Gobernación del Atlántico

ATLÁNTICO LÍDER

ATLÁNTICO LÍDER

Gobernación del Atlántico

SECRETARÍA TIC

UNIDOS POR UN ATLÁNTICO LÍDER EN TECNOLOGÍA

ATLÁNTICO LÍDER

Gobernación del Atlántico

SECRETARÍA TIC

POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

CONTENIDO

Control de Cambios

Versión	Fecha	Descripción	Autor
1.0	Diciembre 30 de 2002	Versión inicial	Secretaría de Informática
2.0	Junio 30 de 2016	Reestructuración de la forma para cumplir con estándares nacionales	Secretaría de Informática
3.0	Julio 30 de 2018	Ajustado a la Norma	Secretaría de Tecnologías

INTRODUCCIÓN

La Gobernación del Atlántico conoce que la información es un componente indispensable para lograr sus objetivos estratégicos, por lo cual es necesario establecer un marco en el cual se asegure que la información es protegida de una manera adecuada independientemente de la forma en la que ésta sea manejada, procesada, transportada o almacenada.

Este documento describe las políticas y normas de seguridad de la información definidas por la Gobernación del Atlántico, las cuales se constituyen como parte fundamental para la gestión de la seguridad de la información y serán la base principal para la implantación de los controles, procedimientos y estándares.

OBJETIVO

El objetivo de este documento es establecer las políticas en seguridad de la información de la Gobernación del Atlántico, con el fin de regular la gestión de la seguridad de la información al interior de la Entidad.

ALCANCE

Las políticas de seguridad de la información cubren todos los aspectos que deben ser acatados por directivos, funcionarios, contratistas y terceros que laboren o tengan relación con la Gobernación del Atlántico, en busca de mantener la confidencialidad, integridad y disponibilidad de la información.

1. POLÍTICA GLOBAL DE SEGURIDAD DE LA INFORMACIÓN

Para la Gobernación del Atlántico la información es un activo fundamental para la prestación de sus servicios y la toma de decisiones, razón por la cual existe un compromiso de protección como parte de una estrategia orientada a la gestión de riesgos y la consolidación de una cultura de seguridad. Consciente de las necesidades actuales, la Gobernación del Atlántico implementa lineamientos para la gestión de seguridad de la información como la herramienta para identificar y minimizar los riesgos a los cuales se expone la información, redundando en establecer una cultura de seguridad y velando por el cumplimiento de los requerimientos legales, regulatorios y de negocio vigentes.

Los funcionarios, contratistas, personal externo, proveedores y todos aquellos que tengan responsabilidades sobre las fuentes, repositorios y recursos de procesamiento de la información de la Gobernación del Atlántico, deben adoptar los lineamientos contenidos en el presente documento y en los documentos relacionados con él, en busca de preservar la confidencialidad, la integridad y disponibilidad de la información.

La política global de seguridad de la Información se encuentra soportada por políticas, normas y procedimientos específicos los cuales guiarán el manejo adecuado de la información de la Gobernación del Atlántico. Las políticas específicas de seguridad de la información se fundamentan en los dominios y objetivos de control del anexo A de la norma internacional ISO 27001:2013.

2. COMPROMISO DE LA DIRECCIÓN

El Gobernador como muestra de su apoyo a la seguridad de la información, demuestra su compromiso a través de:

- La revisión y aprobación de las Políticas de Seguridad de la Información contenidas en este documento.
- La provisión de los recursos necesarios para implementar y mantener las políticas de seguridad de la información
- La promoción activa de una cultura de seguridad.
- Proveer los mecanismos para la divulgación de este documento a todas las partes interesadas de la Gobernación.
- La verificación del cumplimiento de las políticas aquí mencionadas.

3. SANCIONES PARA LAS VIOLACIONES A LAS POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

Las Políticas de Seguridad de la Información pretenden instituir y afianzar la cultura de seguridad de la información entre los funcionarios, contratistas, personal externo y proveedores; por lo cual, es necesario que como producto de violaciones a las Políticas Seguridad de la Información sean tomadas medidas correctivas conforme a la clase de contravención. Las medidas correctivas pueden considerar desde acciones administrativas, hasta acciones de orden disciplinario o penal, de acuerdo con las circunstancias, si así lo ameritan.

4. POLÍTICAS DE LA ORGANIZACIÓN DE SEGURIDAD DE LA INFORMACIÓN

4.1. POLÍTICA DE ESTRUCTURA ORGANIZACIONAL 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.

4.1.1. NORMAS

4.1.1.1. Alta Dirección

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

- La Alta Dirección debe definir y establecer el procedimiento de contacto con las autoridades en caso de ser requerido, así como los responsables 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 promover activamente una cultura de 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 asignar los recursos, la infraestructura física y el personal necesario

para la gestión de la seguridad de la información.

4.1.1.2. Secretaría de Tecnologías de la Información y las Comunicaciones - TIC

- La Secretaría de Tecnologías de la Información y las Comunicaciones, en adelante Secretaría de TIC, 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.

- La Secretaría de TIC debe analizar los incidentes de seguridad que le son escalados y activar el procedimiento de contacto con las autoridades, cuando lo estime necesario.

- La Secretaría de TIC debe verificar el cumplimiento de las políticas de seguridad de la información aquí mencionadas.

- La Secretaría de TIC 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.

- La Secretaría de TIC debe validar y monitorear de manera periódica la implantación de los controles de seguridad establecidos.

- La Secretaría de TIC 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

4.1.1.3. 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.

4.1.1.4. 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.

4.2. POLÍTICA PARA USO DE DISPOSITIVOS MÓVILES

La Gobernación del Atlántico proveerá las condiciones para el manejo de los dispositivos móviles (teléfonos, inteligentes y tabletas, entre otros) institucionales y personales que hagan uso de servicios de la Gobernación. Así mismo, velará porque los funcionarios y contratistas hagan un uso responsable de los servicios y equipos proporcionados.

4.2.1. NORMAS

4.2.1.1. Secretaría de TIC

- La Secretaría de TIC debe investigar y probar las opciones de protección de los dispositivos móviles institucionales y personales que hagan uso de los servicios provistos por la Gobernación.

- La Secretaría de TIC debe establecer las configuraciones aceptables para los dispositivos móviles institucionales o personales que hagan uso de los servicios provistos por la Gobernación.

- La Secretaría de TIC 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.

- La Secretaría de TIC debe contar con una solución de copias de seguridad para la información contenida en los dispositivos móviles institucionales.

4.2.1.2. Todos los Usuarios

- Los usuarios deben evitar usar los dispositivos móviles institucionales en lugares que no les

ofrezcan las garantías de seguridad física necesarias para evitar pérdida o robo de estos.

- Los usuarios no deben modificar las configuraciones de seguridad de los dispositivos móviles institucionales bajo su responsabilidad, ni desinstalar el software provisto con ellos al momento de su entrega.

- Los usuarios deben evitar la instalación de programas desde fuentes desconocidas; se deben instalar aplicaciones únicamente desde los repositorios oficiales de los dispositivos móviles institucionales.

- Los usuarios deben, cada vez que el sistema de sus dispositivos móviles institucionales notifique de una actualización disponible, aceptar y aplicar la nueva versión.

- Los usuarios deben evitar hacer uso de redes inalámbricas de uso público, así como deben desactivar las redes inalámbricas como WIFI, Bluetooth, o infrarrojos en los dispositivos móviles institucionales asignados.

- Los usuarios deben evitar conectar los dispositivos móviles institucionales asignados por puerto USB a cualquier computador público, de hoteles o cafés internet, entre otros.

- Los usuarios no deben almacenar videos, fotografías o información personal en los dispositivos móviles institucionales asignados.

4.3. POLÍTICA PARA USO DE CONEXIONES REMOTAS

La Gobernación del Atlántico establecerá las circunstancias y requisitos para el establecimiento de conexiones remotas a la plataforma tecnológica; así mismo, suministrará las herramientas y controles necesarios para que dichas conexiones se realicen de manera segura.

4.3.1. NORMAS

4.3.1.1. Secretaría de TIC

- La Secretaría de TIC debe analizar y aprobar los métodos de conexión remota a la plataforma tecnológica de la Gobernación.

- La Secretaría de TIC debe implantar los métodos y controles de seguridad para establecer conexiones remotas hacia la plataforma tecnológica.

- La Secretaría de TIC debe restringir las conexiones remotas a los recursos de la plataforma tecnológica; únicamente se deben permitir estos accesos a personal autorizado y por periodos de tiempo establecidos, de acuerdo con las labores desempeñadas.

4.3.1.2. Todos los Usuarios

- Los usuarios que realizan conexión remota deben contar con las aprobaciones requeridas para establecer dicha conexión a los dispositivos de la plataforma tecnológica de la Gobernación del Atlántico y deben acatar las condiciones de uso establecidas para dichas conexiones.

- Los usuarios únicamente deben establecer conexiones remotas en computadores previamente identificados y, bajo ninguna circunstancia, en computadores público, de hoteles o cafés internet, entre otros.

5. POLÍTICAS DE SEGURIDAD DEL PERSONAL

5.1. POLÍTICA RELACIONADA CON LA VINCULACIÓN DE FUNCIONARIOS, CONTRATISTAS Y PERSONAL PROVISTO POR TERCEROS

La Gobernación del Atlántico reconoce la importancia que tiene el factor humano para el cumplimiento de sus objetivos y con el interés de contar con el personal mejor calificado, garantizará que la vinculación de nuevos funcionarios se realizara siguiendo un proceso formal de selección, acorde con la legislación vigente, el cual estará orientado a las funciones y roles que deben desempeñar los funcionarios en sus cargos.

