el Grupo Interno de Trabajo de Gestión Documental de la GOBERNACIÓN DEL ATLÁNTICO, son los responsables de los procesos que permite identificar, clasificar, etiquetar, disponer, valorar y gestionar los

activos de información de acuerdo con el proceso de inventario y clasificación de activos de información y normas aplicables para la clasificación de activos de información vigentes. Por lo anterior se definen las siguientes políticas con el fin de lograr clasificar, etiquetar y gestionar los activos de la Gobernación:

- ✓ Las secretarias de la Gobernación del Atlántico deben actuar como propietarias delegadas de la información física y digital de la organización, ejerciendo así la facultad de aprobar o revocar el acceso a su información con los perfiles adecuados para tal fin.

- ✓ Los propietarios de los activos de información deben generar un inventario de dichos activos para las áreas o procesos que lideran, acogiendo las indicaciones del procedimiento de clasificación de la información; así mismo, deben mantener actualizado el inventario de sus activos de información y revisar su clasificación periódicamente a lo largo del ciclo de vida de la información.

- ✓ La clasificación deberá considerar los requisitos de confidencialidad, integridad y disponibilidad de la información, los responsables de hacer la clasificación del activo deberán ser en todo caso el propietario.

- ✓ Los propietarios de los activos de información junto con Grupo de Gestión de TI deben monitorear periódicamente la validez de los usuarios y sus perfiles de acceso a la información digital.

- ✓ Los propietarios de los activos de información deben ser conscientes que los recursos de procesamiento de información de la Gobernación del Atlántico se encuentran sujetos a auditorías por parte de la Secretaría de Control Interno y a revisiones de cumplimiento por parte del Grupo de Gestión de TI.

- ✓ El etiquetado de información física se puede hacer a través de alguna etiqueta o sello que permita visualizar fácilmente su clasificación y la información digital se puede etiquetar a través del uso del encabezado del documento y de información respecto a su clasificación en los metadatos del archivo.

- ✓ Cada secretaria debe realizar un análisis de riesgos periódico que incluya dentro de este, riesgos relacionados con seguridad de la información, sobre los procesos o áreas definidas por la Gobernación del Atlántico.

5.5 Política de Uso Aceptable y devolución de la información y otros activos

Un comportamiento esperado con respecto al uso de la información y activos de la GOBERNACION DEL ATLANTICO, de parte de propietarios encargados, funcionarios, contratistas, es el respeto y cumplimiento de toda la política de seguridad de la

información de la entidad.

Los recursos informáticos son suministrados por la GOBERNACIÓN DEL ATLÁNTICO a los funcionarios con el único fin de desarrollar las actividades relacionadas a su cargo y al contexto de la Entidad, de acuerdo a los criterios establecidos en el *Manual específico de funciones* de la Entidad, por lo cual estos recursos deben ser utilizados de forma adecuada y eficiente.

Es responsabilidad de los funcionarios, hacer buen uso del equipo de cómputo asignado, así como la conservación, integridad y contenidos de la información que se encuentran en las unidades de almacenamiento de los equipos de cómputo de escritorio y portátiles. Esto incluye las unidades extraíbles asignadas al funcionario, si fuere el caso.

El Grupo de Gestión de TI debe generar y aplicar lineamientos para la disposición segura de los medios de almacenamiento digital de la Gobernación, ya sea cuando son dados de baja o reasignados a un nuevo usuario.

Los funcionarios, contratistas y personal provisto por terceras partes son responsables por la custodia de los medios de almacenamiento institucionales asignados.

Los funcionarios, contratistas y el personal provisto por terceras partes no deben modificar la configuración de los activos digitales como sistemas de información, a menos que este explícitamente definido en el Manual de funciones.

El Grupo de Gestión de TI debe establecer la protección a copias de información, así como el marcado claro de estas copias según su clasificación, para que solo los usuarios autorizados tengan acceso a estas.

El Grupo de Gestión de TI debe definir las condiciones de uso y protección de los activos de Información digital, y el Grupo Interno de Trabajo de Gestión Documental, debe definir las condiciones de uso y protección de los activos de Información física.

El Grupo de Gestión de TI debe realizar revisiones periódicas de los recursos de la plataforma tecnológica y los sistemas de información de la Gobernación.

Los recursos tecnológicos de la Gobernación del Atlántico deben ser utilizados de forma ética y en cumplimiento de las leyes y reglamentos vigentes, con el fin de evitar daños o pérdidas sobre la operación o la imagen de la Gobernación.

El Grupo de Gestión de TI es responsable de preparar las estaciones de trabajo fijas y/o portátiles de los funcionarios y de hacer entrega de estas.

El Grupo de Gestión de TI es responsable de recibir los equipos de trabajo fijo y/o

portátil para su reasignación o disposición final, y generar copias de seguridad de la información de los funcionarios y contratistas que se retiran o cambian de labores, cuando les es formalmente solicitado.

Los recursos tecnológicos de la Gobernación del Atlántico provistos a funcionarios, contratistas y personal suministrado por terceras partes son proporcionados con el único fin de llevar a cabo las labores de la organización; por consiguiente, no deben ser utilizados para fines personales o ajenos a este.

Los funcionarios no deben utilizar equipos de cómputo y dispositivos móviles personales para desempeñar las actividades laborales.

Los funcionarios no deben utilizar software no autorizado o de su propiedad en la plataforma tecnológica de la Gobernación del Atlántico.

Para la disposición final y/o eliminación de la información se debe contar con la autorización del propietario y el visto bueno del Grupo de Gestión de TI, en caso de información digital y/o del Grupo Interno de Trabajo de Gestión Documental en caso de información impresa, siempre teniendo en cuenta el cumplimiento de las tablas de retención documental de la entidad, cuando se dé por terminado el contrato o cese la relación laboral el funcionario, contratista y/o tercero debe devolver los activos de información (equipos, documentos, datos), las llaves físicas y de cifrado. Además, el Grupo de Gestión de TI deberá eliminar los derechos de acceso a los sistemas de información donde este inscrito el usuario.

5.6 Política de Transferencia de Información

La transferencia de información es un proceso requerido en las actividades de la GOBERNACIÓN DEL ATLÁNTICO y, por lo tanto, deberá realizarse protegiendo la confidencialidad, disponibilidad e integridad de los datos de acuerdo con la clasificación del tipo de información involucrada.

5.6.1 Transferencia física de información

La transferencia física de información tanto a nivel interno y externo se debe realizar según lo establecido en la política de Gestión documental.

Usar mensajeros confiables y autorizados, verificando en todo caso su identidad

En caso de información sensible usar bolsas de embalaje a prueba de manipulaciones

5.6.2 Transferencia de información digital

La transferencia de información digital solo debe realizarse a través de los canales autorizados, los cuales deben estar configurados para garantizar la seguridad en el transporte de la información.

Solamente se podrá enviar correos electrónicos a través de la cuenta de correo institucional, haciendo uso de un lenguaje apropiado en sus comunicaciones.

En todo documento transferido se debe incluir un aviso de confidencialidad, de manejo de datos personales de acuerdo con la ley 1581 del 2012 y 1266 del 2008 de Habeas Data.

La información clasificada como crítica o sensible debe ser cifrada antes de ser transferida, tanto a nivel interno como a nivel externo.

Los funcionarios que durante el desarrollo de sus labores requieran transferir información desde sitios de trabajo remotos hacia la Gobernación deberán realizar las actividades a través de una conexión VPN.

5.6.3 Transferencia de información con terceros

Para la transferencia de información a terceros debe existir un acuerdo de transferencia de información, y el mismo deberá contener clausulas donde se establezcan las herramientas que deben ser utilizadas para asegurar la transferencia de información.

No se debe tener conversaciones verbales confidenciales en lugares públicos, ya que puede ser escuchada por personas con fines ilícitos.

Para la transferencia de información a terceros, se deben manejar acuerdos de confidencialidad, compromiso y reserva, así como el cumplimiento de la legislación vigente a nivel nacional e internacional que apliquen para el tratamiento de la información.

Los proveedores y terceros deben cumplir con las políticas de seguridad de la información, que tengan algún tipo de relación con la transferencia de información en medios físicos.

Todo correo electrónico y/o medio físico con destino a terceros que contenga información confidencial y/o reservada, debe enviar por mensajes separados y/o medios diferentes, la información protegida y las herramientas o datos necesarias para acceder o descifrar la información. En ninguna circunstancia se deben enviar junto con la información las contraseñas o claves de cifrado para poder leer el mensaje.

Los acuerdos de confidencialidad deben ser revisados periódicamente, evaluando la pertinencia de estos, con el fin de salvaguardar la confidencialidad, integridad y disponibilidad de la información.

5.7 Política de Control de Acceso

La GOBERNACIÓN DEL ATLÁNTICO define las reglas para el acceso controlado a la información, ya sea de forma física o lógica.

Los funcionarios deben portar su carne durante el ingreso y permanencia a la entidad.

El Grupo de Gestión de TI de la Secretaría General de la GOBERNACIÓN DEL ATLÁNTICO establece con respecto al acceso lógico:

- ✓ El Centro de Datos y zonas de concentración de información deben contar con tecnología de control de acceso basado en biometría y/o pin.

- ✓ El Centro de Datos y zonas de concentración de información deben contar con sistemas de videovigilancia que permitan monitorizar constantemente el flujo de personas en estas áreas.

- ✓ El Grupo de Gestión de TI debe establecer y mantener el procedimiento de gestión de acceso lógico, el cual busca proteger el acceso a las redes de datos, sistemas de información y recursos de red de la Gobernación del Atlántico.

- ✓ El Grupo de Gestión de TI debe asegurar el acceso y uso autorizado de las redes inalámbricas de la Gobernación del Atlántico haciendo uso de métodos de autenticación seguros.

- ✓ El Grupo de Gestión de TI debe verificar en el momento de la conexión y, cuando se considere pertinente, el cumplimiento de las condiciones de conexión de los equipos de cómputo y dispositivos móviles de los terceros en la red de datos de la Gobernación.

- ✓ El Grupo de Gestión de TI debe establecer controles para la identificación y autenticación de los usuarios provistos por terceras partes en las redes o recursos de red, así como velar por la aceptación de las responsabilidades de dichos terceros.

- ✓ El Grupo de Gestión de TI debe verificar periódicamente los controles de acceso para los usuarios provistos por terceras partes, con el fin de revisar que dichos usuarios tengan acceso permitido únicamente a aquellos recursos de red y servicios de la plataforma tecnológica para los que fueron autorizados.

- ✓ Los funcionarios, contratistas y personal provisto por terceras partes, antes de contar con acceso lógico por primera vez a la red de datos de la Gobernación

del Atlántico, deben contar con el registro de creación de cuentas de usuario debidamente autorizado y el Acuerdo de Confidencialidad previamente firmado. Los equipos de cómputo de usuario final que se conecten o deseen conectarse a las redes de datos de la Gobernación del Atlántico deben cumplir con una solución antimalware activa y actualizada para autenticarse en ellas y únicamente podrán realizar las tareas para las que fueron autorizados.

- ✓ El control de acceso a la información se implementa bajo el principio del mínimo privilegio que el funcionario, contratista y/o tercero requiera para el desarrollo de sus actividades diarias.

