1. **TIPO DE INFORME**
   Informe definitivo de Auditoría

2. **NOMBRE DEL PROCESO O ÁREA AUDITADA**
   Gestión de Recursos de TI – Secretaría General

3. **EQUIPO AUDITOR**
   Orlando De la Rosa Bolívar – Profesional Universitario

4. **EQUIPO QUE RECIBIÓ LA AUDITORIA**
   Xavier Mejía – Ingeniero Grupo de TI – Secretaría General

5. **FECHA DE AUDITORIA**
   17 de marzo 2021 – mayo 31 de 2021

6. **OBJETIVO DE LA AUDITORIA**
   Verificar la aplicación y el cumplimiento de las políticas de seguridad de la información de la Gobernación del Atlántico, adoptadas mediante el Decreto 00296 de 2018.

7. **ALCANCE DE LA AUDITORIA**
   La auditoría comprendió la evaluación de las diferentes políticas que forman en su conjunto la POLITICA DE SEGURIDAD DE LA INFORMACION de la Gobernación del Departamento del Atlántico.

   POLÍTICA DE ESTRUCTURA ORGANIZACIONAL DE SEGURIDAD DE LA INFORMACIÓN
   POLÍTICAS DE SEGURIDAD DEL PERSONAL
   POLÍTICAS DE GESTIÓN DE ACTIVOS DE INFORMACIÓN
   POLÍTICAS DE CONTROL DE ACCESO
   POLÍTICAS DE CRIPTOGRAFÍA
   POLÍTICAS DE SEGURIDAD FÍSICA Y MEDIOAMBIENTAL
   POLÍTICAS DE SEGURIDAD EN LAS OPERACIONES
   POLÍTICAS DE SEGURIDAD EN LAS COMUNICACIONES
   POLÍTICAS DE ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN
   POLÍTICAS DE INCLUSIÓN DE SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO
   POLÍTICAS DE GESTIÓN DE INCIDENTES DE SEGURIDAD
   POLÍTICAS DE CUMPLIMIENTO

   Comprendidas entre los numerales 4 y 16 del Manual de Políticas de Seguridad de la Información de la Entidad)

8. CRITERIOS MARCO NORMATIVO UTILIZADOS

Decreto 00296 de 2018 *"Por medio del cual se actualiza el Manual de Políticas Informáticas de la Gobernación del Departamento del Atlántico"*

Manual de implementación de la Política de Gobierno digital – Habilitador Seguridad de la información – publicado en página web

Resolución 500 de marzo de 2021, proferida por Min Tic.

9. PAPELES DE TRABAJO

Consultas en página Web de la entidad:https://www.atlantico.gov.co/index.php/politicas-planes/politicas-informaticas-2018

Archivos Excel generados:
FORMATO AUD GOB DIGITAL 2021.xls
FORMATO AUD SEG INFORMACION_diligenciado.xls
FORMATO INFOMACION ADICIONAL.xls

Archivo PDF:
EVIDENCIAS AUDITORIA SEGURIDAD INFORMATICA.pdf
PROCEDIMIENTO GESTION DE ACCESOS LOGICOS

10. METODOLOGÍA

Para el desarrollo del presente proceso auditor se diseñó un formato en hoja de cálculo a efectos de solicitar la información al auditado y que a su vez sirviera de base para elaborar el informe correspondiente.

Se utilizó de igual forma las técnicas de Análisis y observación de información

11. ANTECEDENTES

Dado que la información es un elemento crítico para lograr los objetivos de la entidad y teniendo en cuenta el grado de automatización actual de la gobernación del Departamento del Atlántico, se llevó a cabo el presente proceso auditor sobre los aspectos mencionados en el alcance y contenidos en las políticas de seguridad de la información vigente, con el fin de verificar su cumplimiento.

Para lo antes expuesto, se deben tener en cuenta los aspectos propios de un ambiente de TI y para tal fin se analiza la información reportada por la Secretaría General, con respecto a la administración de la información y su seguridad considerando además la Tecnología en la que se soporta la Información

relacionada, siendo esta la base para su administración y control, por lo que deben ser evaluados con el fin adicional de lograr evidencia del estado de la Seguridad.

12. PALABRAS CLAVES

Seguridad informática: La seguridad informática es un conjunto de herramientas, procedimientos y estrategias que tienen como objetivo garantizar la integridad, disponibilidad y confidencialidad de la información de una entidad en un sistema.