5.1.1. NORMAS

5.1.1.1. Secretaría General

- La Secretaría General debe velar porque los funcionarios, contratistas y personal provisto por terceras partes firmen un Acuerdo y/o Cláusula de Confidencialidad y un documento de aceptación de políticas de seguridad de la información; estos documentos deben ser anexados a los demás documentos relacionados con la ocupación del cargo.

5.2. POLÍTICA APLICABLE DURANTE LA VINCULACIÓN DE FUNCIONARIOS, CONTRATISTAS Y PERSONAL PROVISTO POR TERCEROS

La Gobernación del Atlántico en su interés por proteger su información y los recursos de

procesamiento de la misma demostrará el compromiso de la Alta Dirección en este esfuerzo, promoviendo que el personal cuente con el nivel deseado de conciencia en seguridad de la información para la correcta gestión de los activos de información y ejecutando el proceso disciplinario necesario cuando se incumplan las Políticas de seguridad de la información.

Todos los funcionarios, contratistas y personal provisto por terceros que desarrolle actividades en la Gobernación del Atlántico debe ser cuidadoso de no divulgar información confidencial en lugares públicos, en conversaciones o situaciones que pongan en riesgo la seguridad y el buen nombre de la Gobernación.

5.2.1. NORMAS

5.2.1.1. Alta Dirección

- La Alta Dirección debe demostrar su compromiso con la seguridad de la información por medio de su aprobación de las políticas, normas y demás lineamientos que desee establecer la Gobernación del Atlántico.

- La Alta Dirección debe promover la importancia de la seguridad de la información entre los funcionarios, contratistas y el personal provisto por terceras partes, así como motivar el entendimiento, la toma de conciencia y el cumplimiento de las políticas, normas, procedimientos y estándares para la seguridad de la información establecidos.

- La Alta Dirección debe definir y establecer el proceso disciplinario o incluir en el proceso disciplinario existente, el tratamiento de las faltas de cumplimiento a las políticas de seguridad o los incidentes de seguridad que lo ameriten.

5.2.1.2. Secretaría de TIC

- La Secretaría de TIC debe diseñar y ejecutar de manera permanente un programa de concienciación en seguridad de la información, con el objetivo de apoyar la protección adecuada de la información y de los recursos de procesamiento la misma.

- La Secretaría de TIC debe capacitar y entrenar a los funcionarios y contratistas de acuerdo con el programa de concienciación, en busca de evitar posibles riesgos de seguridad.

5.2.1.3. Todos los Usuarios

- Los funcionarios, contratistas y personal provisto por terceras partes que por sus

funciones hagan uso de la información de la Gobernación del Atlántico, deben dar cumplimiento a las políticas, normas y procedimientos de seguridad de la información, así como asistir a las capacitaciones que sean referentes a la seguridad de la información.

5.3. POLÍTICA DE DESVINCULACIÓN, LICENCIAS, VACACIONES O CAMBIO DE LABORES DE LOS FUNCIONARIOS, CONTRATISTAS Y PERSONAL PROVISTO POR TERCEROS

La Gobernación del Atlántico asegurará que sus funcionarios, contratistas y el personal provisto por terceros serán desvinculados o reasignados para la ejecución de nuevas labores de una forma ordenada, controlada y segura.

5.3.1. NORMAS

5.3.1.1. Supervisores de Contrato, Secretarios y Jefes de Área

Cada Supervisor de Contrato, Secretario del Gabinete Departamental y Jefe de Área debe monitorear y reportar de manera inmediata la desvinculación o cambio de labores de los funcionarios, contratistas o personal provistos por terceras.

5.3.1.2. Secretaría de TIC

- La Secretaría de TIC debe verificar los reportes de desvinculación o cambio de labores y posteriormente debe solicitar la modificación o inhabilitación de usuarios.

6. POLÍTICAS DE GESTIÓN DE ACTIVOS DE INFORMACIÓN

6.1. POLÍTICA DE RESPONSABILIDAD POR LOS ACTIVOS

La Gobernación del Atlántico como propietario de la información física así como de la información generada, procesada, almacenada y transmitida con su plataforma tecnológica, otorgará responsabilidad a las áreas sobre sus activos de información, asegurando el cumplimiento de las directrices que regulen el uso adecuado de la misma.

La información, archivos físicos, los sistemas, los servicios y los equipos (ej. estaciones de trabajo, equipos portátiles, impresoras, redes, Internet, correo electrónico, herramientas de acceso remoto, aplicaciones, teléfonos y fases, entre otros) propiedad del Gobernación del Atlántico, son activos de la misma y se proporcionan a los funcionarios, contratistas y terceros autorizados, para cumplir con la misión de la organización.

Toda la información sensible de la Gobernación del Atlántico, así como los activos donde ésta se almacena y se procesa deben ser asignados a un responsable, inventariados y posteriormente clasificados, de acuerdo con los requerimientos y los criterios que dicte la Secretaría de TIC. Los propietarios de los activos de información deben llevar a cabo el levantamiento y la actualización permanente del inventario de activos de información al interior de sus procesos o áreas.

6.1.1. NORMAS

6.1.1.1. Propietarios de los Activos de Información

- Las secretarias de la Gobernación del Atlántico, deben actuar como propietarias de la información física y electrónica 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 instructivo de clasificación de la información; así mismo, deben mantener actualizado el inventario de sus activos de información.

- Los propietarios de los activos de información deben monitorear periódicamente la validez de los usuarios y sus perfiles de acceso a la información.

- 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 de la Secretaría de TIC.

6.1.1.2. Secretaría de TIC

- La Secretaría de TIC es la propietaria de los activos de información correspondientes a la plataforma tecnológica de la Gobernación del Atlántico y, en consecuencia, debe asegurar su apropiada operación y administración.

- La Secretaría de TIC debe establecer una configuración adecuada para los recursos tecnológicos, con el fin de preservar la seguridad de la información y hacer un uso adecuado de ellos.

- La Secretaría de TIC es responsable de preparar las estaciones de trabajo fijas y/o portátiles de los funcionarios y de hacer entrega de las mismas.

- La Secretaría de TIC 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.

- La Secretaría de TIC debe realizar un análisis de riesgos de seguridad de manera periódica, sobre los procesos o áreas definidas por la Gobernación del Atlántico.

- La Secretaría de TIC debe definir las condiciones de uso y protección de los activos de información, tanto los tecnológicos como aquellos que no lo son.

- La Secretaría de TIC debe realizar revisiones periódicas de los recursos de la plataforma tecnológica y los sistemas de información de la Gobernación.

6.1.1.3. Todos los Usuarios

- 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.

- 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.

- Todas las estaciones de trabajo, dispositivos móviles y demás recursos tecnológicos son asignados a un responsable, por lo cual es su compromiso hacer uso adecuado y eficiente de dichos recursos.

- En el momento de desvinculación o cambio de labores, los funcionarios y contratistas deben realizar la entrega de su puesto de trabajo Jefe inmediato o quien este delegue; así mismo, deben encontrarse a paz y salvo con la entrega de los recursos tecnológicos y otros activos de información suministrados en el momento de su vinculación.

6.2. POLÍTICA DE CLASIFICACIÓN Y MANEJO DE LA INFORMACIÓN

La Gobernación del Atlántico definirá los niveles más adecuados para clasificar su información de acuerdo con su sensibilidad, y generará una guía o instructivo de clasificación de la información para que los propietarios de la misma la cataloguen y determinen los controles requeridos para su protección.

Toda la información de la Gobernación del Atlántico debe ser identificada, clasificada y documentada de acuerdo con las guía o instructivo de clasificación de información; una vez clasificada la información, la Gobernación del Atlántico proporcionará los recursos necesarios para la aplicación de controles en busca de preservar la confidencialidad, integridad y disponibilidad de la misma, con el fin de promover el uso adecuado por parte de los funcionarios, contratistas y personal provisto por terceras partes que se encuentre autorizado y requiera de ella para la ejecución de sus actividades.

6.2.1. NORMAS

6.2.1.1. Secretaría de TIC

- La Secretaría de TIC debe definir los métodos de cifrado de la información de la Gobernación de acuerdo con el nivel de clasificación de los activos de información.

- La Secretaría de TIC debe definir los niveles de clasificación de la información para el Gobernación y, posteriormente generar la guía o instructivo de clasificación de la Información.

- La Secretaría de TIC debe socializar y divulgar la guía o instructivo de clasificación de la Información a los funcionarios y contratistas de la Gobernación del Atlántico.

- La Secretaría de TIC debe monitorear con una periodicidad establecida la aplicación del instructivo de clasificación de la Información.

- La Secretaría de TIC debe proveer los métodos de cifrado de la información, así como debe administrar el software o herramienta utilizado para tal fin.

- La Secretaría de TIC debe efectuar la eliminación segura de la información, a través de los mecanismos necesarios en la plataforma tecnológica, ya sea cuando son dados de baja o cambian de usuario.

6.2.1.2. Secretaría General

- La Secretaría General debe destruir o desechar correctamente la documentación física, con el fin de evitar la reconstrucción de la misma.

- La Secretaría General debe realizar la destrucción de información cuando se ha cumplido su ciclo de almacenamiento.

6.2.1.3. Propietarios de los Activos de Información

- Los propietarios de los activos de información deben clasificar su información de acuerdo con el instructivo de clasificación de la Información.

- Los propietarios de los activos de información son responsables de monitorear periódicamente la clasificación de sus activos de información y de ser necesario realizar su re-clasificación.

6.2.1.4. Todos los Usuarios

- Los usuarios deben acatar los lineamientos del instructivo de clasificación de la Información para el acceso, divulgación, almacenamiento, copia, transmisión , etiquetado y eliminación de la información contenida en los recursos tecnológicos, así como de la información física de la Gobernación.

- La información física y digital de la Gobernación del Atlántico debe tener un periodo de almacenamiento que puede ser dictaminado por requerimientos legales o misionales; este

período debe ser indicado en las tablas de retención documental y cuando se cumpla el periodo de expiración, toda la información debe ser eliminada adecuadamente.