5.8 Políticas de Gestión de identidad e información de autenticación

La identidad digital solo se asigna a una persona autorizada y solo esta tiene la responsabilidad de las acciones que de su uso se realice después de asignada.

El Grupo de Gestión de TI deberá establecer un procedimiento que asegure la eliminación, reasignación o bloqueo de las identidades digitales otorgadas para el acceso a los recursos tecnológicos, los servicios de red y los sistemas de información de manera oportuna, cuando los funcionarios se desvinculan, toman licencias, vacaciones, son trasladados o cambian de cargo.

Se debe mantener un registro de todos los eventos llevados a cabo con la identidad de los usuarios y de la información de autenticación.

Los usuarios de los recursos tecnológicos y los sistemas de información de la Gobernación del Atlántico realizarán un uso adecuado y responsable de dichos recursos y sistemas, salvaguardando la información a la cual les es permitido el acceso.

Las identidades digitales como credenciales como usuario, contraseñas, tarjetas de acceso o similares no deben ser compartidas con otros funcionarios, contratistas o con personal provisto por terceras partes, para acceso a áreas restringidas de alto riesgo de robo de activos de información debe considerarse como primera opción una solución biométrica ya que esta dificulta el préstamo de la identidad a un tercero.

Los funcionarios y personal provisto por terceras partes que posean acceso a la

plataforma tecnológica, los servicios de red y los sistemas de información de la Gobernación del Atlántico deben acogerse a lineamientos presentes en las políticas de seguridad de la información de la entidad.

El Grupo de Gestión de TI deberá establecer un procedimiento formal para la administración de las identidades para redes de datos, los recursos tecnológicos y sistemas de información de la Gobernación, que contemple la creación, modificación, bloqueo o eliminación de las identidades.

El Grupo de Gestión de TI, previa solicitud de los jefes inmediatos de los solicitantes de las cuentas de usuario y aprobación de los propietarios de los sistemas de información debe crear, modificar, bloquear o eliminar cuentas de usuarios sobre las redes de datos, los recursos tecnológicos y los sistemas de información administrados, acorde con los lineamientos establecidos.

La información de autenticación predeterminada por los proveedores tecnológicos se debe cambiar inmediatamente después de la instalación del producto.

El Grupo de Gestión de TI debe definir lineamientos para la configuración de contraseñas que aplicarán sobre la plataforma tecnológica, los servicios de red y los sistemas de información de la Gobernación del Atlántico; dichos lineamientos deben considerar aspectos como longitud, complejidad, cambio periódico, control histórico, bloqueo por número de intentos fallidos en la autenticación y cambio de contraseña en el primer acceso, entre otros.

La información de autenticación que se confirme o se sospeche comprometida debe cambiarse inmediatamente después de la notificación o actividad sospechosa.

Los usuarios no deben repetir la misma contraseña para diferentes sistemas de información.

5.9 Políticas de derechos de acceso

Las Secretarías y dependencias de la administración departamental, así como los propietarios de los sistemas de información y aplicativos que apoyan los procesos y áreas que lideran, velarán por la asignación, modificación y revocación de privilegios de accesos a sus sistemas o aplicativos de manera controlada. El Grupo de Gestión de TI, como responsable de la administración de dichos sistemas de información y aplicativos, propenderá para que estos sean debidamente protegidos contra accesos no autorizados a través de mecanismos de control de acceso lógico.

Los propietarios de los activos de información deben autorizar los accesos a sus

sistemas de información o aplicativos, de acuerdo con los perfiles establecidos y las necesidades de uso, acogiendo los procedimientos establecidos y considerando la segregación de funciones.

Los propietarios de los activos de información deben monitorear periódicamente los perfiles definidos en los sistemas de información y los privilegios asignados a los usuarios que acceden a ellos.

El Grupo de Gestión de TI deberá establecer un procedimiento para la asignación, modificación y revocación de privilegios a los sistemas y aplicativos de la Gobernación, estos se deben aplicar de forma oportuna.

Se debe mantener un registro de los derechos de acceso físicos y lógicos de los usuarios.

El Grupo de Gestión de TI debe otorgar los privilegios para administración de recursos tecnológicos, servicios de red y sistemas de información sólo a aquellos funcionarios designados para dichas funciones.

El Grupo de Gestión de TI debe establecer cuentas personalizadas con altos privilegios para cada uno de los administradores de los recursos tecnológicos, servicios de red y sistemas de información.

5.10 Política de Relación con Proveedores y Gestión de proyectos

La GOBERNACIÓN DEL ATLÁNTICO periódicamente necesita contratar servicios especializados externos que den soporte a parte de su actividad. En estos casos se debe exigir a los proveedores externos, por lo menos, la misma seguridad interna para que puedan gestionar parte de la información de la Entidad. Así mismo, velará por la adecuada gestión de cambios en la prestación de servicios de dichos proveedores.

Esta política está enfocada en controlar que toda relación con proveedores, y en particular aquellos que tienen acceso a la información de la GOBERNACIÓN DEL ATLÁNTICO, está protegida con base en los acuerdos y contratos correspondientes, antes, durante y a la finalización del contrato o servicio prestado. También es deber asegurar que los productos y servicios contratados cumplen con los requisitos de seguridad informática establecidos por la Entidad.

- ✓ Los requisitos y riesgos asociados a seguridad de la información y propiedad intelectual se deben gestionar desde el comienzo del proyecto y posteriormente se monitorizan a lo largo del ciclo de vida del proyecto.

- ✓ El Grupo de Gestión de TI debe verificar las condiciones de comunicación segura, cifrado y transmisión de información desde y hacia los terceros proveedores de servicios, durante el ciclo de vida del proyecto.

- ✓ El Grupo de Gestión de TI y los Supervisores de contratos con terceros, deben monitorear periódicamente, el cumplimiento de los Acuerdos de Niveles de Servicio, Acuerdos de Confidencialidad, Acuerdos de Intercambio de información y los requisitos de Seguridad de la Información de parte de los terceros proveedores de servicios.

- ✓ Los Supervisores de contratos con terceros, con el apoyo del Grupo de Gestión de TI, deben administrar los cambios en el suministro de servicios por parte de los proveedores, manteniendo los niveles de cumplimiento de servicio y seguridad establecidos con ellos y monitoreando la aparición de nuevos riesgos.

5.11 Política para el uso de servicios en la nube

La Gobernación del Atlántico dentro de sus proveedores tecnológicos puede considerar tercerizar en la plataforma de un tercero o Proveedor de servicios en la nube, parte de su infraestructura tecnológica. Para lo anterior uno de los criterios de selección deberá ser los riesgos de seguridad de la información y la responsabilidad de cada una de las partes.

La Gobernación del Atlántico debe considerar dentro de los criterios de selección del Proveedor de servicios en la nube, la ubicación (país o región) para poder procesar y almacenar información confidencial de la entidad. Esta ubicación debe considerar requerimientos legales y de tratamiento de datos personales de ser el caso.

El Grupo de Gestión de TI deberá encomendar al personal con el conocimiento necesario para el uso y gestión del servicio en la nube

Se debe tener claro cuáles son los controles de seguridad de la información de responsabilidad del proveedor de servicios en la nube y de la Gobernación del Atlántico para cada servicio contratado. Y como podría gestionar las garantías de que el proveedor está gestionando sus responsabilidades.

En el procedimiento de gestión de incidentes de seguridad de la información, se debe considerar cuando estos ocurran en la nube.

En el acuerdo de nivel de servicio, se debe garantizar que el proveedor de servicios en la nube monitorizar, revisar y evaluar de forma constante los riesgos de seguridad de la información.

Se debe dejar claro desde el momento de la contratación las condiciones para dar de baja el servicio y la estrategia de salida a una solución privada y en sitio, para cambio de proveedor de servicios en la nube

En el Acuerdo de nivel de servicio se debe enunciar las garantías de confidencialidad, integridad y disponibilidad que pone a disposición de sus clientes el Proveedor de servicios en la nube

El Grupo de Gestión de TI debe considerar al momento de realizar las auditorias técnicas periódicas a su plataforma, incluir los servicios contratados en la nube.

Se debe implementar de protección y monitoreo de malware en servicios en la nube

El proveedor de servicios en la nube debe apoyar con información relevante en la recopilación de evidencia digital, en caso de investigaciones forenses informáticas.

Dentro de la contratación se debe considerar el manejo de las copias de seguridad correspondientes a la información de la entidad.

El proveedor de servicios en la nube debe garantizar la devolución de la información de la entidad, cuando se solicite durante la prestación del servicio o al finalizar este; en este último caso el proveedor debe garantizar el borrado seguro de la información, de manera que no se pueda recuperar posterior a la terminación de la relación comercial.

El proveedor de servicios en la nube debe proporcionar notificación previa a cambios, notificando fecha, duración y motivos de la venta de mantenimiento.

5.12 Política de Gestión de Incidentes y recopilación de pruebas

La GOBERNACIÓN DEL ATLÁNTICO adopta prácticas de gestión de incidentes de seguridad de la información con el fin de identificarlos, gestionarlos, tratarlos y mitigarlos, para de esta forma mantener la confidencialidad, integridad y disponibilidad de la información de la Entidad, cumpliendo con las directrices de las normas ISO 27001:2022 y el estándar ISO 27035 sobre gestión de incidentes de seguridad.

Entre los distintos tipos de incidentes de seguridad, se pueden destacar los siguientes:

- ✓ Incidentes no intencionados o involuntarios

- ✓ Daños físicos
- ✓ Incumplimiento o violación de requisitos y regulaciones legales
- ✓ Fallos en las configuraciones
- ✓ Denegación de servicio
- ✓ Acceso no autorizado, espionaje y robo de información
- ✓ Borrado o pérdida de información
- ✓ Infección por software malicioso.

La política de gestión de incidentes de seguridad de la información está enfocada a:

- ✓ Detectar, reportar y evaluar incidentes de seguridad de la información.
- ✓ Responder a incidentes de seguridad de la información, incluida la activación de controles adecuados para la prevención y la reducción de impactos.
- ✓ Reportar las vulnerabilidades de seguridad de la información, evaluarlas y tratarlas adecuadamente.
- ✓ Aprender de los incidentes y vulnerabilidades de seguridad de la información, implementar controles preventivos y hacer mejoras al enfoque global para la gestión de incidentes de seguridad de la información.
- ✓ Mejorar la concienciación y la formación de usuarios, para poder evitarlos junto con ellos en el futuro.

Las políticas de recopilación de pruebas están orientadas asegurar una gestión consistente de las pruebas de un incidente informático para efecto de acciones disciplinarias y/o legales.

Se tendrá un procedimiento para la identificación, recopilación, adquisición y conservación de pruebas de acuerdo con los diferentes tipos de medios de almacenamiento.

Se deberá recopilar la evidencia digital, creando imágenes forenses, tan pronto como sea posible después de la ocurrencia, cuidando de hacerlo con las herramientas adecuadas, con el personal calificado y respetando la cadena de custodia.

Asegurar que los registros están completos y que no pueden modificarse; y en caso de que se vean alterados por un tercero, poder evidenciar claramente con un mecanismo como las funciones hash, que estos fueron alterados.