Auditoria de seguridad informática: Procedimiento que evalúa el nivel de seguridad de la entidad, analizando sus procesos y comprobando si sus políticas de seguridad se cumplen, con el fin de detectar vulnerabilidades y debilidades de seguridad que pueden ser utilizadas por terceros malintencionados para robar información, impedir el funcionamiento de sistemas, o en general, causar daños e interrumpir las operaciones.

Estándares: Principios aplicables de manera general y que se utilizan para regular buenas prácticas y aspectos que deben estar presentes en las organizaciones que los aplican.

Buenas Prácticas: Acciones que se han demostrado que funcionan bien y dan buenos resultados.

13. OBSERVACIONES Y/O HALLAZGOS

Para el desarrollo de la presente auditoría, se tomó como base los dos puntos mencionados en el alcance, es decir la política 4a la política 16 y las respuestas aportadas por la Secretaría general, mediante el grupo de Gestión de TI.

13.1 POLÍTICA DE ESTRUCTURA ORGANIZACIONAL DE SEGURIDAD DE LA INFORMACIÓN, corresponde al numeral 4 en el documento de políticas de seguridad de la entidad.

13.1.1 POLÍTICA DE ESTRUCTURA ORGANIZACIONAL DE SEGURIDAD DE LA INFORMACIÓN

Con respecto a este ítem se observan debilidades en el cumplimiento de las actividades *"(...) verificar el cumplimiento de las políticas de seguridad de la información aquí mencionadas y (…) validar y monitorear de manera periódica la implantación de los controles de seguridad establecidos (…)".* Dado que tales acciones no se encuentran enmarcadas en procedimientos administrativos adoptados, generando riesgos frente a la discrecionalidad en la aplicación por parte del funcionario responsable.

13.1.2 POLÍTICA PARA USO DE DISPOSITIVOS MÓVILES

Con respecto a este ítem, se observa el incumplimiento de la totalidad de los puntos de control relacionados con el uso de dispositivos móviles, en particular, no se evidencia el desarrollo de acciones como:

- Investigar y probar las opciones de protección de los dispositivos móviles institucionales y personales que hagan uso de los servicios provistos por la Gobernación.
- Establecer las configuraciones aceptables para los dispositivos móviles institucionales o personales que hagan uso de los servicios provistos por la Gobernación
- 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

13.1.3 POLÍTICA PARA USO DE CONEXIONES REMOTAS.

En lo relativo a este ítem, la entidad presente un adecuado manejo y control de las conexiones remotas. No obstante, se observan debilidades frente a la adopción de procedimientos administrativos que formalicen las acciones de control asociadas.

13.2 <u>POLÍTICAS DE SEGURIDAD DEL PERSONAL, corresponde al numeral 5 en el documento de políticas de seguridad de la entidad.</u>

13.2.1POLÍTICA RELACIONADA CON LA VINCULACIÓN DE FUNCIONARIOS, CONTRATISTAS Y PERSONAL PROVISTO POR TERCEROS.

Se evidencian debilidades por la ausencia de procedimientos administrativos para que la Secretaría General pueda velar y garantizar que 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.

13.2.2POLÍTICA APLICABLE DURANTE LA VINCULACIÓN DE FUNCIONARIOS, CONTRATISTAS Y PERSONAL PROVISTO POR TERCEROS.

No se aportaron evidencias sobre el diseño y realización de jornadas de concientización en seguridad de la información, con el objetivo de apoyar la protección adecuada de la información y de los recursos de procesamiento la misma, en este mismo sentido tampoco existen mecanismos que permitan a

los funcionarios y contratistas contar con un entrenamiento en busca de evitar posibles riesgos de seguridad.

13.3 POLÍTICAS DE GESTIÓN DE ACTIVOS DE INFORMACIÓN, corresponde al numeral 6 en el documento de políticas de seguridad de la entidad.

13.3.1POLÍTICA DE CLASIFICACIÓN Y MANEJO DE LA INFORMACIÓN

No se observan evidencias sobre la realización de jornadas de concientización en seguridad de la información, la elaboración y socialización de guías o instructivos de clasificación de la información, con el fin de establecer claramente los mecanismos y formas en que la entidad clasifica y monitorea la información.