- Los usuarios deben tener en cuenta estas consideraciones cuando impriman, escaneen, saquen copias y envíes faxes: verificar las áreas adyacentes a impresoras, escáneres, fotocopiadoras y máquinas de fax para asegurarse que no quedaron documentos relacionados o adicionales; asimismo, recoger de las impresoras, escáneres, fotocopiadoras y máquinas de fax, inmediatamente los documentos confidenciales para evitar su divulgación no autorizada.
- Los funcionarios, contratistas como el personal provisto por terceras partes deben asegurarse que en el momento de ausentarse de su puesto de trabajo, sus escritorios se encuentren libres de documentos y medios de almacenamiento, utilizados para el desempeño de sus labores; estos deben contar con las protecciones de seguridad necesarias de acuerdo con su nivel de clasificación.

- La información que se encuentra en documentos físicos debe ser protegida, a través de controles de acceso físico y las condiciones adecuadas de almacenamiento y resguardo.

6.3. POLÍTICA DE USO DE PERIFÉRICOS Y MEDIOS DE ALMACENAMIENTO

El uso de periféricos y medios de almacenamiento en los recursos de la plataforma tecnológica de la Gobernación del Atlántico será reglamentado por la Secretaría de TIC, considerando las labores realizadas por los funcionarios y su necesidad de uso.

6.3.1. NORMAS

6.3.1.1. Secretaría de TIC

- La Secretaría de TIC debe establecer las condiciones de uso de periféricos y medios de almacenamiento en la plataforma tecnológica de la Gobernación del Atlántico.

- La Secretaría de TIC debe implantar los controles que regulen el uso de periféricos y medios de almacenamiento en la plataforma tecnológica, de acuerdo con los lineamientos y condiciones establecidas.

- La Secretaría de TIC debe generar y aplicar lineamientos para la disposición segura de los medios de almacenamiento de la Gobernación, ya sea cuando son dados de baja o re-asignados a un nuevo usuario.

6.3.1.2. Todos los Usuarios

- Los funcionarios, contratistas y el personal provisto por terceras partes deben acoger las condiciones de uso de los periféricos y medios de almacenamiento establecidos por la Secretaría de TIC.

- Los funcionarios, contratistas y el personal provisto por terceras partes no deben modificar la configuración de periféricos y medios de almacenamiento establecidos por la Secretaría de TIC.

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

7. POLÍTICAS DE CONTROL DE ACCESO

7.1. POLÍTICA DE ACCESO A REDES Y RECURSOS DE RED

La Secretaría de TIC de la Gobernación del Atlántico, como responsables de las redes de datos y los recursos de red, debe propender porque dichas redes sean debidamente protegidas contra accesos no autorizados a través de mecanismos de control de acceso lógico.

7.1.1. NORMAS

7.1.1.1. Secretaría de TIC

- La Secretaría de TIC debe establecer un procedimiento de autorización y controles para proteger el acceso a las redes de datos y los recursos de red de la Gobernación del Atlántico.

- La Secretaría de TIC debe asegurar que las redes inalámbricas de la Gobernación del Atlántico cuenten con métodos de autenticación que evite accesos no autorizados.

- La Secretaría de TIC 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. Además, se debe formalizar la aceptación de las Políticas de Seguridad de la Información por parte de estos.

- La Secretaría de TIC 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.

7.1.1.2. Todos los Usuarios

- 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 firmado previamente.

- 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 todos los requisitos o controles para autenticarse en ellas y únicamente podrán realizar las tareas para las que fueron autorizados.

7.2. POLÍTICA DE ADMINISTRACIÓN DE ACCESO DE USUARIOS

La Gobernación del Atlántico establecerá privilegios para el control de acceso lógico de cada usuario o grupo de usuarios a las redes de datos, los recursos tecnológicos y los sistemas de información. Así mismo, velará porque los funcionarios, contratistas y el personal provisto por terceras partes tengan acceso únicamente a la información necesaria para el desarrollo de sus labores y porque la asignación de los derechos de acceso esté regulada por normas y procedimientos establecidos para tal fin.

7.2.1. NORMAS

7.2.1.1. Secretaría de TIC

- La Secretaría de TIC debe establecer un procedimiento formal para la administración de los usuarios en las redes de datos, los recursos tecnológicos y sistemas de información de la Gobernación, que contemple la creación, modificación, bloqueo o eliminación de las cuentas de usuario.

- La Secretaría de TIC, 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 Secretaría de TIC debe definir lineamientos para la configuración de contraseñas que

aplicaran 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 Secretaría de TIC debe establecer un procedimiento que asegure la eliminación, reasignación o bloqueo de los privilegios de acceso otorgados sobre 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.

7.2.1.2. Propietarios de los Activos de Información

- Es responsabilidad de los propietarios de los activos de información, definir los perfiles de usuario y autorizar las solicitudes de acceso a dichos recursos de acuerdo con los perfiles establecidos.

7.3. POLÍTICA DE RESPONSABILIDADES DE ACCESO DE LOS USUARIOS

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.

7.3.1. NORMAS

7.3.1.1. Todos los Usuarios

- Los usuarios de la plataforma tecnológica, los servicios de red y los sistemas de información de la Gobernación del Atlántico deben hacerse responsables de las acciones realizadas en los mismos, así como del usuario y contraseña asignados para el acceso a estos.

- Los usuarios no deben compartir sus cuentas de usuario y contraseñas con otros funcionarios, contratistas o con personal provisto por terceras partes.

- 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 para la configuración de contraseñas implantados.

7.4. POLÍTICA DE USO DE ALTOS PRIVILEGIOS Y UTILITARIOS DE ADMINISTRACIÓN

La Secretaría de TIC de la Gobernación del Atlántico velará porque los recursos de la plataforma tecnológica y los servicios de red sean operados y administrados en condiciones controladas y de seguridad, que permitan un monitoreo posterior de la actividad de los usuarios administradores, poseedores de los más altos privilegios sobre dicho plataforma y servicios.

7.4.1. NORMAS

7.4.1.1. Secretaría de TIC

- La Secretaría de TIC debe otorgar los privilegios para administración de recursos tecnológicos, servicios de red y sistemas de información sólo a aquellos funcionarios designados para dichas funciones.

- La Secretaría de TIC debe establecer cuentas personalizadas con altos privilegios para cada uno de los administradores de los recursos tecnológicos, servicios de red y sistemas de información.

- La Secretaría de TIC debe restringir las conexiones remotas a los recursos de la plataforma tecnológica; únicamente se deben permitir estos accesos a personal autorizado, de acuerdo con las labores desempeñadas.

- La Secretaría de TIC 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.

- La Secretaría de TIC 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.

- Los administradores de los recursos tecnológicos y servicios de red, funcionarios de la Secretaría de TIC, no deben hacer uso de los utilitarios que permiten acceso a los sistemas operativos, firmware o conexión a las bases de datos para pasar por alto la seguridad de los sistemas de información alojados sobre la plataforma tecnológica.

- Los administradores de los recursos tecnológicos deben deshabilitar las funcionalidades o

servicios no utilizados de los sistemas operativos, el firmware y las bases de datos. Se debe configurar el conjunto mínimo requerido de funcionalidades, servicios y utilitarios.

7.5. POLÍTICA DE CONTROL DE ACCESO A SISTEMAS Y APLICATIVOS

Las Secretarías y Jefaturas de Oficina, así como los propietarias 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. La Secretaría de TIC, 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. Así mismo, velará porque los desarrolladores, tanto internos como externos, acojan buenas prácticas de desarrollo en los productos generados para controlar el acceso lógico y evitar accesos no autorizados a los sistemas administrados.

7.5.1. NORMAS

7.5.1.1. Propietarios de los Activos de Información

- 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.

- 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.

7.5.1.2. Secretaría de TIC

- La Secretaría de TIC debe establecer un procedimiento para la asignación de accesos a los sistemas y aplicativos de la Gobernación.

- La Secretaría de TIC debe establecer ambientes separados a nivel físico y lógico para desarrollo, pruebas y producción, contando cada uno con su plataforma, servidores, aplicaciones, dispositivos y versiones independientes de los otros ambientes, evitando que las actividades de desarrollo y pruebas puedan poner en riesgo la integridad de la información de producción.

- La Secretaría de TIC debe asegurar, mediante los controles necesarios, que los usuarios

utilicen diferentes perfiles para los ambientes de desarrollo, pruebas y producción, y así mismo que los menús muestren los mensajes de identificación apropiados para reducir los riesgos de error.

- La Secretaría de TIC debe establecer el procedimiento y los controles de acceso a los ambientes de producción de los sistemas de información; así mismo, debe asegurarse que los desarrolladores internos o externos, posean acceso limitado y controlado a los datos y archivos que se encuentren en los ambientes de producción.

- La Secretaría de TIC debe proporcionar repositorios de archivos fuente de los sistemas de información; estos deben contar con acceso controlado y restricción de privilegios, además de un registro de acceso a dichos archivos.

7.5.1.3. Desarrolladores (INTERNOS Y EXTERNOS)

- Los desarrolladores deben asegurar que los sistemas de información construidos requieran autenticación para todos los recursos y páginas, excepto aquellas específicamente clasificadas como públicas.

- Los desarrolladores deben certificar la confiabilidad de los controles de autenticación, utilizando implementaciones centralizadas para dichos controles.

- Los desarrolladores deben certificar que no se almacenen contraseñas, cadenas de conexión u otra información sensible en texto claro y que se implementen controles de integridad de dichas contraseñas.

- Los desarrolladores deben establecer los controles de autenticación de tal manera que cuando fallen, lo hagan de una forma segura, evitando indicar específicamente cual fue la falla durante el proceso de autenticación y, en su lugar, generando mensajes generales de falla.