5.13 Políticas de seguridad de la información durante una interrupción y preparación de las TIC para la continuidad del negocio.

La GOBERNACIÓN DEL ATLÁNTICO brinda a sus funcionarios, contratistas y/o terceros una serie de servicios tecnológicos para la realización de sus respectivas actividades laborales. Estos recursos deben ser utilizados exclusivamente para dichas actividades.

Se debe identificar las amenazas que puedan ocasionar posibles interrupciones en los procesos críticos, por ejemplo, fallas en el equipamiento, interrupción del suministro de energía eléctrica, inundación, incendio, desastres naturales, destrucción en la infraestructura física, atentados, etc.

Evaluar los riesgos para determinar el impacto de dichas interrupciones, tanto en términos de magnitud de daño como del período de recuperación. Dicha evaluación debe identificar los recursos críticos, los impactos producidos por una interrupción, los tiempos de interrupción aceptables o permitidos, y debe especificar las prioridades de recuperación.

Dentro de los recursos críticos se debe considerar los controles de seguridad de la información, por lo cual estos se deben mantener durante la interrupción y de no ser posible considerar controles compensatorios eficaces que permitan establecer medidas de control para acceso, uso, modificación y eliminación de la información.

Debido a que los servicios tecnológicos de la entidad dependen del fluido eléctrico se debe contar con un generador de respaldo y/o UPSs(Suministro de energía ininterrumpible) para los casos en que el procesamiento deba continuar ante una falla prolongada en el suministro de energía. Deberá realizarse un análisis de impacto de las posibles consecuencias ante una interrupción prolongada del procesamiento, con el objeto de definir qué componentes adicionales son necesarios abastecer de energía alternativa.

Uno de los servicios tecnológicos más importantes es el servicio de Internet, suministrado por la GOBERNACIÓN DEL ATLÁNTICO como una herramienta de apoyo a las funciones y responsabilidades de los funcionarios; por lo tanto, en caso de una interrupción de este servicio, independientemente de la causa raíz, se debe esperar que este se restablezca para poder enviar o recibir información sensible referente a la entidad. Por lo cual queda prohibido hacer uso de planes de datos personales para transmisión de información sensible de la entidad, ya que esto podría ocasionar perdidas en la confidencialidad o integridad de la información.

Todos los elementos que permitan dar redundancia deben ser probados una vez al mes para verificar su estado y su correcto funcionamiento, esto considerando diversos escenarios.

Se deberá preparar un plan de continuidad para las TIC, y sus procedimientos de respuesta y recuperación, estos deben ser aprobados por secretaria general y deben detallar como gestionar una interrupción de algún servicio TIC. Periódicamente deben ser evaluados a través de pruebas y ejercicios con el fin de revisar si cumplen con los objetivos de continuidad de negocio.

5.14 Política de derechos de propiedad intelectual

Los requisitos y riesgos asociados a seguridad de la información y propiedad intelectual se deben gestionar desde el comienzo del proyecto y posteriormente se monitorizan a lo largo del ciclo de vida del proyecto.

La propiedad intelectual y los derechos patrimoniales sobre los estudios, documentos y en general los productos resultantes de la ejecución de contratos, nombramientos u otro acuerdo contractual del GOBERNACIÓN DEL ATLÁNTICO, deberá regirse con la normatividad vigente relacionada con este tema. Debido a lo anterior, todas las bases de datos, trabajos de investigación, desarrollos, interfaces, código fuente, información y otros, creada o recopilada por el GOBERNACIÓN DEL ATLÁNTICO, es propiedad de esta, por lo cual el funcionario, contratista o tercero, no podrá disponer de ella para ningún otro fin.

Además, el funcionario, contratista o tercero deberá garantizar la confidencialidad de la información y en ningún caso deberá usar esta información para su propio beneficio. El funcionario, contratista o tercero transferirá o cederá al GOBERNACIÓN DEL ATLÁNTICO de manera escrita la totalidad de la titularidad de los derechos patrimoniales sobre el conjunto de productos de desarrollos, incluyendo las obras del intelecto y bases de datos, de manera ilimitada en el tiempo e ilimitada en el territorio. En tal sentido éstas corresponderán exclusivamente al GOBERNACIÓN DEL ATLÁNTICO para actos de reproducción, comunicación pública, distribución, traducción, adaptación, edición o cualquier otro uso o transformación en calidad de titular del derecho. El GOBERNACIÓN DEL ATLÁNTICO como titular del derecho patrimonial tendrá el control absoluto sobre las formas de utilización y en consecuencia estará facultado para autorizar o prohibir cualquier explotación sobre la información creada por esta y bajo la autorización del titular que corresponda.

5.15 Política para la Protección de Datos Personales

La GOBERNACIÓN DEL ATLÁNTICO mediante la Resolución 215 del 2019 adopta la política de tratamiento de datos personales de la gobernación del atlántico, documento que establece la forma como se recopilan, manejan y conservan los datos personales de los sujetos que la entidad en desarrollo de sus funciones constitucionales y legales requiere de su uso; y señala el procedimiento por el cual el interesado puede acudir ante la administración para solicitar el acceso, inclusión, exclusión, corrección, adición, actualización y certificación de sus datos, así como la limitación en las posibilidades de divulgación, publicación o cesión de los mismos, de conformidad con los principios que regulan el proceso de administración de datos personales que allí mismo se señalan.

Los lineamientos asociados a la protección de datos personales se encuentran definidos en el documento de *Política para la Privacidad y Protección de Datos*

Personales.

La GOBERNACIÓN DEL ATLÁNTICO cuenta, además, con una Política de privacidad y términos de uso del sitio web, la cual puede ser consultada a través del enlace: https://www.atlantico.gov.co/index.php/politica/12011-politica-de-tratamientos-de-datos-personales

5.16 Política para revisiones independientes de seguridad de la información

Se debe planificar e incluir en el presupuesto anual del Grupo de Gestión de TI, al menos una evaluación independiente al año o antes si surge un cambio sustancial en la plataforma tecnológica, después de un incidente significativo, cambios en los controles de ciberseguridad, al implementar un nuevo producto o servicio o al incluirse o modificarse el contexto reglamentario de la entidad.

La evaluación independiente debe contener una evaluación de vulnerabilidades y una prueba de penetración para los servidores privados y en sitio, en la nube, y estaciones de trabajo, buscando que las que no fueron evaluadas la ultimas vez, en la nueva evaluación se tengan en cuenta. El informe debe mostrar evidencias de los hallazgos y oportunidades de mejora.

Las personas del equipo de evaluadores deben ser personas competentes, con certificaciones internacionales en seguridad de la información e informática, con experiencia comprobada en pruebas de auditoria similares.

Los resultados de estas evaluaciones se deben informar a la dirección del Grupo de Gestión de TI y a la alta dirección si procede. Estos registros deben mantenerse y deben ejecutarse las oportunidades de mejora.

5.17 Cumplimiento de Política, normas y estándares de seguridad de la información

La GOBERNACIÓN DEL ATLÁNTICO garantiza el cumplimiento de las obligaciones legales, regulatorias o contractuales relacionadas con seguridad de la información, y de cualquier requisito de seguridad.

Los requerimientos legales, regulatorios y contractuales vigentes y aplicables para la Entidad en relación con la Seguridad de la Información serán parte integral del normograma de la entidad.

El normograma relacionado con seguridad de la información debe ser anualmente o antes de surgir un cambio sustancial en la legislación aplicable a la entidad; el oficial de seguridad de la información será el encargado junto con el área jurídica de constatar tal cambio.

6 POLITICAS RELACIONADAS CON LOS CONTROLES DE PERSONAS

6.1 Política de verificación de antecedentes

La información sobre candidatos que recibe la gobernación o alguno de sus aliados para contratación y nombramientos, debe recopilarse y manejarse teniendo en cuenta la legislación pertinente.

Se debe realizar un proceso de selección para todo el personal de la entidad. Cuando estas personas sean contratadas a través de proveedores de servicios, los requisitos de selección deben incluirse en los acuerdos contractuales entre la entidad y los proveedores.

La verificación debe tener en cuenta toda la legislación vigente sobre privacidad, y se debe procurar que la entidad o a través del proveedor realice verificación de antecedentes, confirmación de las calificaciones académicas y profesionales, verificación de antecedentes en Procuraduría, Contraloría, policía y demás que se consideren pertinentes.

6.2 Política de condiciones y responsabilidades durante y a la terminación del empleo

Los acuerdos contractuales de empleo de la entidad deben establecer responsabilidades del personal en cuanto a la seguridad de la información, dentro de estos acuerdos encontramos:

Acuerdo de confidencialidad o de no divulgación para todo el personal de la entidad a la cual se les de acceso a información confidencial, este debe ser firmado antes del acceso a esta información. Este debe mantenerse validos incluso si ya el funcionario o contratista ha terminado su relación contractual con la GOBERNACIÓN DEL ATLANTICO.

Se debe determinar dentro del contrato o nombramiento su responsabilidad con respecto al cumplimiento de las políticas de seguridad de la información y la clasificación y gestión de la información, además de su responsabilidad de

información recibida por terceros.

Los acuerdos anteriores deben revisarse anualmente o antes en caso de modificarse las leyes, reglamentos o la presente política. Esta responsabilidad es compartida entre el comité de Seguridad de la Información y el líder de los procesos de contratación y recursos humanos.

6.3 Política de concientización, educación y capacitación en seguridad

Las políticas de concientización, educación y entrenamiento, buscan que los funcionarios y contratistas de la Gobernación del Atlántico conozcan e interioricen las políticas de seguridad de la información de la entidad, esto mediante actividades, talleres, charlas, volantes, vídeos, emails y cualquier otra forma de comunicación, que permita dar a conocer la información asociada a la privacidad y protección de la seguridad de la información que van a crear, transmitir, transformar, y consultar para la ejecución de su trabajo.

La entidad deberá poseer un plan de concientización, educación y capacitación la cual debe ser liderada por el comité de seguridad de la información de la Gobernación del Atlántico, todas estas se deben establecer desde el marco de referencia que son las presentes políticas de seguridad de la información y se debe revisar anualmente evaluando su estado de cumplimiento y efectividad.

6.4 Política de proceso disciplinario

Se inicia un proceso disciplinario al verificarse una violación de cualquiera de las políticas de seguridad de la información, esta debe liderarse por el proceso de quejas y control disciplinario de la entidad, siguiendo sus procedimientos para este tema.

Dentro del proceso disciplinario debe considerarse factores como: gravedad del incumplimiento y sus consecuencias, si e delito fue malicioso o accidental, si se trata de primera vez o es reiterativo, si el infractor fue capacitado o no. Para todos los efectos legales se tendrá en cuenta la legislación pertinente.

Contra las decisiones que se den en los procesos disciplinarios proceden los recursos de reposición, apelación y queja, los cuales se interpondrán por escrito, salvo disposición expresa en contrario.