13.3.2POLÍTICA DE USO DE PERIFÉRICOS Y MEDIOS DE ALMACENAMIENTO

Al analizar este componente de la política de seguridad, se observa que la Secretaría general ha establecido algunas condiciones sobre el uso de periféricos y medios de almacenamiento en la plataforma tecnológica de la Gobernación del Atlántico y algunos controles para regular su uso, pero es notoria la ausencia de mecanismos para su verificación y de acciones enmarcadas en procedimiento adoptado, que permita determinar y evaluar su cumplimiento.

13.4 POLÍTICAS DE CONTROL DE ACCESO corresponde al numeral 7 en el documento de políticas de seguridad de la entidad

13.4.1*POLÍTICA DE ACCESO A REDES Y RECURSOS DE RED*

a) De acuerdo con lo informado por la Secretaría General, esta política se cumple mediante la ejecución del procedimiento "GESTION DE ACCESOS LOGICOS", cuyo objetivo es "*Planear, ejecutar y controlar las actividades relacionadas con la creación, modificación y eliminación/bloqueo de cuentas de usuario en los recursos, servicios y sistemas de información de la Gobernación del Departamento del Atlántico, con el fin de garantizar la integridad de los accesos a dichos recursos, servicios y sistemas*".

Analizadas las actividades establecidas en el citado procedimiento, se aprecia que dentro del objetivo se menciona la actividad de planear, pero a lo largo del procedimiento no se ven actividades que lleven a concluir que tal actividad, en particular, se esté ejecutando.

b) Dentro de los aspectos que conforman esta política se observa el siguiente: "*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." Sobre este tema, no se evidencia el registro documental de este control, ya que se habla de la aceptación de las responsabilidades, lo que implica un vínculo con el usuario y que debería soportase con un documento que evidencie tal aceptación.

c) En el procedimiento descrito, no se observa el registro o evidencia documental asociado con la actividad de "*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" .*

13.4.2POLÍTICA DE ADMINISTRACIÓN DE ACCESO DE USUARIOS.

a) No se evidencia el cumplimiento del aspecto relacionado con "*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*". Lo anterior, permitiría establecer y documentar un esquema adecuado de contraseñas y dar cumplimiento a la esta política

13.4.3POLÍTICA DE RESPONSABILIDADES DE ACCESO DE LOS USUARIOS.

a) En este punto la política hace referencia al control sobre los accesos de los usuarios y en particular establece condiciones sobre el manejo de las contraseñas y la salvaguarda de la información. Para efectos de llevar a cabo la revisión de este punto se solicitó información sobre los controles sobre

   i. 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.

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

   Sobre los ítems anteriores no se obtuvo respuesta en el cuestionario de auditoría.

b) Un elemento de este punto de la política, es el relacionado con *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. Si bien es cierto que se respondió afirmativamente que la política se cumple, no se suministró evidencia documental acerca de la existencia de un inventario de 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 Entidad.

13.4.4POLÍTICA DE USO DE ALTOS PRIVILEGIOS Y UTILITARIOS DE ADMINISTRACIÓN

a) Si bien es cierto se respondió de forma afirmativa que la política se cumple, no se suministró evidencia documental acerca de la existencia de puntos de control sobre esta política en la entidad.

13.4.5POLÍTICA DE CONTROL DE ACCESO A SISTEMAS Y APLICATIVOS

a) Si bien es cierto se respondió de forma afirmativa que la política se cumple, no se suministró evidencia documental acerca de la existencia de puntos de control sobre esta política en la entidad.

13.5 POLÍTICAS DE CRIPTOGRAFÍA corresponde al numeral 8 en el documento de políticas de seguridad de la entidad

13.5.1POLÍTICA DE CONTROLES CRIPTOGRÁFICOS

De acuerdo con la información suministrada por la Secretaría General, en la entidad hacen falta procedimientos relacionados con el manejo y control criptográfico, principalmente en la elaboración de técnicas de cifrado para el almacenamiento y transmisión de información clasificada como reservada o restringida lo cual debe tener como propósito fundamental la protección de la confidencialidad y la integridad de la misma. De igual se deben establecer y formalizar los mecanismos para que todo sistema de información o aplicativo que requiera realizar transmisión de información reservada o restringida, cuente con cifrado de datos, todo esto acompañado de una administración de llaves de cifrados basados en estándares que puedan ser verificadas y monitoreadas.