- Los desarrolladores deben asegurar que no se despliegan en la pantalla las contraseñas ingresadas, así como deben deshabilitar la funcionalidad de recordar campos de contraseñas.

- Los desarrolladores deben certificar que se inhabilitan las cuentas luego de un número establecido de intentos fallidos de ingreso a los sistemas desarrollados.

- Los desarrolladores deben asegurar que si se utiliza la reasignación de contraseñas, únicamente se envíe un enlace o contraseñas temporales a cuentas de correo electrónico previamente registradas en los aplicativos, los cuales deben tener un periodo de validez

establecido; se deben forzar el cambio de las contraseñas temporales después de su utilización.

- Los desarrolladores deben certificar que el último acceso (fallido o exitoso) sea reportado al usuario en su siguiente acceso exitoso a los sistemas de información.

- Los desarrolladores deben asegurar la re-autenticación de los usuarios antes de la realización de operaciones críticas en los aplicativos.

- Los desarrolladores deben, a nivel de los aplicativos, restringir acceso a archivos u otros recursos, a direcciones URL protegidas, a funciones protegidas, a servicios, a información de las aplicaciones, a atributos y políticas utilizadas por los controles de acceso y a la información relevante de la configuración, solamente a usuarios autorizados.

- Los desarrolladores deben establecer que periódicamente se re-valide la autorización de los usuarios en los aplicativos y se asegure que sus privilegios no han sido modificados.

8. POLÍTICAS DE CRIPTOGRAFÍA

8.1. POLÍTICA DE CONTROLES CRIPTOGRÁFICOS

La Gobernación del Atlántico velará porque la información clasificada como reservada o restringida, sea cifrada al momento de almacenarse y/o transmitirse por cualquier medio.

8.1.1. NORMAS

8.1.1.1. Secretaría de TIC

- La Secretaría de TIC debe almacenar y/o transmitir la información digital clasificada como reservada o restringida bajo técnicas de cifrado con el propósito de proteger su confidencialidad e integridad.

- La Secretaría de TIC debe verificar que todo sistema de información o aplicativo que requiera realizar transmisión de información reservada o restringida, cuente con mecanismos de cifrado de datos.

- La Secretaría de TIC debe desarrollar y establecer un procedimiento para el manejo y la administración de llaves de cifrado.

- La Secretaría de TIC, debe desarrollar y establecer estándares para la aplicación de controles criptográficos.

8.1.1.2. Desarrolladores (INTERNOS O EXTERNOS)

- Los desarrolladores deben cifrar la información reservada o restringida y certificar la confiabilidad de los sistemas de almacenamiento de dicha información.

- Los desarrolladores deben asegurarse que los controles criptográficos de los sistemas construidos cumplen con los estándares establecidos por la Secretaría de TIC.

9. POLÍTICAS DE SEGURIDAD FÍSICA Y MEDIOAMBIENTAL

9.1. POLÍTICA DE ÁREAS SEGURAS

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.

9.1.1. NORMAS

9.1.1.1. Secretaría de TIC

- Las solicitudes de acceso al centro de cómputo o a los centros de cableado deben ser aprobadas por personal de la Secretaría de TIC 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.

- La Secretaría de TIC 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.

- La Secretaría de TIC 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.

- La Secretaría de TIC 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 de TIC 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.

- La Secretaría de TIC 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.

- La Secretaría de TIC debe asegurar que las labores de mantenimiento de redes eléctricas, 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.

9.1.1.2. Secretarios y Jefes de Oficina

- 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 implantados en el área.

- 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.

9.1.1.3. Secretaría General

- 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.

9.1.1.4. Todos los Usuarios

- Los ingresos y egresos de personal a las instalaciones de la Gobernación del Atlántico deben ser registrados; por consiguiente, los funcionarios y personal provisto por terceras partes deben cumplir completamente con los controles físicos implantados.

- 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, en razón del 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.

9.2. POLÍTICA DE SEGURIDAD PARA LOS EQUIPOS INSTITUCIONALES

La Gobernación del Atlántico para evitar la pérdida, robo o exposición al peligro de los recursos de la plataforma tecnológica que se encuentren dentro o fuera de sus instalaciones, proveerá los recursos que garanticen la mitigación de riesgos sobre dicha plataforma tecnológica.

9.2.1. NORMAS

9.2.1.1. Secretaría de TIC

- La Secretaría de TIC 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.
- La Secretaría de TIC debe realizar mantenimientos preventivos y correctivos de los recursos de la plataforma tecnológica.

- La Secretaría de TIC debe generar estándares de configuración segura para los equipos de cómputo y posteriormente configurar dichos equipos acogiendo los estándares generados.

- La Secretaría de TIC 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.

- La Secretaría de TIC debe aislar los equipos de áreas sensibles, en busca de proteger su acceso de los demás funcionarios de la red de la Gobernación.

- La Secretaría de TIC 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 cambian de usuario.

9.2.1.2. Secretaría de Control Interno

- 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.

9.2.1.3. Todos los Usuarios

- La Secretaría de TIC 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 la Secretaría de TIC.

- 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 de la Secretaría de TIC, o personal de terceras partes autorizado por dicha dirección.
- 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 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.

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

- 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 inmediato para que se inicie el trámite interno y se debe poner la denuncia ante la autoridad competente.

- 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.

10. POLÍTICAS DE SEGURIDAD EN LAS OPERACIONES

10.1. POLÍTICA DE ASIGNACIÓN DE RESPONSABILIDADES OPERATIVAS

La Secretaría de TIC asignará funciones específicas a sus funcionarios y contratistas quienes deben efectuar la operación y administración de los recursos tecnológicos, manteniendo y actualizando la documentación de los procesos operativos para la ejecución de las actividades. Así mismo, velará por la eficiencia de los controles implantados en los procesos operativos asociados a los recursos tecnológicos con el objeto de proteger la confidencialidad, la integridad y la disponibilidad de la información manejada y asegurará que los cambios efectuados sobre dichos recursos serán adecuadamente controlados y debidamente autorizados.

La Secretaría de TIC proveerá la capacidad de procesamiento requerida en los recursos tecnológicos y sistemas de información de la Gobernación, efectuando proyecciones de crecimiento y provisiones en la plataforma tecnológica con una periodicidad definida.

10.1.1. NORMAS

10.1.1.1. Secretaría de TIC

- La Secretaría de TIC debe efectuar, a través de sus funcionarios, la documentación y actualización de los procedimientos relacionados con la operación y administración de la plataforma tecnológica de la Gobernación.

- La Secretaría de TIC debe proporcionar a sus funcionarios manuales de configuración y operación de los sistemas operativos, firmware, servicios de red, bases de datos y sistemas de información que conforman la plataforma tecnológica.

- La Secretaría de TIC debe proveer los recursos necesarios para la implantación de controles que permitan la separación de ambientes de desarrollo, pruebas y producción, teniendo en cuenta consideraciones como: controles para el intercambio de información entre los

ambientes de desarrollo y producción, la inexistencia de compiladores, editores o fuentes en los ambientes de producción y un acceso diferente para cada uno de los ambientes.

- La Secretaría de TIC, a través de sus funcionarios y contratistas, debe realizar estudios sobre la demanda y proyecciones de crecimiento de los recursos administrados (capacity planning) de manera periódica, con el fin de asegurar el desempeño y capacidad de la plataforma tecnológica. Estos estudios y proyecciones deben considerar aspectos de consumo de recursos de procesadores, memorias, discos, servicios de impresión, anchos de banda, internet y tráfico de las redes de datos, entre otros.

10.2. POLÍTICA DE PROTECCIÓN FRENTE A SOFTWARE MALICIOSO

La Gobernación del Atlántico proporcionará los mecanismos necesarios que garanticen la protección de la información y los recursos de la plataforma tecnológica en donde se procesa y almacena, adoptando los controles necesarios para evitar la divulgación, modificación o daño permanente ocasionados por software malicioso. Además, proporcionará los mecanismos para generar cultura de seguridad entre sus funcionarios, contratistas y personal provisto por terceras partes frente a los ataques de software malicioso.

10.2.1. NORMAS

10.2.1.1. Secretaría de TIC

- La Secretaría de TIC debe proveer herramientas tales como antivirus, antimalware, antispam, antispyware, entre otras, que reduzcan el riesgo de contagio de software malicioso y respalden la seguridad de la información contenida y administrada en la plataforma tecnológica de la Gobernación del Atlántico y los servicios que se ejecutan en la misma.

- La Secretaría de TIC debe asegurar que el software de antivirus, antimalware, antispam y antispyware cuente con las licencias de uso requeridas, certificando así su autenticidad y la posibilidad de actualización periódica de las últimas bases de datos de firmas del proveedor del servicio.

- La Secretaría de TIC debe certificar que la información almacenada en la plataforma tecnológica sea escaneada por el software de antivirus, incluyendo la información que se encuentra contenida y es transmitida por el servicio de correo electrónico.

- La Secretaría de TIC, a través de sus funcionarios y contratistas, debe asegurarse que los usuarios no puedan realizar cambios en la configuración del software de antivirus, antispyware, antispam, antimalware.

- La Secretaría de TIC, a través de sus funcionarios y contratistas, debe certificar que el software de antivirus, antispyware, antispam, antimalware, posea las últimas actualizaciones y parches de seguridad, para mitigar las vulnerabilidades de la plataforma tecnológica.

10.2.1.2. Todos los Usuarios

- Los usuarios de recursos tecnológicos no deben cambiar o eliminar la configuración del software de antivirus, antispyware, antimalware, antispam definida por la Secretaría de TIC; por consiguiente, únicamente podrán realizar tareas de escaneo de virus en diferentes medios.