6.5 Política de acuerdos de confidencialidad o no divulgación

Funcionarios, contratistas y terceros se obligan a no divulgar la información confidencial a la cual tendrá acceso con ocasión de su nombramiento o contrato con la entidad, incluida su etapa precontractual, salvo cuando reserva se extiende hasta después de terminado el contrato y subsistirá mientras la información tenga las características por ser considerada secreta. De igual manera ambas partes reconocen y aceptan que podrán tener acceso a información que puede tener ideas y conceptos originales, secretos comerciales y otros elementos que no son de dominio público y son considerados confidenciales, o de propiedad restringida, o que podrá ser comunicada entre las partes de forma oral, la cual se identificará como información confidencial en el momento en que se expone. En consecuencia, las partes se comprometen a:

- ✓ No revelar o circular la información contenida en documentos digitales o físicos, ni a discutir dicha información con personas que hacen parte de las instituciones.

- ✓ No utilizar esa información con personas que no forman parte de la entidad.
- ✓ Las partes tampoco podrán dar a terceros información de carácter técnico o administrativo confidencial con personas naturales o jurídicas distinta de aquellas que laboren por alguna de las partes o que no tuvieren autorización para recibir información.

6.6 Política de Teletrabajo y Trabajo en Casa

La Entidad bajo el decreto 508 de 2022 “Por medio de la cual se adopta el Teletrabajo Suplementario como una forma de organización laboral en la Gobernación del Atlántico". La presente política complementa las directrices establecidas en el decreto en mención, en lo concerniente a los aspectos de Seguridad de la Información aplicables dentro del desarrollo del Teletrabajo y trabajo en casa a los funcionarios asignados.

Dentro del documento “Acuerdo de Trabajo”, se consignan las obligaciones de la GOBERNACIÓN DEL ATLÁNTICO y las obligaciones generales de los teletrabajadores, bajo la modalidad de teletrabajo, las cuales con su aceptación se darán entendidas como de obligatorio cumplimiento.

Debido a esto, la GOBERNACIÓN DEL ATLÁNTICO amplía la política para incluir dentro de las políticas de seguridad de la información, las actividades asociadas al trabajo en casa.

Es obligación del funcionario atender las instrucciones respecto de uso y apropiación de tecnologías de la información y las comunicaciones, así como respecto de seguridad digital, efectuadas por la GOBERNACIÓN DEL ATLÁNTICO.

El funcionario debe restituir cuando aplique, los equipos y herramientas de trabajo entregados por la entidad para el desempeño de sus labores, en el estado en que fueron recibidos, salvo el deterioro por el uso normal de los mismos.

La GOBERNACIÓN DEL ATLÁNTICO consultando la disponibilidad al interior de la entidad, suministrará las herramientas de trabajo para la realización del teletrabajo, tales como equipos de cómputo, software y repositorios virtuales y programas requeridos para el desarrollo de la labor contratada. En todo caso, el teletrabajador asumirá la obligación del cuidado y uso correcto de las herramientas, siendo responsable único del uso indebido de los mismos. En todo caso las partes de mutuo acuerdo, podrán acordar que el funcionario ponga a disposición de la GOBERNACIÓN DEL ATLÁNTICO sus propios equipos y herramientas de trabajo, caso en el cual, el teletrabajador se obliga a mantener en buenas condiciones funcionales para atender los requerimientos propios del servicio.
Para el desarrollo del artículo 6° de la Ley 1221 de 2008, una vez seleccionado el funcionario o grupo de funcionarios participantes en la modalidad de teletrabajo, se debe incluir en el expediente de hoja de vida, debidamente diligenciado el documento de Compromiso debidamente firmado por el servidor de adoptar las políticas de seguridad de la información y aquellas que se adopten relacionadas con la modalidad de Teletrabajo para el desarrollo de la actividad laboral en el lugar de residencia.

6.7 Reporte de eventos de seguridad de la información

Todos los funcionarios y contratistas tienen el deber de reportar posibles incidentes de seguridad de la información o sospechas de estos, lo antes posible buscando minimizar o evitar los riesgos asociados a una posible explotación.
Los eventos de seguridad incluyen vulnerabilidades, incidentes y/o violaciones. Como, por ejemplo:
Errores humanos, incumplimientos de las políticas de seguridad de la información, malos funcionamientos que afecten la seguridad de la información, infracciones de acceso físico o lógico a instalaciones donde se procese información de la entidad, vulnerabilidades, sospechas de infección por malware, emails sospechosos, entre otros.
En los anteriores escenarios, el funcionario o contratista deberá reportar inmediatamente al oficial de seguridad de la información de la entidad, quien deberá dejar un registro en el formato designado para el reporte de incidentes, dejando constancia de la persona que reporta, como detectó el incidente, hora, lugar, entre otros datos relevantes.
Es importante saber que los usuarios, sean funcionarios o contratistas no deben

probar las vulnerabilidades por si mismos. Ya que lo anterior puede impactar negativamente a la entidad y puede interpretarse como un mal uso del sistema, además de dificultar la tarea de recolección de evidencia digital, lo que pudiera resultar en una responsabilidad legal de la persona que realiza la prueba.

7 POLITICAS DE CONTROLES FISICOS

7.1 Perímetro de seguridad y entrada físicas

La Gobernación del Atlántico proveerá la implantación y velará por la efectividad de los mecanismos de seguridad física y control de acceso que aseguren el perímetro de sus instalaciones en todas sus sedes. Así mismo, controlará las amenazas físicas externas e internas y las condiciones medioambientales de sus oficinas.

Todas las áreas destinadas al procesamiento o almacenamiento de información sensible, así como aquellas en las que se encuentren los equipos y demás infraestructura de soporte a los sistemas de información y comunicaciones, se consideras áreas de acceso restringido.

Los funcionarios y contratistas deben portar el carné que los identifica como tales en un lugar visible mientras se encuentren en las instalaciones de la Gobernación del Atlántico; en caso de pérdida del carné o tarjeta de acceso a las instalaciones, deben reportarlo a la mayor brevedad posible.

Aquellos funcionarios o personal provisto por terceras partes para los que aplique, debido al servicio prestado, deben utilizar prendas distintivas que faciliten su identificación.

Los funcionarios, contratistas y el personal provisto por terceras partes no deben intentar ingresar a áreas a las cuales no tengan autorización.

7.2 Políticas de aseguramiento de oficinas, salas e instalaciones

Los secretarios y jefes de oficina que se encuentren en áreas restringidas deben velar mediante por la efectividad de los controles de acceso físico y equipos de vigilancia.

Los secretarios y jefes de oficina que se encuentren en áreas restringidas deben autorizar cualquier ingreso temporal a sus áreas, evaluando la pertinencia del ingreso; así mismo, deben delegar en personal del área el registro y supervisión de cada ingreso.

Los secretarios y jefes de oficina deben velar porque las contraseñas de sistemas de alarma, cajas fuertes, llaves y otros mecanismos de seguridad de acceso a sus áreas solo sean utilizados por personal autorizado y, salvo situaciones de emergencia u otro tipo de eventos que por su naturaleza lo requieran, estos no sean transferidos a otros funcionarios de la Gobernación.

7.3 Políticas de supervisión de la seguridad física

La Secretaría General debe proporcionar los recursos necesarios para ayudar a proteger, regular y velar por el perfecto estado de los controles físicos implantados en las instalaciones.

La Secretaría General debe identificar mejoras a los mecanismos implantados y, de ser necesario, la implementación de nuevos mecanismos, con el fin de proveer la seguridad física de las instalaciones de la Gobernación.

La Secretaría General debe almacenar y custodiar los registros del sistema de control de acceso a las instalaciones de la Gobernación.

La Secretaría General debe certificar la efectividad de los mecanismos de seguridad física y control de acceso al centro de cómputo, centros de cableado y demás áreas de procesamiento de información.

La Secretaría de Control Interno tiene la responsabilidad de incluir dentro del plan anual de auditorías la verificación aleatoria a los equipos de cómputo de todas las dependencias la Gobernación.

7.4 Protección contra amenaza físicas y ambientales

La Secretaría General debe proveer las condiciones físicas y medioambientales necesarias para certificar la protección y correcta operación de los recursos de la plataforma tecnológica ubicados en el centro de cómputo; deben existir sistemas de control ambiental de temperatura y humedad, sistemas de detección y extinción de incendios, sistemas de descarga eléctrica, sistemas de vigilancia y monitoreo y alarmas en caso de detectarse condiciones ambientales inapropiadas. Estos sistemas se deben monitorear de manera permanente.

La Secretaría General debe velar porque los recursos de la plataforma tecnológica de la Gobernación ubicados en el centro de cómputo se encuentran protegidos contra fallas o interrupciones eléctricas.

El Grupo de Gestión de TI debe certificar que el centro de cómputo y los centros de cableado que están bajo su custodia, se encuentren separados de áreas que tengan líquidos inflamables o que corran riesgo de inundaciones e incendios.

El Grupo de Gestión de TI debe asegurar que las labores de mantenimiento de redes de voz y de datos, sean realizadas por personal idóneo y apropiadamente autorizado e identificado; así mismo, se debe llevar control de la programación de los mantenimientos preventivos.

7.5 Políticas para trabajar en áreas seguras

Las solicitudes de acceso al centro de cómputo o a los centros de cableado deben ser aprobadas por personal del Grupo de Gestión de TI autorizado; no obstante, los visitantes siempre deberán estar acompañados de un funcionario de dicha secretaría durante su visita al centro de cómputo o los centros de cableado.

El Grupo de Gestión de TI debe registrar el ingreso de los visitantes al centro de cómputo y a los centros de cableado que están bajo su custodia, en una bitácora ubicada en la entrada de estos lugares de forma visible.

El Grupo de Gestión de TI debe descontinuar o modificar de manera inmediata los privilegios de acceso físico al centro de cómputo y los centros de cableado que están bajo su custodia, en los eventos de desvinculación o cambio en las labores de personal autorizado.

El Grupo de Gestión de TI debe aislar los equipos de áreas sensibles, en busca de proteger su acceso de los demás funcionarios de la red de la Gobernación.

7.6 Política de Escritorio despejado y Pantalla Despejada

La política de escritorio limpio conlleva la obligación de guardar la documentación de trabajo al ausentarse del puesto de trabajo y al terminar la jornada laboral. Por esta razón no se debe dejar información sensible a la vista de personas que pudieran hacer uso indebido de la misma. El cumplimiento de esta política conlleva, entre otras actividades, a mantener el puesto de trabajo limpio y ordenado, guardar la documentación y los dispositivos extraíbles que no están siendo usados en el momento o al estar ausentes del puesto o al fin de la jornada laboral y a no apuntar nombres de usuarios ni contraseñas en ningún documento.

Los funcionarios, contratistas y el personal provisto por terceras partes deben bloquear sus estaciones de trabajo en el momento de abandonar su puesto de trabajo.

Los equipos de cómputo, en ninguna circunstancia, deben ser dejados desatendidos en lugares públicos o a la vista, en el caso de que estén siendo transportados.

Los funcionarios, contratistas y el personal provisto por terceras partes deben asegurar que sus escritorios se encuentran libres de los documentos que son utilizados durante el desarrollo de sus funciones al terminar la jornada laboral y, que estos sean almacenados bajo las protecciones de seguridad necesarias.