13.6 POLÍTICAS DE SEGURIDAD FÍSICA Y MEDIOAMBIENTAL corresponde al numeral 9 en el documento de políticas de seguridad de la entidad

13.6.1 POLÍTICA DE ÁREAS SEGURAS

La Secretaría General mantiene de forma adecuada las instalaciones físicas del centro de cableado y se observan medidas de seguridad sobre el acceso físico del personal, sin embargo, las acciones de control carecen de una formalidad en procedimiento administrativo, de igual forma, el control en bitácora del acceso del personal se encuentra ausente. Por otra parte, hace falta establecer la formalidad al momento del retiro de personal o de cambios en sus responsabilidades.

Las tareas de 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, carecen de procedimientos adoptados

Desde el punto de vista de condiciones físicas y medioambientales necesarias para certificar la protección y correcta operación de los recursos de la plataforma tecnológica para la protección del centro de cómputo, la entidad cuenta con aspectos tales como la ubicación en el centro de cómputo; de 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. Sin embargo, no se evidencia documento que evidencie el monitoreo de estos sistemas, ya que deben realizarse de manera permanente y establecerse así en el procedimiento correspondiente.

Se presentan debilidades en la programación para mantenimiento de redes eléctricas, de voz y de datos, por cuanto hace falta enmarcar esta actividad en el procedimiento correspondiente y dejar la evidencia documental del programa de mantenimiento.

13.6.2 POLÍTICA DE SEGURIDAD PARA LOS EQUIPOS INSTITUCIONALES

En la entidad, hace falta establecer en procedimiento las actividades para definir 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.

13.7 POLÍTICAS DE SEGURIDAD EN LAS OPERACIONES corresponde al numeral 10 en el documento de políticas de seguridad de la entidad

13.7.1POLÍTICA DE ASIGNACIÓN DE RESPONSABILIDADES OPERATIVAS

Al analizar este punto se aprecian debilidades en lo relativo a la ausencia de la entrega de 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, por parte de la Secretaría General a sus funcionarios.

13.7.2POLÍTICA DE PROTECCIÓN FRENTE A SOFTWARE MALICIOSO

Frente a los componentes de este punto, la entidad controla de manera adecuada la posibilidad de instalación de software por parte de sus funcionarios, dado el esquema de dominio y de protección que maneja. Sin embargo, no se ha iniciado el proceso para certificar que la información almacenada en la plataforma tecnológica sea escaneada por el software de antivirus, incluyendo la información que viaja por medio del servicio de correo electrónico.

13.7.3POLÍTICA DE COPIAS DE RESPALDO DE LA INFORMACIÓN

De acuerdo con lo mencionado por la Secretaría General, se presentan debilidades en cuanto a la ausencia de procedimientos para realizar pruebas de recuperación a las copias de respaldo mediante lo cual se pueda comprobar su integridad y posibilidad de uso en caso de ser necesario.

De igual forma, la dependencia encargada, no ha definido mediante procedimientos las condiciones de transporte o transmisión y custodia de las copias de respaldo de la información que son almacenadas externamente y en este mismo sentido lo debe hacer para la definición de las estrategias de generación, retención y rotación de las copias de respaldo de la los activos información de la Entidad.

13.7.4POLÍTICA DE REGISTRO DE EVENTOS Y MONITOREO DE LOS RECURSOS TECNOLÓGICOS Y LOS SISTEMAS DE INFORMACIÓN

En este punto la debilidad más evidente se observa en la ausencia de documentación y registro de eventos, así como su monitoreo y la periodicidad de revisión de los mismos.

En este mismo sentido, es ausente la habilitación de los registros de auditoría y sistemas de monitoreo de la plataforma tecnológica administrada, acorde con los eventos establecidos, para todos los aplicativos de la entidad.

Con todo lo a antes expuesto, se debe llegar a contar con una certificación sobre la integridad y disponibilidad de los registros de auditoria generados en la plataforma tecnológica y los sistemas de información de la Gobernación, en los que además se debe garantizar que estos registros están almacenados y su acceso es exclusivo al personal autorizado

13.7.5POLÍTICA DE CONTROL AL SOFTWARE OPERATIVO

Se cuenta con procedimientos de control para sobre la instalación y actualización del software operativo, su soporte por medio de proveedores, monitoreo y verificación para la instalación de actualizaciones, validación de riesgos en la migración a nuevas versiones y las restricciones necesarias para la instalación de software en los equipos de la entidad.