- Los usuarios de recursos tecnológicos deben ejecutar el software de antivirus, antispyware, antispam, antimalware sobre los archivos y/o documentos que son abiertos o ejecutados por primera vez, especialmente los que se encuentran en medios de almacenamiento externos o que provienen del correo electrónico.
- Los usuarios deben asegurarse que los archivos adjuntos de los correos electrónicos descargados de internet o copiados de cualquier medio de almacenamiento, provienen de fuentes conocidas y seguras para evitar el contagio de virus informáticos y/o instalación de software malicioso en los recursos tecnológicos.

- Los usuarios que sospechen o detecten alguna infección por software malicioso deben notificar al área de soporte técnico, para que se tomen las medidas de control correspondientes.

10.3. POLÍTICA DE COPIAS DE RESPALDO DE LA INFORMACIÓN

La Gobernación del Atlántico certificará la generación de copias de respaldo y almacenamiento de su información crítica, proporcionando los recursos necesarios y estableciendo los procedimientos y mecanismos para la realización de estas actividades. Las áreas propietarias de la información, con el apoyo de la Secretaría de TIC, definirán la estrategia a seguir y los periodos de retención para el respaldo y almacenamiento de la información.

Así mismo, se velará porque los medios magnéticos que contienen la información crítica sean almacenados en una ubicación diferente a las instalaciones donde se encuentra dispuesta. El sitio externo donde se resguarden las copias de respaldo debe contar con los controles de seguridad física y medioambiental apropiados.

10.3.1. NORMAS

10.3.1.1. Secretaría de TIC

- La Secretaría de TIC, a través de sus funcionarios y contratistas, debe generar y adoptar los procedimientos para la generación, restauración, almacenamiento y tratamiento para las copias de respaldo de la información, velando por su integridad y disponibilidad.

- La Secretaría de TIC 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.

- La Secretaría de TIC, a través de sus funcionarios y contratistas, debe llevar a cabo los procedimientos para realizar pruebas de recuperación a las copias de respaldo, para así comprobar su integridad y posibilidad de uso en caso de ser necesario.

- La Secretaría de TIC debe definir las condiciones de transporte o transmisión y custodia de las copias de respaldo de la información que son almacenadas externamente.

- La Secretaría de TIC debe proporcionar apoyo para la definición de las estrategias de generación, retención y rotación de las copias de respaldo de la los activos información de la Gobernación del Atlántico.

10.3.1.2. Todos los Usuarios

- 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.

10.4. POLÍTICA DE REGISTRO DE EVENTOS Y MONITOREO DE LOS RECURSOS TECNOLÓGICOS Y LOS SISTEMAS DE INFORMACIÓN

La Gobernación del Atlántico realizará monitoreo permanente del uso que dan los funcionarios, contratistas y el personal provisto por terceras partes a los recursos de la plataforma tecnológica y los sistemas de información. Además, velará por la custodia de los registros de auditoria cumpliendo con los periodos de retención establecidos para dichos registros.

10.4.1. NORMAS

10.4.1.1. Secretaría de TIC

- La Secretaría de TIC debe determinar los eventos que generarán registros de auditoría en los recursos tecnológicos y los sistemas de información de la Gobernación del Atlántico.

- La Secretaría de TIC deben definir la roles y responsabilidades respecto al monitoreo de eventos, así como, la periodicidad de revisión de los mismos.

- La Secretaría de TIC, a través de sus funcionarios y contratistas, debe habilitar los registros de auditoría y sistemas de monitoreo de la plataforma tecnológica administrada, acorde con los eventos establecidos.
- La Secretaría de TIC debe certificar la integridad y disponibilidad de los registros de auditoria generados en la plataforma tecnológica y los sistemas de información de la Gobernación. Estos registros deben ser almacenados y solo deben ser accedidos por personal autorizado.

10.4.1.2. Secretaría de Control Interno

- La Secretaría de Control Interno debe revisar periódicamente los registros de auditoria de la plataforma tecnológica y los sistemas de información con el fin de identificar brechas de seguridad y otras actividades propias del monitoreo.

10.4.1.3. Desarrolladores (INTERNOS Y EXTERNOS)

- Los desarrolladores deben generar registros (logs) de auditoría de las actividades realizadas por los usuarios finales y administradores en los sistemas de información desarrollados. Se deben utilizar controles de integridad sobre dichos registros.

- Los desarrolladores deben registrar en los logs de auditoría eventos como: fallas de validación, intentos de autenticación fallidos y exitosos, fallas en los controles de acceso, intento de evasión de controles, excepciones de los sistemas, funciones administrativas y cambios de configuración de seguridad, entre otros, de acuerdo con las directrices establecidas por la Secretaría de TIC.

- Los desarrolladores deben evitar almacenar datos innecesarios de los sistemas construidos en los logs de auditoría que brinden información adicional a la estrictamente requerida.

10.5. POLÍTICA DE CONTROL AL SOFTWARE OPERATIVO

La Gobernación del Atlántico, a través de la Secretaría de TIC, designará responsables y establecerá procedimientos para controlar la instalación de software operativo, se cerciorará de contar con el soporte de los proveedores de dicho software y asegurará la funcionalidad de los sistemas de información que operan sobre la plataforma tecnológica cuando el software operativo es actualizado.

10.5.1. NORMAS

10.5.1.1. Secretaría de TIC

- La Secretaría de TIC debe establecer responsabilidades y procedimientos para controlar la instalación del software operativo, que interactúen con el procedimiento de control de cambios definido por la Gobernación.

- La Secretaría de TIC debe asegurarse que el software operativo instalado en la plataforma tecnológica de la Gobernación cuenta con soporte de los proveedores.

- La Secretaría de TIC debe conceder accesos temporales y controlados a los proveedores para realizar las actualizaciones sobre el software operativo, así como monitorear dichas actualizaciones.

- La Secretaría de TIC debe validar los riesgos que genera la migración hacia nuevas versiones del software operativo. Se debe asegurar el correcto funcionamiento de sistemas de información y herramientas de software que se ejecutan sobre la plataforma tecnológica cuando el software operativo es actualizado.

- La Secretaría de TIC debe establecer las restricciones y limitaciones para la instalación de software operativo en los equipos de cómputo de la Gobernación.

10.6. POLÍTICA DE GESTIÓN DE VULNERABILIDADES

La Gobernación del Atlántico, a través de la Secretaría de TIC, revisará periódicamente la aparición de vulnerabilidades técnicas sobre los recursos de la plataforma tecnológica por medio de la realización periódica de pruebas de vulnerabilidades, con el objetivo de realizar la corrección sobre los hallazgos arrojados por dichas pruebas.

10.6.1. NORMAS

10.6.1.1. Secretaría de TIC

- La Secretaría de TIC debe gestionar los trámites correspondientes para la realización de pruebas de vulnerabilidades y hacking ético con una periodicidad establecida, por un ente independiente al área objeto de las pruebas, con el fin de garantizar la objetividad del desarrollo de las mismas.

- La Secretaría de TIC debe generar los lineamientos y recomendaciones para la mitigación de vulnerabilidades, resultado de las pruebas de vulnerabilidades y hacking ético.

- La Secretaría de TIC 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.

11. POLÍTICAS DE SEGURIDAD EN LAS COMUNICACIONES

11.1. POLÍTICA DE GESTIÓN Y ASEGURAMIENTO DE LAS REDES DE DATOS

La Gobernación del Atlántico establecerá, a través de la Secretaría de TIC, los mecanismos de control necesarios para proveer la disponibilidad de las redes de datos y de los servicios que dependen de ellas; así mismo, velará por que se cuente con los mecanismos de seguridad que protejan la integridad y la confidencialidad de la información que se transporta a través de dichas redes de datos.

11.1.1. NORMAS

11.1.1.1. Secretaría de TIC

- La Secretaría de TIC debe adoptar medidas para asegurar la disponibilidad de los recursos y servicios de red de la Gobernación del Atlántico.

- La Secretaría de TIC debe implantar controles para minimizar los riesgos de seguridad de la información transportada por medio de las redes de datos.

- La Secretaría de TIC debe mantener las redes de datos segmentadas por dominios, grupos de servicios, grupos de usuarios, ubicación geográfica o cualquier otra tipificación que se considere conveniente para la Gobernación.

- La Secretaría de TIC debe identificar los mecanismos de seguridad y los niveles de servicio de red requeridos e incluirlos en los acuerdos de servicios de red, cuando estos se contraten externamente.

- La Secretaría de TIC debe establecer los estándares técnicos de configuración de los dispositivos de seguridad y de red de la plataforma tecnológica, acogiendo prácticas de configuración segura.

- La Secretaría de TIC, a través de sus funcionarios y contratistas, debe identificar, justificar y documentar los servicios, protocolos y puertos permitidos por la Gobernación en sus redes de datos e inhabilitar o eliminar el resto de los servicios, protocolos y puertos.

- La Secretaría de TIC debe instalar protección entre las redes internas y cualquier red externa, que este fuera de la capacidad de control y administración de la Gobernación.

- La Secretaría de TIC debe velar por la confidencialidad de la información del direccionamiento y el enrutamiento de las redes de datos de la Gobernación del Atlántico.

11.2. POLÍTICA DE USO DEL CORREO ELECTRÓNICO

La Gobernación del Atlántico, entendiendo la importancia del correo electrónico como herramienta para facilitar la comunicación entre funcionarios, contratistas y terceras

partes, proporcionará un servicio idóneo y seguro para la ejecución de las actividades que requieran el uso del correo electrónico, respetando siempre los principios de confidencialidad, integridad, disponibilidad y autenticidad de quienes realizan las comunicaciones a través de este medio.

11.2.1. NORMAS

11.2.1.1. Secretaría de TIC

- La Secretaría de TIC debe generar y divulgar un procedimiento para la administración de cuentas de correo electrónico.

- La Secretaría de TIC debe diseñar y divulgar las directrices técnicas para el uso de los servicios de correo electrónico.

- La Secretaría de TIC debe proveer un ambiente seguro y controlado para el funcionamiento de la plataforma de correo electrónico.