Para la seguridad de las impresoras, el personal asignado por el Grupo de Gestión de TI verificará que las impresoras conectadas a la red de la Entidad cumplan con las siguientes indicaciones:

- ✓ Se encuentren conectadas en los segmentos de red institucionales correspondientes.
- ✓ El acceso a su panel de configuración debe ser mediante contraseña y por canales cifrados.
- ✓ Si están conectadas por WIFI se debe configurar su seguridad y cifrado.
- ✓ Los discos duros de las impresoras deben revisarse periódicamente.
- ✓ Los puertos USB de las impresoras no deben estar habilitados.
- ✓ Siempre que sea posible, se debe disponer de mecanismos de impresión segura (con contraseña).
- ✓ El usuario debe recoger inmediatamente aquellos documentos enviados a imprimir. No se deben dejar documentos en la impresora al finalizar el día de trabajo o al receso de almuerzo.

7.7 Políticas de ubicación y protección de los equipos

El Grupo de Gestión de TI es la única área autorizada para realizar movimientos y asignaciones de recursos tecnológicos; por consiguiente, se encuentra prohibida la disposición que pueda hacer cualquier funcionario de los recursos tecnológicos de la Gobernación.

Las estaciones de trabajo, dispositivos móviles y demás recursos tecnológicos asignados a los funcionarios, contratistas y personal provisto por terceras partes deben acoger las instrucciones técnicas de proporcione el Grupo de Gestión de TI.

La instalación, reparación o retiro de cualquier componente de hardware o

software de las estaciones de trabajo, dispositivos móviles y demás recursos tecnológicos, solo puede ser realizado por personal del Grupo de Gestión de TI, o personal de terceras partes autorizado por dicha dirección.
Los funcionarios, contratistas y el personal provisto por terceras partes no deben dejar encendidas las estaciones de trabajo u otros recursos tecnológicos en horas no laborables.

7.8 Políticas de seguridad para los activos y medios fuera de las instalaciones

El Grupo de Gestión de TI debe proveer los mecanismos y estrategias necesarios para proteger la confidencialidad, integridad y disponibilidad de los recursos tecnológicos, dentro y fuera de las instalaciones de la Gobernación del Atlántico.

Los equipos de cómputo deben ser transportados con las medidas de seguridad apropiadas, que garanticen su integridad física.

En caso de pérdida o robo de un equipo de cómputo de la Gobernación, se debe informar de forma inmediata al jefe directo para que se inicie el trámite interno y se debe poner la denuncia ante la autoridad competente.

7.9 Políticas de utilidades de apoyo energético

Las estaciones de trabajo deben estar conectadas a una red eléctrica aterrizada y regulada para evitar posibles daños ante circunstancia de daños eléctricos internos o del operador.

En el caso de activos digitales de vital importancia como por ejemplo los cámaras de vigilancia, servidores y equipos de red, deben estar conectados a una UPS y/o generador eléctrico alterno a la alimentación eléctrica principal.

Todos los equipos de apoyo energético alterno deben ser mantenidos según las especificaciones del fabricante e inspeccionados para verificar su correcto funcionamiento.

En caso de interrupción de la energía eléctrica se debe asegurar la iluminación correcta para mantener el perímetro de las instalaciones física seguro.

7.10 Políticas de seguridad en el cableado

Se debe asegurar que las instalaciones de cableado de red, debe ser en la medida de lo posible subterránea o en escalerillas o conductos elevados de difícil

acceso, minimizando riesgos de interrupciones deliberadas o accidentales.

Se debe procurar que los cables de alimentación eléctrica estén separados del cableado de red para evitar interferencias.

Se debe realizar una inspección visual al subsistema de cableado de datos para detectar posibles dispositivos no autorizados conectados a tomas de red, patchpanels, o equipos activos de red.

Se debe etiquetar en cada extremo el origen y el destino del cableado para permitir la localización de posibles fallas físicas.

7.11 Política de mantenimiento de equipos y eliminación segura de equipos

Se debe realizar mantenimientos preventivos y correctivos de los recursos de la plataforma tecnológica, incluidas UPS, generadores de energía, sistemas de alarma, extintores, aires acondicionados y ascensores.

Para lo anterior se debe elaborar un plan de mantenimientos que detalle la periodicidad, las tareas y responsables. Con respecto a la periodicidad dependerá de las recomendaciones del fabricante.

Solo el personal designado por el Grupo de Gestión de TI tiene la autorización para realizar los mantenimientos preventivos y correctivos de la tecnología de la entidad.

Se debe mantener el registro de los mantenimientos realizados y de posibles fallas que fuesen detectadas y reparadas.

Está prohibido que los equipos tecnológicos de la entidad que sean utilizados fuera de las instalaciones sean reparados por terceros no autorizados.

El Grupo de Gestión de TI debe generar y aplicar lineamientos para la disposición segura de los equipos de cómputo de los funcionarios y contratistas, ya sea cuando son dados de baja o cuando cambian de usuario.
Los medios de almacenamiento que contienen o contuvieron información sensible confidencial o personal debe destruirse de forma física buscando que sea imposible recuperar con herramientas de software esta información.

8 POLITICAS DE CONTROLES TECNOLOGICOS

8.1 Política de dispositivos finales de usuario y dispositivos móviles

El Grupo de Gestión de TI debe proveer los mecanismos y estrategias necesarios para proteger la confidencialidad, integridad y disponibilidad de los recursos tecnológicos, dentro y fuera de las instalaciones de la Gobernación del Atlántico.

El Grupo de Gestión de TI debe generar estándares de configuración segura para los equipos de cómputo y posteriormente configurar dichos equipos acogiendo los estándares generados.

El Grupo de Gestión de TI debe establecer las condiciones que deben cumplir los equipos de cómputo de personal provisto por terceros, que requieran conectarse a la red de datos de la Gobernación y verificar el cumplimiento de dichas condiciones antes de conceder a estos equipos acceso a los servicios de red.

El Grupo de Gestión de TI debe aislar los equipos de áreas sensibles, en busca de proteger su acceso de los demás funcionarios de la red de la Gobernación.

Las estaciones de trabajo, dispositivos móviles y demás recursos tecnológicos asignados a los funcionarios, contratistas y personal provisto por terceras partes deben acoger las instrucciones técnicas de proporcione del Grupo de Gestión de TI.

La instalación, reparación o retiro de cualquier componente de hardware o software de las estaciones de trabajo, dispositivos móviles y demás recursos tecnológicos, solo puede ser realizado por personal del Grupo de Gestión de TI, o personal de terceras partes autorizado por dicha dirección.

El Grupo de Gestión de TI debe contar con una opción de borrado remoto de información en los dispositivos móviles institucionales, con el fin de eliminar los datos de dichos dispositivos y restaurarlos a los valores de fábrica, de forma remota, evitando así divulgación no autorizada de información en caso de pérdida o hurto.

El Grupo de Gestión de TI debe contar con una solución de copias de seguridad para la información contenida en los dispositivos móviles institucionales.

Los funcionarios, contratistas y el personal provisto por terceras partes deben bloquear sus estaciones de trabajo en el momento de abandonar su puesto de trabajo y cancelar los servicios tecnológicos cuando ya no se requieran.

Los funcionarios, contratistas y el personal provisto por terceras partes no deben dejar encendidas las estaciones de trabajo u otros recursos tecnológicos en horas no laborables.

Está prohibido el uso de dispositivos personales para acceder a información sensible o personal en custodia de la entidad.

La GOBERNACIÓN DEL ATLÁNTICO proporciona las condiciones adecuadas para el manejo de los dispositivos móviles (computadores portátiles, tabletas y teléfonos inteligentes) institucionales y personales que hagan uso de los servicios de la Entidad. Así mismo, vela porque los funcionarios hagan un uso responsable de los servicios, equipos y aplicativos disponibles en la Entidad.

Se autorizará acceso a la plataforma de tecnologías y sistemas de información a proveedores de servicios, que por la naturaleza de sus actividades requieran acceder a estos servicios en forma periódica, previa solicitud enviada al jefe o al líder del área de Infraestructura del Grupo de Gestión de TI, por el interventor del contrato o profesional responsable de las actividades del contratista o proveedor de servicios.

El Grupo de Gestión de TI, es responsable de gestionar la implementación y el cumplimiento de la presente política, así como de su revisión periódica, actualización, difusión, concientización y capacitación para su adecuado cumplimiento.

La sincronización de la cuenta de correo electrónico corporativo en el dispositivo móvil de uso institucional debe ser configurada por los profesionales designados por el Grupo de Gestión de TI de la Entidad.

Para la sincronización de la cuenta de correo electrónico corporativo en el dispositivo móvil de uso personal debe realizarse una solicitud a través de comunicación remitida al jefe o al líder del área de Infraestructura del Grupo de Gestión de TI, previa autorización del jefe directo del usuario que lo requiere.

Los dispositivos móviles personales podrán unirse temporalmente a la red de datos de la GOBERNACIÓN DEL ATLÁNTICO, de forma inalámbrica o cableada, obteniendo la configuración por defecto que los equipos de redes y seguridad tengan determinada. Para el ajuste en los niveles de navegación o la aprobación de acceso a aplicativos, debe realizarse una solicitud a través de comunicación remitida al jefe o al líder del área de Infraestructura del Grupo de Gestión de TI, previa autorización del Jefe directo del usuario que lo requiere.

8.2 Políticas de derechos de acceso privilegiado

El Grupo de Gestión de TI es el responsable de asignar y revocar derechos de acceso privilegiado a los usuarios según sea necesario y caso por caso de acuerdo con la política sobre control de acceso y basado en el mínimo privilegio basado en su rol.

El Grupo de Gestión de TI debe otorgar los privilegios para administración de recursos tecnológicos, servicios de red y sistemas de información sólo a aquellos funcionarios designados para dichas funciones y por el tiempo necesario para realizar la tarea.

El Grupo de Gestión de TI debe restringir las conexiones remotas a los recursos de la plataforma tecnológica.

El Grupo de Gestión de TI debe asegurarse que los usuarios o perfiles de usuario que traen por defecto los sistemas operativos, el firmware y las bases de datos sean suspendidos o renombrados en sus autorizaciones y que las contraseñas que traen por defecto dichos usuarios o perfiles sean modificadas.

El Grupo de Gestión de TI debe establecer los controles para que los usuarios finales de los recursos tecnológicos, los servicios de red y los sistemas de información no tengan instalados en sus equipos de cómputo utilitarios que permitan accesos privilegiados a dichos recursos, servicios o sistemas.

Se debe registrar todos los accesos privilegiados a los sistemas con fines de auditoría y verificar que si estos por sus deberes, roles, responsabilidades y competencias aun los califican para trabajar con derechos de acceso privilegiado.

Está prohibido compartir o vincular identidades con derechos de acceso privilegiado a múltiples personas, asignando a cada persona una identidad separada que permita asignar derechos de acceso privilegiado específicos.

8.3 Políticas sobre la restricción de derechos de información

El Grupo de Gestión de TI y el grupo interno de trabajo de gestión documental, debe ser responsable de no permitir el acceso a información sensible por la parte de usuarios con identidades desconocidas o de forma anónima. El acceso público o anónimo solo otorgarse a lugares de almacenamiento que no contengan

información confidencial.