13.7.6POLÍTICA DE GESTIÓN DE VULNERABILIDADES

La entidad carece de una gestión para la realización de pruebas de vulnerabilidades y hacking ético con una periodicidad establecida, por parte de un agente independiente al área objeto de las pruebas, con el fin de garantizar la objetividad del desarrollo de las mismas.

Una vez se logre lo antes mencionado, debería poder generarse los lineamientos y recomendaciones para la mitigación de vulnerabilidades, resultado de las pruebas de vulnerabilidades y hacking ético.

El área encargada, debe diseñar un cronograma o programación, en la que se determinen las acciones de revisión periódica de la aparición de nuevas vulnerabilidades técnicas, que sean reportadas a los administradores de la plataforma tecnológica y desarrolladores de los sistemas de información, con el fin de mitigar la exposición al riesgo de estos.

13.8 POLÍTICAS DE SEGURIDAD EN LAS COMUNICACIONES corresponde al numeral 11 en el documento de políticas de seguridad de la entidad

13.8.1POLÍTICA DE GESTIÓN Y ASEGURAMIENTO DE LAS REDES DE DATOS

En el mapa de Riesgos del proceso de las tecnologías, falta actualización sobre aspectos relacionados con la seguridad de la información transportada por medio de las redes de datos. Así mismo, deben establecerse y documentarse estándares técnicos de configuración de los dispositivos de seguridad y de red de la plataforma tecnológica, los servicios y protocolos permitidos en la entidad, acogiendo prácticas de configuración segura y siempre velando por la confidencialidad de la información del direccionamiento y el enrutamiento de las redes de datos de la Gobernación del Atlántico

Falta la conservación documental (física o lógica) de la segmentación de las redes de datos por dominios, grupos de servicios, grupos de usuarios, ubicación geográfica o cualquier otra tipificación que se considere conveniente para la entidad.

13.8.2POLÍTICA DE USO DEL CORREO ELECTRÓNICO

En términos generales se da un adecuado cumplimiento a los aspectos relacionados con el manejo del correo electrónico en la entidad.

Sin embargo, hace falta la actualización y divulgación de las directrices técnicas para el uso de los servicios de correo electrónico, Así como también, la formalización de las acciones para implantar controles que permitan detectar y proteger la plataforma de correo electrónico contra código malicioso que pudiera ser transmitido a través de los mensajes y 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.

13.8.3POLÍTICA DE USO ADECUADO DE INTERNET

En la entidad existen controles para el manejo y acceso adecuado de internet, así como restricciones generales que permiten un uso correcto del mismo.

Tal como en otros aspectos de todas estas políticas, se aprecia la ausencia de documentación y adopción de procedimientos o acciones de control que permitan dejar evidencia y generar informes o reporte sobre el monitoreo de los siguientes aspectos:

- Canales de internet con que cuenta la Gobernación.

- 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.
- Continuidad o restablecimiento del servicio de Internet en caso de contingencia interna.
- Descarga de software no autorizado, evitar código malicioso proveniente de Internet y evitar el acceso a sitios catalogados como restringidos.
- Registro de la navegación y los accesos de los usuarios a Internet
- Uso del servicio de internet

13.8.4POLÍTICA DE INTERCAMBIO DE INFORMACIÓN

Se aprecia la inexistencia de un procedimiento para controlar, verificar y monitorear el intercambio de información con los diferentes terceros que, hacen parte de la operación de la Gobernación, en el que se consideren aspectos como:

- Uso de medios de transmisión confiables.
- Adopción de controles.
- Protección y garantía de la confidencialidad e integridad de los datos.
- Cumplimiento de las políticas de seguridad relacionadas con el intercambio de información
- Acuerdos de Intercambio de Información.
- Cifrado de información.
- Divulgación o modificaciones no autorizadas.

13.9 POLÍTICAS DE ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN corresponde al numeral 12 en el documento de políticas de seguridad de la entidad

13.9.1POLÍTICA PARA EL ESTABLECIMIENTO DE REQUISITOS DE SEGURIDAD

Dentro del procedimiento para el desarrollo de software existen controles y actividades tendientes a dar cumplimiento a los requisitos de seguridad.