- La Secretaría de TIC debe establecer procedimientos e implantar controles que permitan detectar y proteger la plataforma de correo electrónico contra código malicioso que pudiera ser transmitido a través de los mensajes.

- La Secretaría de TIC debe generar campañas para concientizar a funcionarios, contratistas y personal provisto por terceras partes, respecto a las precauciones que deben adoptar en el intercambio de información sensible por medio del correo electrónico.

11.2.1.2. Todos los Usuarios

- La cuenta de correo electrónico asignada es de carácter individual; por consiguiente, ningún funcionario, contratista o personal provisto por terceras partes que desarrolle actividades en la Gobernación del Atlántico, bajo ninguna circunstancia debe utilizar una cuenta de correo que no sea la asignada formalmente.

- Los mensajes y la información contenida en los correos electrónicos deben ser relacionados con el desarrollo de las labores y funciones de cada usuario en apoyo a los objetivos organizacionales de la Gobernación del Atlántico. El correo institucional no debe ser utilizado para actividades personales.

- Los mensajes y la información contenida en los buzones de correo son propiedad de la Gobernación del Atlántico y cada usuario, como responsable de su buzón, debe mantener solamente los mensajes relacionados con el desarrollo de sus funciones.

- Los usuarios de correo electrónico institucional tienen prohibido él envió de cadenas de mensajes de cualquier tipo, ya sea comercial, político, religioso, material audiovisual, contenido discriminatorio, pornografía y demás condiciones que degraden la condición humana y resulten ofensivas para los funcionarios, contratistas o personal provisto por terceras partes que desarrolle actividades en la Gobernación del Atlántico.

- No es permitido el envío de archivos que contengan extensiones ejecutables, bajo ninguna circunstancia.

11.3. POLÍTICA DE USO ADECUADO DE INTERNET

La Gobernación del Atlántico consciente de la importancia de Internet como una herramienta para el desempeño de labores, proporcionará los recursos necesarios para asegurar su disponibilidad a los usuarios que así lo requieran para el desarrollo de sus actividades diarias en la institución.

11.3.1. NORMAS

11.3.1.1. Secretaría de TIC

- La Secretaría de TIC debe generar y divulgar un procedimiento para la administración de cuentas de correo electrónico.
- La Secretaría de TIC debe proporcionar los recursos necesarios para la implementación, administración y mantenimiento requeridos para la prestación segura del servicio de Internet, bajo las restricciones de los perfiles de acceso establecidos.

- La Secretaría de TIC debe diseñar e implementar mecanismos que permitan la continuidad o restablecimiento del servicio de Internet en caso de contingencia interna.

- La Secretaría de TIC debe monitorear continuamente el canal o canales del servicio de Internet.

- La Secretaría de TIC debe establecer procedimientos e implementar controles para evitar la descarga de software no autorizado, evitar código malicioso proveniente de Internet y evitar el acceso a sitios catalogados como restringidos.

- La Secretaría de TIC debe generar registros de la navegación y los accesos de los usuarios a Internet, así como establecer e implantar procedimientos de monitoreo sobre la utilización del servicio de Internet.

- La Secretaría de TIC debe generar campañas para concientizar tanto a los funcionarios, contratistas y personal provisto por terceras partes, respecto a las precauciones que deben tener en cuenta cuando utilicen el servicio de Internet.

11.3.1.2. Todos los Usuarios

- Los usuarios del servicio de Internet de la Gobernación deben hacer uso del mismo en relación con las actividades laborales que así lo requieran.

- Los usuarios del servicio de Internet deben evitar la descarga de software desde internet, así como su instalación en las estaciones de trabajo o dispositivos móviles asignados para el desempeño de sus labores.

- No está permitido el acceso a páginas relacionadas con pornografía, drogas, alcohol, webproxys, hacking y/o cualquier otra página que vaya en contra de la ética moral, las leyes vigentes o políticas establecidas en este documento.

- Los usuarios del servicio de internet tienen prohibido el acceso y el uso de servicios interactivos o mensajería instantánea como Facebook, Yahoo, Skype, Servicios P2P y otros similares, que tengan como objetivo crear comunidades para intercambiar información, o bien para fines diferentes a las actividades propias de la Gobernación del Atlántico.

- No está permitida la descarga, uso, intercambio y/o instalación de juegos, música, películas, protectores y fondos de pantalla, software de libre distribución, información y/o productos

que de alguna forma atenten contra la propiedad intelectual de sus autores, o que contengan archivos ejecutables y/o herramientas que atenten contra la integridad, disponibilidad y/o confidencialidad de la infraestructura tecnológica (hacking), entre otros.

11.4. POLÍTICA DE INTERCAMBIO DE INFORMACIÓN

La Gobernación del Atlántico asegurará la protección de la información en el momento de ser transferida o intercambiada con otras entidades y establecerá los procedimientos y controles necesarios para el intercambio de información; así mismo, se establecerán Acuerdos de Confidencialidad y/o de Intercambio de Información con las terceras partes con quienes se realice dicho intercambio. La Gobernación propenderá por el uso de tecnologías informáticas y de telecomunicaciones para llevar a cabo el intercambio de información; sin embargo, establecerá directrices para el intercambio de información en medio físico.

11.4.1. NORMAS

11.4.1.1. Secretaría General

- La Secretaría General, en acompañamiento con la Secretaría de TIC, debe definir los modelos de Acuerdos de Confidencialidad y/o de Intercambio de Información entre la Gobernación y sus funcionarios y contratistas, en los cuales deben incluir los compromisos adquiridos y las penalidades civiles o penales por el incumplimiento de dichos acuerdos. Entre los aspectos a considerar se debe incluir la prohibición de divulgar la información entregada por la Gobernación del Atlántico.

11.4.1.2. Secretaría de TIC

- La Secretaría de TIC debe establecer el procedimiento de intercambio de información con los diferentes terceros que, hacen parte de la operación de la Gobernación, el cual debe considerar la utilización de medios de transmisión confiables y la adopción de controles, con el fin de proteger la confidencialidad e integridad de la misma.

- La Secretaría de TIC debe velar porque el intercambio de información con entidades externas se realice en cumplimiento de las políticas de seguridad para el intercambio de información aquí descrita, los Acuerdos de Intercambio de Información y el procedimiento definido para dicho intercambio de información.

- La Secretaría de TIC debe ofrecer servicios o herramientas de intercambio de información seguros, así como adoptar controles como el cifrado de información, que permitan el cumplimiento del procedimiento para el intercambio de información, con el fin de proteger dicha información contra divulgación o modificaciones no autorizadas.

11.4.1.3. Propietarios de los Activos de Información

- Los propietarios de los activos de información deben velar porque la información de la Gobernación del Atlántico sea protegida de divulgación no autorizada por parte de los terceros a quienes se entrega esta información, verificando el cumplimiento de las clausulas relacionadas en los contratos, Acuerdos de confidencialidad o Acuerdos de intercambio establecidos.

- Los propietarios de los activos de información deben asegurar que los datos requeridos de los beneficiarios sólo puedan ser entregada a terceros, previo consentimiento de los titulares de los mismos, salvo en los casos que lo disponga una ley o sea una solicitud de los entes de control.

- Los propietarios de los activos de información deben autorizar los requerimientos de solicitud/envío de información de la Gobernación por/a terceras partes, salvo que se trate de solicitudes de entes de control o de cumplimiento de la legislación vigente.

- Los propietarios de los activos de información deben asegurarse que el Intercambio de información solamente se realice si se encuentra autorizada y dando cumplimiento a las políticas y procedimientos existentes.

- Los propietarios de los activos de información deben verificar la destrucción de la información suministrada a los terceros, realizada por ellos una vez esta ha cumplido el cometido por el cual fue enviada.

11.4.1.4. Terceros con Quienes se Intercambia Información

- Los terceros con quienes se intercambia información de la Gobernación del Atlántico deben darle manejo adecuado a la información recibida, en cumplimiento de las políticas de seguridad, procedimientos y las condiciones contractuales establecidas.

- Los terceros con quienes se intercambia información de la Gobernación del Atlántico deben destruir de manera segura la información suministrada, una vez esta cumpla con la función para la cual fue enviada y demostrar la realización de las actividades de destrucción.

11.4.1.5. Todos los Usuarios

- Los usuarios no deben utilizar el correo electrónico como medio para enviar o recibir información sensible de la Gobernación del Atlántico.

- No está permitido el intercambio de información sensible de la Gobernación del Atlántico por vía telefónica.

12. POLÍTICAS DE ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN

12.1. POLÍTICA PARA EL ESTABLECIMIENTO DE REQUISITOS DE SEGURIDAD

La Gobernación del Atlántico asegurará que el software adquirido y desarrollado tanto al interior, como por terceras partes, cumplirá con los requisitos de seguridad y calidad establecidos. Las áreas propietarias de sistemas de información y la Secretaría de TIC incluirán requisitos de seguridad en la definición de requerimientos y, posteriormente se asegurarán que estos se encuentren generados a cabalidad durante las pruebas realizadas sobre los desarrollos del software construido.

12.1.1. NORMAS

12.1.1.1. Propietarios de los Sistemas de Información

- Todos los sistemas de información o desarrollos de software deben tener un área propietaria formalmente asignada dentro de la Gobernación del Atlántico.

- La Secretaría de TIC debe establecer metodologías para el desarrollo de software, que incluyan la definición de requerimientos de seguridad y las buenas prácticas de desarrollo seguro, con el fin de proporcionar a los desarrolladores una visión clara de lo que se espera.

- Las áreas propietarias de los sistemas de información, en acompañamiento con la Secretaría de TIC deben establecer las especificaciones de adquisición o desarrollo de sistemas de información, considerando requerimientos de seguridad de la información.