El Grupo de Gestión de TI debe proporcionar mecanismos de configuración para controlar el acceso a la información en sistemas, aplicaciones y servicios.

El Grupo de Gestión de TI debe controlar que identidades o grupo de identidades tienen que acceso, como lectura, escritura, eliminación y ejecución en los sistemas informáticos o aplicaciones.

El Grupo de Gestión de TI o terceras partes, según corresponda, deben brindar mecanismos de configuración para controlar el acceso a la información en sistemas, aplicaciones y servicios, permitiendo un control granular de quien pudo acceder y a que datos pudo acceder.

El Grupo de Gestión de TI debe procurar tener controles sobre el privilegio de impresión de los archivos de la entidad en las impresoras que hacen parte de su plataforma tecnológica, dejando el registro que permita saber que, quien y cuando se realizó la impresión del archivo.

8.4 Política del Ciclo de desarrollo seguro de software

La GOBERNACIÓN DEL ATLÁNTICO establece e implementa un conjunto de lineamientos y controles para garantizar la Seguridad de la Información durante todo el ciclo de vida de los desarrollos realizados por terceros o al interior de la Entidad a los sistemas de información.

Para la GOBERNACIÓN DEL ATLÁNTICO es importante asegurar la confidencialidad, disponibilidad, integridad y no repudio de la información que se encuentra almacenada en los diferentes sistemas de información, por esta razón se considera que para todas las fases del ciclo de vida de desarrollo de software se deben incluir requisitos de seguridad, y estos deben ser obligatorios, con el fin de minimizar vulnerabilidades que podrían aparecer en caso de no implementar planes de seguridad al desarrollo realizado.

En todas las fases del ciclo de vida de desarrollo de software los desarrolladores y terceros deben tener en cuenta los siguientes numerales, con respecto a la adquisición o desarrollo seguro de software.

8.4.1 Arquitectura de software segura

Se deben diseñar, implementar y operar sistemas de información que consideren requisitos de ingeniería y seguridad desde su inicio hasta el fin de vida útil del sistema de información, por lo cual se deben incluir puntos de chequeo de seguridad dentro de las fases del ciclo de vida de desarrollo de software.

Se debe procurar el uso de principios de arquitectura de seguridad, tales como: “seguridad por diseño”, “defensa en profundidad”,” seguridad por defecto”,” denegación predeterminada”,” fallo seguro”, “desconfianza de la entrada de aplicaciones”,” seguridad en la implementación”,” asumir incumplimiento” y ”privilegio mínimo”.

8.4.2 Desarrollo subcontratado

Los principios de ingeniería de seguridad establecidos deben aplicarse, cuando corresponda, al desarrollo subcontratado de sistemas de información a través de contratos u otros acuerdos vinculantes entre la entidad y el proveedor. La entidad desde el Grupo de Gestión de TI debe garantizar que las prácticas de ingeniería de seguridad de los proveedores se alineen con las necesidades de la entidad y que quede en el contrato claridad sobre acuerdos de licencia, propiedad del código y derechos de propiedad intelectual relacionados con el contenido subcontratado.

En lo posible el proveedor debe suministrar los resultados de las pruebas donde se han evaluado los niveles mínimos aceptables de confidencialidad, integridad, disponibilidad, protección de código malicioso y capacidades de privacidad.

A través del contrato con el proveedor se debe dejar habilitada a la entidad el derecho contractual a auditar procesos y controles de desarrollo, de la aplicación contratada por la GOBERNACIÓN DEL ATLANTICO.

8.4.3 Requisitos de seguridad de la información

- ✓ Se deben identificar, justificar, acordar y documentar los requisitos de seguridad en todas las fases del ciclo de vida de desarrollo de software.
- ✓ Se deben incluir requisitos de autenticación, segregación de acceso, en

función a la clasificación de la información.

- ✓ Se debe considerar requisitos legales, estatutarios y reglamentarios de donde se genera, procesa y almacena la información. Dentro de estos requisitos se debe considerar la privacidad de la información reservada o personal.

- ✓ Dentro de los requisitos se debe considerar el cifrado de la información sensible en tránsito y en reposo, como por ejemplo credenciales de usuario.

- ✓ Se deben considerar controles que permitan sanitizar los datos de entrada a las aplicaciones, para minimizar riesgos de ataques de inyección de código.

- ✓ Se deben filtrar los mensajes de error de las aplicaciones, contenedores y servidores, para que no informen nombres de servicios, puertos lógicos, versiones de productos o cualquier otra información que facilite la búsqueda de vulnerabilidades conocidas.

8.4.4 Codificación

Las presentes son las políticas que ha dispuesto la Gobernación de Atlántico antes, durante o después de la codificación de software por parte del Grupo de Gestión de TI.

Antes de la codificación:

La planificación y los requisitos previos antes de la codificación deben considerar lo siguiente:

- ✓ Prácticas y defectos de codificación comunes e históricos de vulnerabilidades de seguridad de la información, para no integrarlos a los nuevos desarrollos, para esto se debe consultar la base de datos CWE - Common Weakness Enumeration de Mitre.

- ✓ Instalar la última versión estable y licenciada las herramientas de desarrollo, como entornos de desarrollo integrados (IDE), compiladores, etc.

- ✓ diseño y arquitectura segura del sistema de información, incluido el modelado de amenazas;

- ✓ uso de ambientes controlados para el desarrollo

Durante la codificación:

Las consideraciones durante la codificación deben incluir:

- ✓ prácticas de codificación seguras específicas para lenguajes de programación y técnicas que se utilizan, para esto se debe consultar la base de datos CWE - Common Weakness Enumeration de Mitre.
- ✓ utilizar técnicas de programación seguras, como programación en pares, revisión por pares, utilizar técnicas de programación estructurada y desarrollo basado en pruebas;
- ✓ documentar el código y eliminar los defectos de programación, la documentación debe ser tanto para otros desarrolladores como para el usuario final.
- ✓ prohibir el uso de técnicas de diseño inseguras (por ejemplo, el uso de contraseñas codificadas, implementación de código no aprobados y servicios web no autenticados).

Después de la codificación:

- ✓ Las actualizaciones deben empaquetar e implementarse de forma segura;
- ✓ se deben manejar las vulnerabilidades de seguridad de la información informadas en las auditorias técnicas.
- ✓ los errores y los ataques sospechosos deben registrarse y los registros deben revisarse periódicamente para hacer los ajustes necesarios al código;
- ✓ el código fuente debe protegerse contra el acceso no autorizado y manipulación con controles de acceso, manejo de perfiles y permisos, cifrados o cualquier otro que el Grupo de Gestión de TI considere conveniente.
- ✓ garantizar que las bibliotecas externas se gestionen manteniendo un inventario de las bibliotecas utilizadas y sus versiones, estas deben actualizarse periódicamente.
- ✓ Debe haber un proceso de selección, autorización y reutilización de

componentes de software para examinarlos a nivel de seguridad, en particular componentes de autentificación y criptográficos;

8.4.5 Acceso al código fuente

El acceso de escritura al código fuente solo debe estar disponible para personal privilegiado o propietarios designados por el Grupo de Gestión de TI.

Cuando los componentes del código son utilizados por varios desarrolladores dentro de la entidad, se debe implementar el acceso de lectura a un repositorio de código centralizado, otorgando acceso de lectura y escritura al código fuente en función de las necesidades para minimizar los riesgos de alteración o uso indebido.

Para proceder a actualizar el código fuente y elementos anexos a este debe seguirse el procedimiento de control de cambios y realizar el cambio solo después de haber recibido la autorización correspondiente.

No se debe otorgar a los desarrolladores acceso directo al repositorio del Código fuente, sino a través de herramientas para desarrolladores que controlan las actividades y autorizaciones en el Código fuente, buscando que se deje siempre rastros de auditoría de todos los accesos y cambios al código fuente.

8.4.6 Pruebas de seguridad

Las pruebas de seguridad deben realizarse frente al conjunto de requisitos funcionales o no funcionales de seguridad. Las pruebas de seguridad deben incluir pruebas de:

Autenticación de usuario, restricciones de acceso y el uso de la criptografía para información en tránsito y en reposo.

Se deben realizar pruebas de seguridad de aplicaciones estáticas (SAST), las cuales permitirán identificar vulnerabilidades de seguridad en el código fuente del software, antes de lanzarlo a producción. Para los desarrollos internos, estas pruebas deben ser realizadas inicialmente por el equipo de desarrollo. Luego se debe realizar pruebas de aceptación independientes para garantizar que el sistema funcione como se espera.

Se debe buscar una configuración segura por defecto, incluido el de las aplicaciones, sistemas operativos, cortafuegos y otros componentes de terceros.

Se debe elaborar un plan de prueba deben determinarse utilizando un conjunto de

criterios de seguridad. El alcance de las pruebas debe ser proporcional a la importancia, la naturaleza del sistema y el impacto potencial del cambio que se está introduciendo.

Las pruebas deben realizarse en un entorno de prueba que coincida lo más posible con el entorno de producción de destino de la entidad para garantizarse que las pruebas sean confiables.

8.4.7 Separación de entornos de desarrollo, prueba y producción

El cambio de versionamiento en el ambiente de producción debe contar con controles de seguridad, para esto se debe hacer una copia de respaldo en caso de que se deba dar marcha atrás, para mantener la integridad de los datos y de los sistemas de información.

Se deben realizar pruebas de seguridad en el ambiente de pruebas, con el fin de identificar vulnerabilidades, las cuales deben ser resueltas antes del paso a producción.

Los ambientes de desarrollo, pruebas, capacitación y producción deben estar separados.

Los usuarios y/o terceros que están involucrados en esta instancia, deben utilizar perfiles diferentes en el ambiente de desarrollo, pruebas y producción; además, asegurar que cada usuario cuente únicamente con los privilegios necesarios en cada ambiente.

El ambiente de prueba debe simular el ambiente de producción. Sin embargo, los datos de prueba utilizados, a pesar de corresponder a una estructura similar a la de producción, deben utilizarse traslapados, para garantizar la seguridad y protección de los datos.

En caso de requerirse hacer copia de la información del ambiente de producción al ambiente de pruebas, se podrá realizar únicamente si la información se encuentra enmascarada o anonimizada, con el fin de que no se llegue a comprometer la confidencialidad.

8.5 Políticas de autenticación segura

La información de autenticación debe ir acompañada de factores de autentificación adicionales para acceder a los sistemas de información crítica.

La información de autentificación biométrica debe invalidarse si alguna vez se ve comprometida. Hay que considerar que la autentificación biométrica puede no estar disponible según las condiciones de uso por lo cual debe ir acompañada de al menos una técnica de autenticación alternativa.

No se debe proporcionar mensajes de ayuda durante el procedimiento de inicio de sesión que ayuden a un usuario no autorizado, no se debe indicar que parte de los datos es correcta o incorrecta.

Se debe restringir los intentos fallidos para minimizar el riesgo de intentos de inicio de sesión de fuerza bruta en nombres de usuario y contraseñas además se debe aplicar una prueba de CAPTCHA, para permitir identificar robots de software.