13.9.2POLÍTICA DE DESARROLLO SEGURO, REALIZACIÓN DE PRUEBAS Y SOPORTE DE LOS SISTEMAS

Dentro del procedimiento para el desarrollo de software existen controles y actividades tendientes a dar cumplimiento para garantizar el cumplimiento de los requerimientos del aplicativo, mediante pruebas con el área dueña de la información.

13.9.3POLÍTICA PARA LA PROTECCIÓN DE LOS DATOS DE PRUEBA

Dentro de las acciones contenidas en el PROCEDIMIENTO PARA LA CONTRUCCION Y/O MANTENIMIENTO DE APLICACIONES, la Secretaría general no contempla la actividad de 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, así como tampoco se incluye una relacionada con la eliminación de la información de los ambientes de pruebas, una vez estas han concluido.

13.10 POLÍTICAS QUE RIGEN DE LA RELACIÓN CON TERCERAS PARTES corresponde al numeral 13 en el documento de políticas de seguridad de la entidad

13.10.1 POLÍTICA DE INCLUSIÓN DE CONDICIONES DE SEGURIDAD EN LA RELACIÓN CON TERCERAS PARTES

Dentro de los documentos que hacen falta con el fin de establecer las condiciones de seguridad en la relación con terceros encontramos:

- 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.
- Condiciones de comunicación segura, cifrado y transmisión de información desde y hacia los terceros proveedores de servicios.
- Riesgos relacionados con terceras partes que tengan acceso a los sistemas de información y la plataforma tecnológica de la Gobernación del Atlántico
- Evaluación y aprobación de los accesos a la información de la Gobernación requeridos por terceras partes

13.10.2 POLÍTICA DE GESTIÓN DE LA PRESTACIÓN DE SERVICIOS DE TERCERAS PARTES

En la entidad son inexistente los mecanismos y la documentación que permitan 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, en este mismo sentido se deben verificar las condiciones de comunicación segura, cifrado y transmisión de información desde y hacia los terceros proveedores de servicios.

13.11 POLÍTICAS DE GESTIÓN DE INCIDENTES DE SEGURIDAD corresponde al numeral 14 en el documento de políticas de seguridad de la entidad

13.11.1 POLÍTICA PARA EL REPORTE Y TRATAMIENTO DE INCIDENTES DE SEGURIDAD

No obstante, el área encargada, cuenta con personal y lineamientos relativos a la seguridad y/o el manejo de los incidentes relacionado con este tema, no se cuenta con mecanismos, procedimientos o esquemas formales y adoptados que puedan establecer de manera clara y directa las responsabilidades y

acciones que puedan asegurar una respuesta rápida, ordenada y efectiva frente a los incidentes de seguridad de la información.

De igual forma se debe diseñar y documentar la gestión para la evaluación de todos los incidentes de seguridad de acuerdo a sus circunstancias particulares y escalar a los roles adecuados aquellos en los que se considere pertinente, esto incluye contar o capacitar al personal con el objeto de que esté calificado, para indagar adecuadamente sobre los incidentes de seguridad reportados, identificando las causas, realizando una investigación exhaustiva, proporcionando las soluciones y finalmente previniendo su re-ocurrencia.

Actualmente hace falta 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.

13.12 POLITICA INCLUSIÓN DE SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO corresponde al numeral 15 en el documento de políticas de seguridad de la entidad

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

Tomando como base la definición que nos muestra la norma ISO 22301, entre otros estándares internacionales, sobre planes de contingencia y/o continuidad de operaciones, encontramos que se refiere a que *Existe la posibilidad de que, en un determinado momento, una organización independientemente de su tamaño, número de trabajadores o de la actividad que realice, pueda verse afectada por una crisis o desastre.*

Teniendo en cuenta lo antes definido, se busca mediante la creación de estos planes minimizar la posibilidad de ocurrencia de un desastre y en caso de producirse, que su impacto sea mínimo y lograr que el tiempo de reanudación de las operaciones sea el más corto posible.