- Las áreas propietarias de los sistemas de información deben definir qué información sensible puede ser eliminada de sus sistemas y solicitar que estos soporten la eliminación de dicha información, como es el caso de los datos personales o financieros, cuando estos ya no son requeridos.

- La Secretaría de TIC debe liderar la definición de requerimientos de seguridad de los sistemas de información, teniendo en cuenta aspectos como la estandarización de herramientas de desarrollo, controles de autenticación, controles de acceso y arquitectura de aplicaciones, entre otros.

12.1.1.2. Desarrolladores (INTERNOS O EXTERNOS)

- Los desarrolladores deben documentar los requerimientos establecidos y definir la arquitectura de software más conveniente para cada sistema de información que se quiera desarrollar, de acuerdo con los requerimientos de seguridad y los controles deseados.

- Los desarrolladores deben certificar que todo sistema de información adquirido o desarrollado utilice herramientas de desarrollo licenciadas y reconocidas en el mercado.

- Los desarrolladores deben deshabilitar las funcionalidades de completar automáticamente en formularios de solicitud de datos que requieran información sensible.

- Los desarrolladores deben establecer el tiempo de duración de las sesiones activas de las aplicaciones, terminándolas una vez se cumpla este tiempo.

- Los desarrolladores deben asegurar que no se permitan conexiones recurrentes a los sistemas de información con el mismo usuario.

- Los desarrolladores deben utilizar usar los protocolos sugeridos por la Secretaría de TIC en los aplicativos desarrollados.

12.2. POLÍTICA DE DESARROLLO SEGURO, REALIZACIÓN DE PRUEBAS Y SOPORTE DE LOS SISTEMAS

La Gobernación del Atlántico velará porque el desarrollo interno o externo de los sistemas de información cumpla con los requerimientos de seguridad esperados, con las buenas prácticas para desarrollo seguro de aplicativos, así como con metodologías para la realización de pruebas de aceptación y seguridad al software desarrollado. Además, se asegurará que todo software desarrollado o adquirido, interna o externamente cuenta con el nivel de soporte requerido por la Gobernación.

12.2.1. NORMAS

12.2.1.1. Propietarios de los Sistemas de Información

- Los propietarios de los sistemas de información son responsables de realizar las pruebas para asegurar que cumplen con los requerimientos funcionales establecidos antes del paso a producción de los sistemas, utilizando metodologías establecidas para este fin, documentado las pruebas realizadas y aprobando los pasos a producción. Estas pruebas deben realizarse por entrega de funcionalidades nuevas, por ajustes de funcionalidad o por cambios sobre la plataforma tecnológica en la cual funcionan los aplicativos.

- Los propietarios de los sistemas de información deben aprobar las migraciones entre los ambientes de desarrollo, pruebas y producción de sistemas de información nuevos y/o de cambios o nuevas funcionalidades.

12.2.1.2. Secretaría de TIC

- La Secretaría de TIC debe implantar los controles necesarios para asegurar que las migraciones entre los ambientes de desarrollo, pruebas y producción han sido aprobadas, de acuerdo con el procedimiento de control de cambios.

- La Secretaría de TIC debe contar con sistemas de control de versiones para administrar los cambios de los sistemas de información de la Gobernación del Atlántico.

- La Secretaría de TIC debe asegurase que los sistemas de información adquiridos o desarrollados por terceros, cuenten con un acuerdo de licenciamiento el cual debe especificar las condiciones de uso del software y los derechos de propiedad intelectual.

- La Secretaría de TIC debe generar metodologías para la realización de pruebas al software desarrollado, que contengan pautas para la selección de escenarios, niveles, tipos, datos de pruebas y sugerencias de documentación.

- La Secretaría de TIC, a través de sus funcionarios y contratistas, se debe asegurar que la plataforma tecnológica, las herramientas de desarrollo y los componentes de cada sistema de información estén actualizados con todos los parches generados para las versiones en uso y que estén ejecutando la última versión aprobada del sistema.

- La Secretaría de TIC debe incluir dentro del procedimiento y los controles de gestión de cambios el manejo de los cambios en el software aplicativo y los sistemas de información de la Gobernación.

- La Secretaría de TIC debe verificar que las pruebas de seguridad sobre los sistemas de información se realicen de acuerdo con las metodologías definidas, contando con pruebas debidamente documentadas

12.2.1.3. Desarrolladores (INTERNOS O EXTERNOS)

- Los desarrolladores de los sistemas de información deben considerar las buenas prácticas y lineamientos de desarrollo seguro durante el ciclo de vida de los mismos, pasando desde el diseño hasta la puesta en marcha.

- Los desarrolladores deben proporcionar un nivel adecuado de soporte para solucionar los problemas que se presenten en el software aplicativo de la Gobernación del Atlántico; dicho soporte debe contemplar tiempos de respuesta aceptables.

- Los desarrolladores deben construir los aplicativos de tal manera que efectúen las validaciones de datos de entrada y la generación de los datos de salida de manera confiable, utilizando rutinas de validación centralizadas y estandarizadas.

- Los desarrolladores deben asegurar que los sistemas de información construidos validen la información suministrada por los usuarios antes de procesarla, teniendo en cuenta aspectos como: tipos de datos, rangos válidos, longitud, listas de caracteres aceptados, caracteres considerados peligrosos y caracteres de alteración de rutas, entre otros.

- Los desarrolladores deben suministrar opciones de desconexión o cierre de sesión de los aplicativos (logout) que permitan terminar completamente con la sesión o conexión asociada, las cuales deben encontrarse disponibles en todas las páginas protegidas por autenticación.

- Los desarrolladores deben asegurar el manejo de operaciones sensibles o críticas en los aplicativos desarrollados permitiendo el uso de dispositivos adicionales como tokens o el ingreso de parámetros adicionales de verificación.

- Los desarrolladores deben asegurar que los aplicativos proporcionen la mínima información de la sesión establecida, almacenada en cookies y complementos, entre otros.

- Los desarrolladores deben garantizar que no se divulgue información sensible en respuestas de error, incluyendo detalles del sistema, identificadores de sesión o información de las cuentas de usuarios; así mismo, deben implementar mensajes de error genéricos.

- Los desarrolladores deben remover todas las funcionalidades y archivos que no sean necesarios para los aplicativos, previo a la puesta en producción.

- Los desarrolladores deben prevenir la revelación de la estructura de directorios de los sistemas de información construidos.

- Los desarrolladores deben remover información innecesaria en los encabezados de respuesta que se refieran a los sistemas operativos y versiones del software utilizado.

- Los desarrolladores deben evitar incluir las cadenas de conexión a las bases de datos en el código de los aplicativos. Dichas cadenas de conexión deben estar en archivos de configuración independientes, los cuales se recomienda que estén cifrados.

- Los desarrolladores deben certificar el cierre de la conexión a las bases de datos desde los aplicativos tan pronto como estas no sean requeridas.

- Los desarrolladores deben desarrollar los controles necesarios para la transferencia de archivos, como exigir autenticación, vigilar los tipos de archivos a transmitir, almacenar los archivos transferidos en repositorios destinados para este fin o en bases de datos, eliminar privilegios de ejecución a los archivos transferidos y asegurar que dichos archivos solo tengan privilegios de lectura.

- Los desarrolladores deben proteger el código fuente de los aplicativos construidos, de tal forma de que no pueda ser descargado ni modificado por los usuarios.

- Los desarrolladores deben asegurar que no se permite que los aplicativos desarrollados ejecuten comandos directamente en el sistema operativo.

12.3. POLÍTICA PARA LA PROTECCIÓN DE LOS DATOS DE PRUEBA

La Secretaría de TIC protegerá los datos de prueba que se entregarán a los desarrolladores, asegurando que no revelan información confidencial de los ambientes de producción.

12.3.1. NORMAS

12.3.1.1. Secretaría de TIC

- La Secretaría de TIC debe certificar que la información a ser entregada a los desarrolladores para sus pruebas será enmascarada y no revelará información confidencial de los ambientes de producción.

- La Secretaría de TIC debe eliminar la información de los ambientes de pruebas, una vez estas han concluido.

13. POLÍTICAS QUE RIGEN DE LA RELACIÓN CON TERCERAS PARTES

13.1. POLÍTICA DE INCLUSIÓN DE CONDICIONES DE SEGURIDAD EN LA RELACIÓN CON TERCERAS PARTES

La Gobernación del Atlántico establecerá mecanismos de control en sus relaciones con terceras partes, con el objetivo de asegurar que la información a la que tengan acceso o

servicios que sean provistos por las mismas, cumplan con las políticas, normas y procedimientos de seguridad de la información.

Los funcionarios o contratistas responsables de la realización y/o firma de contratos o convenios con terceras partes se asegurarán de la divulgación de las políticas, normas y procedimientos de seguridad de la información a dichas partes.

13.1.1. NORMAS

13.1.1.1. Secretaría Jurídica y Secretaría de TIC

- La Secretaría Jurídica y la Secretaría de TIC deben generar un modelo base para los Acuerdos de Niveles de Servicio y requisitos de Seguridad de la Información, con los que deben cumplir terceras partes o proveedores de servicios; dicho modelo, debe ser divulgado a todas las áreas que adquieran o supervisen recursos y/o servicios tecnológicos.

- La Secretaría Jurídica y la Secretaría de TIC deben elaborar modelos de Acuerdos de Confidencialidad y Acuerdos de Intercambio de Información con terceras partes. De dichos acuerdos deberá derivarse una responsabilidad tanto civil como penal para la tercera parte contratada.

13.1.1.2. Secretaría de TIC

- La Secretaría de TIC debe establecer las condiciones de conexión adecuada para los equipos de cómputo y dispositivos móviles de los terceros en la red de datos de la Gobernación del Atlántico.

- La Secretaría de TIC debe establecer las condiciones de comunicación segura, cifrado y transmisión de información desde y hacia los terceros proveedores de servicios.