Se debe requerir el restablecimiento de la contraseña después de un número predefinido de intentos fallidos o bloquear al usuario después de un número máximo de errores.

Se debe finalizar sesiones inactivas después de un periodo definido de inactividad.

8.6 Políticas de Gestión de la capacidad

Se debe tener un plan de gestión de capacidad anual documentado para los sistemas de misión crítica, con el fin de prever la capacidad suficiente en caso de aumento de capacidad o por el contrario en caso de disminución de demanda para hacer uso efectivo de los recursos.

Los responsables de la administración de cada sistema de información deben establecer controles de detección para indicar los problemas de no capacidad, debido tiempo. Además de generar proyecciones de los futuros requisitos de capacidad de procesamiento de información de la entidad para cada sistema de información.

En los mantenimientos preventivos de las estaciones de trabajo se puede aprovechar para con ayuda del propietario de la información lograr realizar alguna

de estas tareas:

- ✓ Eliminación de datos obsoletos para liberar espacio en disco
- ✓ Eliminación de registros impresos que tienen su periodo de retención para liberar espacio en estanterías o gavetas.

8.7 Política de Control de Malware

La GOBERNACIÓN DEL ATLÁNTICO dispone de forma permanente de una plataforma antimalware con la cual se facilita la detección de amenazas basadas en software malicioso que puedan afectar los activos de información de la Entidad.

El Grupo de Gestión de TI de la Secretaría General de la GOBERNACIÓN DEL ATLÁNTICO es responsable de determinar qué tipo de solución es la más conveniente para la Entidad, seleccionando la más apropiada de entre las disponibles en el mercado, considerando los activos informáticos, servicios actuales, compatibilidad con la infraestructura y la versatilidad de la plataforma.

El Grupo de Gestión de TI de la GOBERNACIÓN DEL ATLÁNTICO es responsable de instalar el sistema antimalware en cada dispositivo de cómputo y en los servidores; debe utilizarse únicamente este software licenciado para la revisión y verificación de malware en los equipos y archivos, y los funcionarios no deben desactivar, alterar o desinstalar el aplicativo instalado para este fin. Grupo de gestión de TI debe garantizar que los funcionarios no puedan realizar ninguna de las actividades indicadas.

El Grupo de Gestión de TI de la GOBERNACIÓN DEL ATLÁNTICO debe garantizar la actualización permanente de la plataforma antimalware con el fin de replicar en los equipos de la Entidad las últimas firmas de búsqueda y contención de programas maliciosos.

Es responsabilidad de cada usuario utilizar el aplicativo antimalware instalado en su equipo para diagnosticar la presencia de malware en la información que provenga de diferentes medios, tales como páginas de internet, correos electrónicos, memorias USB, discos portátiles, etc. Este proceso debe ser realizado antes de abrir o ejecutar los archivos, con el fin de no propagar software malicioso al interior de la red.

Todos los medios de almacenamiento externos suministrados por un tercero deben ser revisados por el antimalware de la entidad antes que estos sean

utilizados en los equipos de cómputo de la Entidad.

Cada usuario será responsable por cualquier afectación no deseada que provoque al abrir un enlace o un archivo contaminado con software malicioso, si dicho archivo no fuese escaneado previamente con el software antimalware instalado en su equipo.

En caso de que se presente una infección por ejecución de malware, el funcionario debe informar al personal encargado responsable del Grupo de Gestión de TI, los cuales deberán realizar por lo menos las siguientes acciones:

- ✓ Desconexión y aislamiento del equipo afectado
- ✓ Desinfección de los archivos, y en caso de que no sea posible, la eliminación de estos
- ✓ Reinstalación del software o aplicativos afectados
- ✓ Registro formal del incidente en la herramienta dispuesta para tal fin.

Al recibir un correo con un archivo o un enlace adjunto, este se debe analizar cuidadosamente antes de abrirlo. Aunque el remitente sea conocido puede haber sido suplantado y esta condición no se percibe con facilidad. La descarga de archivos adjuntos maliciosos o abrir links presentes en los mensajes, podría hacer que se infecten los equipos con algún tipo de malware. Siempre se deben vacunar los archivos descargados con el antivirus de la Entidad, procurando que éste se encuentre activo y actualizado.

8.8 Políticas de gestión de vulnerabilidades técnicas

El responsable de seguridad de la información de la entidad es el encargado de la gestión técnica de las vulnerabilidades, incluido procedimientos, monitoreo de vulnerabilidades, la evaluación de riesgos de vulnerabilidades, la actualización, el seguimiento de activos y cualquier responsabilidad de coordinación requerida para el ciclo de vida de la vulnerabilidad.

Se debe realizar al menos una vez al año la identificación de vulnerabilidades técnicas relevantes para lo anterior se debe asegurar tener actualizada la lista de recursos de información de la entidad.

En los acuerdos con los proveedores tecnológicos incluidos los operadores de servicios en la nube, se debe exigir que garanticen la notificación, el manejo y la divulgación oportuna de vulnerabilidades de sus productos y/o servicios.

Se debe contratar con un tercero una vez al año, pruebas de penetración a activos digitales críticos, estas deben ser planificadas, documentadas y repetibles por parte de personas competentes que permitan evaluar el nivel de riesgo y

facilidad de explotación desde vectores externos e internos de cualquier posible actor malicioso, con el fin de subsanar posibles brechas que puedan ser aprovechadas por terceros.

Se deben utilizar únicamente actualizaciones de fuentes legítimas, estas se deben probar y evaluar antes de instalarlas para garantizar que sean efectivas y no produzcan efectos secundarios adversos. Posteriormente se debe realizar las pruebas necesarias para verificar la efectividad del control o controles implementados.

El Grupo de Gestión de TI debe revisar periódicamente la aparición de nuevas vulnerabilidades técnicas y reportarlas a los administradores de la plataforma tecnológica y los desarrolladores de los sistemas de información, con el fin de prevenir la exposición al riesgo de estos.

Para todos los casos el encargado debe mantener un registro de auditoria para todos los pasos realizados en la gestión de vulnerabilidades técnicas.

8.9 Políticas de gestión de la configuración segura

El Grupo de Gestión de TI debe definir plantillas estándar para la configuración segura de hardware, software, servicios y redes. Para lo anterior se pueden seguir lineamientos del mismo fabricante o del CIS (Center for Internet Security)

Las plantillas deben revisarse periódicamente y actualizarse cuando será necesario abordar nuevas amenazas o vulnerabilidades detectadas en la entidad o cuando se introduzcan nuevas versiones de software o hardware.

Las configuraciones establecidas de hardware, software, servicios y redes deben registrase y debe mantenerse un registro de todos los cambios de configuración. Estos registros deben almacenarse de forma segura.

Las configuraciones deben monitorearse y deben revisarse periódicamente para verificar los ajustes de configuración; las configuraciones reales se pueden comparar con las plantillas de destino definidas. Cualquier desviación debe abordarse siguiendo las acciones correctivas, que se consideren pertinentes.

8.10 Políticas de eliminación de información

La información confidencial no debe conservarse más tiempo del necesario, para reducir el riesgo de divulgación no deseada por lo que se debe procurar auditar su periodo de retención.
Al eliminar información sobre sistemas, aplicaciones y servicio, se debe considerar lo siguiente:

Al eliminar la información se debe procurar dejar registros de la evidencia de los resultados de la eliminación.

Si se contrata a un proveedor de servicios de eliminación de información, obtener evidencia de la eliminación de información de ellos y deben certificar la eliminación y método usado para posteriores consultas.

Cuando la entidad contrate a terceros para que almacenen la información confidencial o sensible se debe procurar incluir en los acuerdos contractuales la inclusión de requisitos sobre la eliminación de información para hacerlos cumplir durante y después de la finalización de dichos servicios.

Cada propietario de la información debe procurar eliminar versiones obsoletas, copias y archivos temporales donde quiera que se encuentren, para este último caso con el acompañamiento del Grupo de Gestión de TI.

Se debe en la medida de lo posible, en especial para información sensible o confidencial, usar un software de eliminación seguro y aprobado para eliminar información de forma permanente para ayudar a garantizar que la información no se pueda recuperar mediante el uso de herramientas forenses o de recuperación especializadas.

8.11 Políticas de enmascaramiento y prevención de fuga de información

Se debe enmascarar información sensible, confidencial o personal, no se debe otorgar a todos los usuarios, y a todos los datos, por lo tanto, se deben diseñar consultas y máscaras para mostrar solo los datos mínimos requeridos al usuario que consulta y permitidos por el titular de la información.

Se debe identificar y monitorizar posibles vías de escape de información y de acuerdo a la clasificación de la información aplicar controles para protegerla contra fugas.

Se debe bloquear las acciones de los usuarios o las trasmisiones de la red que

expongan información confidencial como es el caso del uso del correo electrónico.

La toma de capturas de pantalla o fotografías con el uso de dispositivos móviles de la pantalla debe abordarse a través de los términos contractuales con funcionarios y contratistas, además de ser tema en el plan de capacitaciones.

El responsable de realizar la copia de seguridad de los datos debe tener cuidado para garantizar que la información confidencial este protegida mediante medidas como el cifrado, el control de acceso y protección física de los medios de almacenamiento que contienen la copia de seguridad.

También se debe considerar dentro del plan de capacitaciones el tema de ingeniería social y la prevención de fuga de datos para protegerse contra las acciones de inteligencia de obtener información confidencial o secreta.

8.12 Políticas de copias de seguridad de la información

La GOBERNACIÓN DEL ATLÁNTICO adoptará prácticas de Copias de Respaldo o Backup para garantizar la disponibilidad de la información y la continuidad de las operaciones de la entidad.

La GOBERNACIÓN DEL ATLÁNTICO debe contar con procedimientos de Copias de Respaldo o Backup y procedimientos de restauración de los datos, para mantener la integridad y disponibilidad de la información y de los servicios de procesamiento de esta.

El Grupo de Gestión de TI debe disponer de los recursos necesarios para permitir la identificación de los medios de almacenamiento, la información contenida en ellos y la ubicación física de los mismos para permitir un rápido y eficiente acceso a los medios que contienen la información resguardada.

El Grupo de Gestión de TI, a través de sus funcionarios y contratistas, debe llevar a cabo los procedimientos para realizar la copia y luego realizar las pruebas de recuperación a la copia de respaldo, para así comprobar su integridad y posibilidad de uso en caso de ser necesario.

Una de las copias de seguridad debe realizarse en una ubicación remota segura y protegida, a una distancia suficiente para escapar de cualquier daño de un desastre en el sitio principal.

El Grupo de Gestión de TI debe definir las condiciones de transporte o transmisión y custodia de las copias de respaldo de la información que son almacenadas externamente. Para información sensible, privada o personal esta copia debe

almacenarse cifrada.

El Grupo de Gestión de TI debe proporcionar apoyo para la definición de las estrategias de generación, retención y rotación de las copias de respaldo a los activos información de la Gobernación del Atlántico.

Es responsabilidad de los usuarios de la plataforma tecnológica identificar la información crítica que debe ser respaldada y almacenarla de acuerdo con su nivel de clasificación

8.13 Políticas de redundancia en las instalaciones de procesamiento de información

El Grupo de Gestión de TI debe analizar y establecer los requerimientos de redundancia para los sistemas de información críticos para la Gobernación del Atlántico y la plataforma tecnológica que los apoya.