Con base en lo antes expuesto y teniendo en cuenta que este numeral establece la existencia de dicho plan, se aprecia la existencia del mismo en la entidad, con actividades para garantizar la continuidad, pero no hay evidencia documentada de las pruebas y evaluación de resultados del mismo, tal como se establece en el punto 6 del numeral 15.1.1.1. el cual describe que en la entidad se debe "Asegurarla 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"

13.12.2 POLÍTICA DE REDUNDANCIA

a) Se aprecia la existencia de un plan de contingencia, en el que se muestran las actividades para garantizar la continuidad, pero no hay evidencia documentada de las pruebas y evaluación de resultados del mismo, tal como se establece en el aspecto de "*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"*, propio de esta política.

13.13 POLÍTICAS DE CUMPLIMIENTO corresponde al numeral 16 en el documento de políticas de seguridad de la entidad

13.13.1 POLÍTICA DE CUMPLIMIENTO CON REQUISITOS LEGALES Y CONTRACTUALES

En la entidad se cumplen los parámetros establecidos y se cuenta con procedimientos para el control de los requisitos legales y contractuales en los aspectos relacionados con la seguridad de la información.

14. RIESGOS ASOCIADOS

En el marco de las funciones asignadas a la Secretaría de Control Interno, se procedió a hacer un análisis de este tema a partir del mapa de riesgos del proceso TIC y de las observaciones y hallazgos detectados en la presente auditoría. En relación con este tema, se concluye:

14.1 La Política de Gestión de Riesgos vigente para la Entidad, es pertinente y adecuada a los procesos auditados y se observa acorde con la normatividad vigente, emanada principalmente del Departamento Administrativo de la Función Pública.

14.2 En el mapa de riesgos del proceso evaluado, se observa la aplicación de la Política adoptada, evidenciando el seguimiento a los controles implementados de los primeros dos trimestres del año.

14.3 En la revisión del mapa de riesgos y oportunidades del proceso GESTION DE TI, se pudo constatar la falta de análisis de riesgos asociados a algunos aspectos contenidos en la política de seguridad de la información. Dentro de los cuales mostramos los siguientes:

a) En lo relativo a la POLÍTICA APLICABLE DURANTE LA VINCULACIÓN DE FUNCIONARIOS, CONTRATISTAS Y PERSONAL PROVISTO POR TERCEROS, dada la ausencia de evidencia de jornadas de socialización a este personal,

se pueden presentar riesgos de seguridad de la información, ya sea por error involuntario o mal manejo de la misma.

b) Al analizar lo contenido en los aspectos de la POLÍTICA DE CONTROL AL SOFTWARE OPERATIVO, no obstante, la existencia de procedimiento, se hace necesario contar con verificaciones periódicas que minimicen la posible ocurrencia de riesgos asociados a la inclusión de códigos o instrucciones que apunten a acciones indebidas o no autorizadas.

c) En la POLÍTICA DE GESTIÓN DE VULNERABILIDADES, básicamente el riesgo asociado consiste en la posibilidad de no contar con mecanismo para la detección oportuna de situaciones que impliquen nuevas vulnerabilidades técnicas y que no sean reportadas.

d) En la POLÍTICA DE GESTIÓN Y ASEGURAMIENTO DE LAS REDES DE DATOS, se deben tener en cuenta en el mapa de riesgos del proceso, aspectos sobre la actualización de los datos asociados con la seguridad de la información transportada por medio de las redes de datos y documentarlos a efectos de lograr siempre contar con formas adecuadas para la recuperación de información y las rutas de estas en la red de la entidad.

e) En la POLÍTICA DE INCLUSIÓN DE CONDICIONES DE SEGURIDAD EN LA RELACIÓN CON TERCERAS PARTES, tener en cuenta y analizar los riesgos asociados con el hecho que terceras partes tengan acceso a los sistemas de información y la plataforma tecnológica de la Gobernación del Atlántico

15. RECOMENDACIONES GENERALES Y DE COMPLEMENTO A LAS CONTENIDAS EN REPORTE DE FURAG

15.1 Realizar las acciones correspondientes para documentar y formalizar los aspectos de las políticas analizadas, con el fin de organizar y crear el esquema de control adecuado a partir de la organización y normatización de los mismos.

15.2 Actualizar el procedimiento de GESTION DE ACCESOS LOGICOS, en lo relativo a las actividades de planeación de su objetivo, así como también en los aspectos que hacen referencia al cumplimiento de los contenidos de las políticas revisadas en este proceso auditor

15.3 Continuar con el seguimiento a los mapas de riesgos por parte de la oficina de planeación o quien haga sus veces, dentro del rol que cumplen en el esquema de líneas de defensa.