- La Secretaría de TIC debe mitigar los riesgos relacionados con terceras partes que tengan acceso a los sistemas de información y la plataforma tecnológica de la Gobernación del Atlántico.

- La Secretaría de TIC debe evaluar y aprobar los accesos a la información de la Gobernación requeridos por terceras partes.

- La Secretaría de TIC debe identificar y monitorear los riesgos relacionados con terceras partes o los servicios provistos por ellas, haciendo extensiva esta actividad a la cadena de suministro de los servicios de tecnología o comunicaciones provistos.

13.1.1.3. Supervisores de Contratos con Terceros

- Los Supervisores de contratos con terceros deben divulgar las políticas, normas y procedimientos de seguridad de la información de la Gobernación del Atlántico a dichos terceros, así como velar porque el acceso a la información y a los recursos de almacenamiento o procesamiento de la misma, por parte de los terceros se realice de manera segura, de acuerdo con las políticas, normas y procedimientos de seguridad de la información.

13.2. POLÍTICA DE GESTIÓN DE LA PRESTACIÓN DE SERVICIOS DE TERCERAS PARTES

La Gobernación del Atlántico propenderá por mantener los niveles acordados de seguridad de la información y de prestación de los servicios de los proveedores, en concordancia con los acuerdos establecidos con estos. Así mismo, velará por la adecuada gestión de cambios en la prestación de servicios de dichos proveedores.

13.2.1. NORMAS

13.2.1.1. Secretaría de TIC

- La Secretaría de TIC 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.

- La Secretaría de TIC debe verificar las condiciones de comunicación segura, cifrado y transmisión de información desde y hacia los terceros proveedores de servicios.

13.2.1.2. Secretaría de TIC y Supervisores de Contratos con Terceros

- La Secretaría de TIC 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 de la Secretaría de TIC, 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.

14. POLÍTICAS DE GESTIÓN DE INCIDENTES DE SEGURIDAD

14.1. POLÍTICA PARA EL REPORTE Y TRATAMIENTO DE INCIDENTES DE SEGURIDAD

La Gobernación del Atlántico promoverá entre los funcionarios, contratistas y personal provisto por terceras partes el reporte de incidentes relacionados con la seguridad de la información y sus medios de procesamiento, incluyendo cualquier tipo de medio de almacenamiento de información, como la plataforma tecnológica, los sistemas de información, los medios físicos de almacenamiento y las personas.

De igual manera, asignará responsables para el tratamiento de los incidentes de seguridad de la información, quienes tendrán la responsabilidad de investigar y solucionar los incidentes reportados, tomando las medidas necesarias para evitar su reincidencia y escalando los incidentes de acuerdo con su criticidad.

La Alta Dirección o a quien delegue, son los únicos autorizados para reportar incidentes de seguridad ante las autoridades; así mismo, son los únicos canales de comunicación autorizados para hacer pronunciamientos oficiales ante entidades externas.

14.1.1. NORMAS

14.1.1.1. Propietarios de los Activos de Información

- Los propietarios de los activos de información deben informar a la Secretaría de TIC, los incidentes de seguridad que identifiquen o que reconozcan su posibilidad de materialización.

14.1.1.2. Secretaría de TIC

- La Secretaría de TIC debe establecer responsabilidades y procedimientos para asegurar una respuesta rápida, ordenada y efectiva frente a los incidentes de seguridad de la información.

- La Secretaría de TIC debe evaluar todos los incidentes de seguridad de acuerdo a sus circunstancias particulares y escalar a los roles adecuados aquellos en los que se considere pertinente.

- La Secretaría de TIC debe designar personal calificado, para investigar adecuadamente los incidentes de seguridad reportados, identificando las causas, realizando una investigación exhaustiva, proporcionando las soluciones y finalmente previniendo su re-ocurrencia.

- La Secretaría de TIC debe crear bases de conocimiento para los incidentes de seguridad presentados con sus respectivas soluciones, con el fin de reducir el tiempo de respuesta para los incidentes futuros, partiendo de dichas bases de conocimiento.

14.1.1.3. Todos los Usuarios

- Es responsabilidad de los funcionarios, contratistas y personal provisto por terceras partes reportar cualquier evento o incidente relacionado con la información y/o los recursos tecnológicos con la mayor prontitud posible.

- En caso de conocer la pérdida o divulgación no autorizada de información clasificada reservada o restringida, los funcionarios, contratistas y personal provisto por terceras partes deben notificarlo a la Secretaría de TIC para que se registre y se le dé el trámite necesario.

15. POLÍTICAS DE INCLUSIÓN DE SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO

15.1. POLÍTICA DE CONTINUIDAD, CONTINGENCIA, RECUPERACIÓN Y RETORNO A LA NORMALIDAD CON CONSIDERACIONES DE SEGURIDAD DE LA INFORMACIÓN

La Gobernación del Atlántico proporcionará los recursos suficientes para suministrar una respuesta efectiva de funcionarios, contratistas y procesos en caso de contingencia o eventos catastróficos que se presenten y que afecten la continuidad de la operación.

Además, responderá de manera efectiva ante eventos catastróficos según la magnitud y el grado de afectación de los mismos; se restablecerán las operaciones con el menor costo y pérdidas posibles, manteniendo la seguridad de la información durante dichos eventos. La

Gobernación del Atlántico mantendrá canales de comunicación adecuados hacia funcionarios, contratistas, proveedores y terceras partes interesadas.

15.1.1. NORMAS

15.1.1.1. Secretaría de TIC

- La Secretaría de TIC debe reconocer las situaciones que serán identificadas como emergencia o desastre para la Gobernación, los procesos o las áreas y determinar cómo se debe actuar sobre las mismas.

- La Secretaría de TIC debe liderar los temas relacionados con la continuidad del negocio y la recuperación ante desastres

- La Secretaría de TIC debe realizar los análisis de impacto al negocio y los análisis de riesgos de continuidad para posteriormente proponer posibles estrategias de recuperación en caso de activarse el plan de contingencia o continuidad, con las consideraciones de seguridad de la información a que haya lugar.

- La Secretaría de TIC producto del análisis BIA debe seleccionar las estrategias de recuperación más convenientes para la Gobernación del Atlántico.

- La Secretaría de TIC debe validar que los procedimientos de contingencia, recuperación y retorno a la normalidad incluyan consideraciones de seguridad de la información.
- La Secretaría de TIC debe asegurar la realización de pruebas periódicas del plan de recuperación ante desastres y/o continuidad de negocio, verificando la seguridad de la información durante su realización y la documentación de dichas pruebas.

- La Secretaría de TIC deben elaborar un plan de recuperación ante desastres para el centro de cómputo y un conjunto de procedimientos de contingencia, recuperación y retorno a la normalidad para cada uno de los servicios y sistemas prestados.

15.1.1.2. Secretarios y Jefes de Oficina

- Los Secretarios y Jefes de Oficina deben identificar y, al interior de sus áreas, generar la documentación de los procedimientos de continuidad que podrían ser utilizados en caso de un

evento adverso, teniendo en cuenta la seguridad de la información. Estos documentos deben ser probados para certificar su efectividad.

15.2. POLÍTICA DE REDUNDANCIA

La Gobernación del Atlántico propenderá por la existencia de una plataforma tecnológica redundante que satisfaga los requerimientos de disponibilidad aceptables para la organización.

15.2.1. NORMAS

15.2.1.1. Secretaría de TIC

- La Secretaría de TIC 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.

- La Secretaría de TIC debe evaluar y probar soluciones de redundancia tecnológica y seleccionar la solución que mejor cumple los requerimientos de la Gobernación del Atlántico.

- La Secretaría de TIC a través de sus funcionarios y contratistas, debe administrar las soluciones de redundancia tecnológica y realizar pruebas periódicas sobre dichas soluciones, para asegurar el cumplimiento de los requerimientos de disponibilidad de la Gobernación del Atlántico.

16. POLÍTICAS DE CUMPLIMIENTO

16.1. POLÍTICA DE CUMPLIMIENTO CON REQUISITOS LEGALES Y CONTRACTUALES

La Gobernación del Atlántico velará por la identificación, documentación y cumplimiento de la legislación relacionada con la seguridad de la información, entre ella la referente a derechos de autor y propiedad intelectual, razón por la cual propenderá porque el software instalado en los recursos de la plataforma tecnológica cumpla con los requerimientos legales y de licenciamiento aplicables.

16.1.1. NORMAS

16.1.1.1. Secretaría Jurídica y Secretaría de TIC

- La Secretaría Jurídica y la Secretaría de TIC deben identificar, documentar y mantener actualizados los requisitos legales, reglamentarios o contractuales aplicables a la Gobernación del Atlántico y relacionados con seguridad de la información.

16.1.1.2. Secretaría de TIC

- La Secretaría de TIC debe certificar que todo el software que se ejecuta en la Gobernación del Atlántico esté protegido por derechos de autor y requiera licencia de uso o, en su lugar sea software de libre distribución y uso.

- La Secretaría de TIC debe establecer un inventario con el software y sistemas de información que se encuentran permitidos en las estaciones de trabajo o equipos móviles de la Gobernación del Atlántico para el desarrollo de las actividades laborales, así como verificar periódicamente que el software instalado en dichas estaciones de trabajo o equipos móviles corresponda únicamente al permitido.

16.1.1.3. Todos los Usuarios

- Los usuarios no deben instalar software o sistemas de información en sus estaciones de trabajo o equipos móviles suministrados para el desarrollo de sus actividades.

- Los usuarios deben cumplir con las leyes de derechos de autor y acuerdos de licenciamiento de software. Es ilegal duplicar software o su documentación sin la autorización del propietario de los derechos de autor y, su reproducción no autorizada es una violación de ley; no obstante, puede distribuirse un número de copias bajo una licencia otorgada.

Original Firmada.

Gobernación del Atlántico

ATLÁNTICO LÍDER