El Grupo de Gestión de TI debe evaluar y probar los componentes redundantes y las instalaciones de procedimiento de información, para garantizar el mismo nivel de seguridad que los principales.

Se debe contratar con dos proveedores de internet para garantizar la disponibilidad de servicios de procesamiento de información críticos, debe probarse la conmutación de estos con regularidad, para asegurar que funcione según lo previsto y de acuerdo con los requerimientos de disponibilidad de la Gobernación del Atlántico.

En cuanto al suministro eléctrico se debe procurar usar fuentes o fuentes de alimentación físicamente redundantes, para todos los componentes tecnológicos que soporten procesos críticos.

8.14 Políticas de registro, actividades de seguimiento y sincronización de reloj

Los registros que generan los sistemas operativos y aplicaciones de uso de la Gobernación del Atlántico deben concentrase, protegerse y monitorizarse con el objetivo de tener estadísticas de errores, eventos y posibles incidentes que se hayan o se estén presentando en la plataforma tecnológica de la entidad.

Los usuarios, incluidos aquellos con derechos de acceso privilegiados, no deben tener permiso para eliminar o desactivar registros de sus propias actividades por lo cual estos deben estar en modo solo lectura, solo en caso de vencimiento de su tiempo de retención se podrá realizar el debido procedimiento de eliminación de información.

Se debe utilizar un monitoreo continuo a través de una herramienta de monitoreo o a través de un servicio contratado de SOC(Security Operation Center), que permita el monitoreo en tiempo real de los servicios críticos de la entidad. Este debe ser capaz de notificar en tiempo real actividades sospechosas sobre los activos críticos monitorizados.

El personal del Grupo de Gestión de TI debe dedicarse a responder las alertas y debe estar debidamente capacitado para interpretar con precisión los posibles incidentes en caso de no subsanarse la vulnerabilidad o no bloquearse al origen generadora de la alerta.

Los informes del SOC deben comunicarse a las partes relevantes para mejorar las siguientes actividades: auditoria, evaluación de seguridad, exploración y monitoreo de vulnerabilidades.

Debe utilizarse el protocolo de tiempo de red(NTP) en todos los sistemas en red, esto permitirá sincronizarse con un reloj de referencia y facilitará la correlación de eventos en actividades de seguimiento o en posible investigaciones forenses informáticas.

8.15 Políticas de instalación de software y de programas de utilidad privilegiados

La instalación de sistemas operativos y actualizaciones de software solo le corresponde hacerla al personal del Grupo de Gestión de TI autorizados para la realización de esta tarea.

A través de controles como servidores de autenticación y autorización el Grupo de Gestión de TI debe garantizar que solo se instale código ejecutable aprobado en los sistemas operativos.

En cuanto a la instalación de software este solo se puede colocar en producción luego de pruebas extensas y exitosas.

Se debe mantener un registro de auditoría de todas las actualizaciones del software operativo.

Se debe limitar el uso de programas de utilidad al número mínimo práctico de usuarios autorizados de confianza del Grupo de Gestión de TI.

Una vez usado el programa de utilidad se debe eliminar o deshabilitar todos los programas de utilidad innecesarios.

Se debe dejar registro de todos los usos de los programas de utilidad.

8.16 Políticas de seguridad de redes, servicios de red y segregación

El Grupo de Gestión de TI debe mantener la documentación actualizada, incluidos los diagramas de red y los archivos de configuración de los dispositivos de red.

El Grupo de Gestión de TI debe establecer controles para salvaguardar la confidencialidad e integridad de los datos que pasan por redes públicas, redes de terceros o redes inalámbricas para proteger los sistemas y aplicaciones conectados, como es el uso de redes privadas virtuales o VPNs.

Se deben deshabilitar protocolos de red vulnerables en dispositivos finales de usuario y en equipos de red.

Los canales oficiales de la GOBERNACIÓN DEL ATLÁNTICO se mantendrán habilitados para su consulta y divulgación. En caso de observarse altas mediciones en el ancho de banda institucional, el Grupo de Gestión de TI, podrá restringir su acceso hasta tanto se normalice el servicio.

Es función del Grupo de Gestión de TI, el control del tráfico de internet en los equipos institucionales, mediante los dispositivos de seguridad perimetral. Este tráfico podrá ser registrado y eventualmente revisado con el fin de determinar los accesos no permitidos y establecer las acciones correctivas a que haya lugar.

La revocación del servicio institucional de Internet es una medida de prevención contra el uso no permitido o mal uso y que puedan afectar los niveles de servicio o atentar contra los principios y valores institucionales.

El jefe o superior inmediato será informado sobre el mal uso que se le está dando al servicio de Internet por los funcionarios de su área.

En caso de comprobarse el reiterado uso indebido del servicio de internet, se pueden revocar al funcionario los permisos de navegación asignados.

La GOBERNACIÓN DEL ATLÁNTICO brinda a sus funcionarios, contratistas y/o terceros una serie de servicios tecnológicos para la realización de sus respectivas actividades laborales. Estos recursos deben ser utilizados exclusivamente para dichas actividades.

El servicio de correo electrónico institucional es una herramienta de apoyo a las funciones y responsabilidades de los funcionarios de la GOBERNACIÓN DEL ATLÁNTICO y en tal virtud, sin perjuicio de la responsabilidad penal, administrativa o disciplinaria a que haya lugar, su uso debe sujetarse a las directrices en el presente documento.

La GOBERNACIÓN DEL ATLÁNTICO tiene instalada en su infraestructura de seguridad perimetral un filtro antispam que permite que los correos maliciosos sean identificados y no lleguen a la bandeja de entrada de los funcionarios evitando así su posible apertura. Sin embargo, en algunas ocasiones existen correos maliciosos que se filtran en la bandeja del correo institucional y probablemente contienen malware, buscan infectar los equipos o sustraer información personal solicitando los datos de los funcionarios en alguna página fraudulenta. Por lo cual los usuarios deben estar pendientes de correos sospechosos, estos no se deben abrir y se debe notificar al encargado de seguridad informática de la entidad para su revisión.

La organización debe asegurarse de que los proveedores de servicios de red y/o internet implementen medidas de seguridad**.** El derecho a la auditoria debe acordarse entre la entidad y el proveedor.

La entidad debe segregar o separar las redes de la entidad en función de los niveles de confianza, criticidad y sensibilidad. La segregación se puede realizar usando redes físicamente diferentes usando diferentes subredes IP, uso de Virtual LANs y/o dominios en servidores de autenticación y autorización.

Las redes inalámbricas requieren un tratamiento especial, deben estar segregadas las redes inalámbricas para invitados de las del personal de la entidad y esta última debe cumplir con las políticas específicas de seguridad para su uso. La red wifi para invitados debe tener al menos las mismas restricciones que la red wifi para el personal, a fin de desalentar el uso de WiFi de invitados por parte del personal de la entidad.

8.17 Políticas de filtrado web

El Grupo de Gestión de TI está habilitado para limitar el acceso a determinadas sitios web en Internet, establecer los horarios de conexión, supervisar los servicios ofrecidos por la red, autorizar la descarga de archivos y verificar cualquier otra

petición relacionada con la navegación para el cumplimiento de los fines institucionales.

Está prohibido para todos los usuarios finales la navegación sobre sitios web inseguros como los que usan el protocolo HTTP, sitios web maliciosos conocidos o sospechosos, sitios web que comparten contenido ilegal, sitios de descarga de software, sitios para uso de proxies o VPNs, sitios de contenido sexual, y en general sitios que no tengan relación con la actividad para el cual fue contratado.

8.18 Política de Uso de Criptografía

La Información clasificada como pública reservada o pública clasificada debe ser cifrada siguiendo los lineamientos definidos de la presente política

Para establecer el sistema de cifrado, se tiene en la cuenta la normatividad colombiana vigente frente a la protección de los datos, estándares aplicables y la tecnología existente.

Los propietarios de los activos individuales sobre los cuales se aplican controles criptográficos son los responsables por la correcta aplicación de los controles criptográficos particulares.

Las llaves criptográficas se deben proteger contra pérdida, modificación, destrucción no autorizada y divulgación.

El respaldo de información confidencial debe protegerse por medio de cifrado.

8.19 Política de Gestión de cambios

Para la adicción de nuevos sistemas de información, software o actualizaciones en los sistemas existentes de la GOBERNACIÓN DEL ATLANTICO deben seguirse las políticas y procedimientos formales establecidos para los cambios, pruebas, control de calidad e implementación suministrada por el Grupo de Gestión de TI.

Dentro del Grupo de Gestión de TI deben existir responsabilidades de gestores de cambio para garantizar un control satisfactorio de todos los cambios.

Los procedimientos de control de cambios deben documentarse y aplicarse para garantizar la confidencialidad, integridad y disponibilidad de la información en las instalaciones y los sistemas de información de la entidad, durante todo el ciclo de vida del desarrollo del sistema de información.

8.20 Política de protección de los sistemas de información durante pruebas de auditoria

En los acuerdos con proveedores de auditorías externas se debe considerar acordar solicitudes formales de auditoria para el acceso a sistemas y datos con la gestión adecuada, estas solicitudes se debe determinar claramente el alcance de las pruebas.

Las pruebas de auditoría interna y externa deben realizarse con acceso de solo lectura al software y los datos. En caso de querer realizarse pruebas de verificación de controles de integridad, puede acordase habilitar por un tiempo limitado el acceso a los sistemas a evaluar.

Se debe supervisar y registrar todos los accesos con fines de auditoría y prueba. Al igual que se debe guardar como información documentada los informes finales de cada auditoria protegiéndolos de consulta, modificación o eliminación no autorizada.

9 REFERENCIAS

Los conceptos especificados en los términos y condiciones fueron tomados de las siguientes referencias:

1. Modelo de Seguridad y Privacidad de la Información – MinTIC, https://www.mintic.gov.co/gestionti/615/articles5482_Modelo_de_Seguridad_Privacidad.pdf
2. Norma Técnica Colombiana NTC-ISO/IEC 27000:2018, NTC-ISO/IEC 27001:2022, NTC-ISO/IEC 27002:2022, ISO /IEC 27032:2012
3. Glosario MinTIC, https://www.mintic.gov.co/portal/inicio/Glosario/
4. Ley 1712 de 2014
5. Ley 1581 de 2012
6.https://www.ccn-cert.cni.es/publico/seriesCCN-STIC/series/400Guias_Generales/401-Glosario_y_abreviaturas/topics/201.html
7. Articulo- Dispositivos móviles de la Universidad de Oviedo, http://isa.uniovi.es/docencia/SIGC/pdf/telefonia_movil.pdf
8. Guía de Implementación de Seguridad de la Información MIPYME - MinTIC, https://www.mintic.gov.co/gestionti/615/articles 5482_Guia_Seguridad_informacion_Mypimes.pdf
9. Ley 1221 de 2008
10. Circular 021 de 2020 MinTrabajo

11. Decreto 1377 de 2013
12. Decreto 1413 de 2017
13.https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_glosario_ciberseguridad_2021.pdf