Proponer acciones de mejora para el diseño y la ejecución de controles, por parte de los cargos que lideran de manera transversal temas estratégicos de gestión (tales como jefes de planeación, financieros, contratación, TI, servicio al ciudadano, líderes de otros sistemas de gestión, comités de riesgos).

15.4 Desarrollar jornadas de capacitación y/o divulgación a sus servidores y contratistas sobre seguridad digital.

15.5 Fortalecer las capacidades en seguridad digital de la entidad a través de su participación en las jornadas de socialización y promoción del uso del modelo de gestión de riesgos de seguridad digital convocadas por el Ministerio de Tecnologías de la Información y las Comunicaciones

15.6 Fortalecer las capacidades en seguridad digital de la entidad a través de convenios o acuerdos de intercambio de información para fomentar la investigación, la innovación y el desarrollo de temas relacionados con la defensa y seguridad nacional en el entorno digital.

15.7 Fortalecer las capacidades en seguridad digital de la entidad a través de ejercicios de simulación de incidentes de seguridad digital al interior de la entidad.

15.8 Adelantar acciones para la gestión sistemática y cíclica del riesgo de seguridad digital en la entidad tales como registrarse en el CSIRT Gobierno y/o ColCERT

15.9 Adelantar acciones para la gestión sistemática y cíclica del riesgo de seguridad digital en la entidad tales como adoptar e implementar la guía para la identificación de infraestructura crítica cibernética

15.10 Adelantar acciones para la gestión sistemática y cíclica del riesgo de seguridad digital en la entidad tales como realizar la identificación anual de la infraestructura crítica cibernética e informar al CCOC

15.11 Adelantar acciones para la gestión sistemática y cíclica del riesgo de seguridad digital en la entidad tales como participar en la construcción de los planes sectoriales de protección de la infraestructura crítica cibernética

15.12 Adelantar acciones para la gestión sistemática y cíclica del riesgo de seguridad digital en la entidad tales como adoptar e implementar la Guía para la Administración de los Riesgos de Gestión, Corrupción y Seguridad Digital y el Diseño de Controles en entidades públicas

15.13

15.14 Implementar un Sistema de Gestión de Seguridad de la Información (SGSI) en la entidad a partir de las necesidades identificadas, y formalizarlo mediante un acto administrativo.

15.15 Hacer campañas de concientización en temas de seguridad de la información de manera frecuente y periódica, específicas para cada uno de los distintos roles dentro de la entidad.

15.16 Establecer un procedimiento de gestión de incidentes de seguridad de la información, formalizarlo y actualizarlo de acuerdo con los cambios de la entidad

15.17 Clasificar y etiquetar la información de la entidad de acuerdo con las leyes aplicables vigentes

15.18 Al momento de establecer los nuevos lineamientos o actualizar la política de seguridad de la entidad, recomendamos tener en cuenta lo mencionado en la Resolución 500 de marzo 10 de 2021, del MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES

16. CONCLUSIÓN

En lo relativo a los aspectos evaluados en el documento de la Política de Seguridad Digital de la Entidad y tomando como base el objetivo del presente proceso auditor, se puede concluir, que, no obstante, contar con un procedimiento específico para el manejo de la Gestión de TI, existen aún aspectos dentro de la política, que deben ser objeto de revisión, documentación y/o actualización. Lo anterior, con el fin de lograr una mejora y una mayor cobertura en la seguridad de los datos soportados por la plataforma informática de la Gobernación del Departamento del Atlántico, dando así un cumplimiento integral a la política.

Este informe se emite en versión final, toda vez que ya fue revisado, socializado y aceptado por el auditor y área auditada, tal como consta en el acta del 13 de octubre de 2021, en la que participaron, por parte del Grupo de Gestión de TI, los funcionarios, ADRIANA MARTINEZ, Líder de Programa, MIGUEL DOMINGUEZ SANDOVAL, Profesional Especializado, JOSE GUERRERO RADA, Contratista, GUILLERMO CASTRO, Contratista, YANNETH CHAPARRO RUEDA, Profesional Especializado, quien se conectó vía telefónica.

PLAN DE MEJORAMIENTO

Como resultado de la Auditoría, deberán elaborar y suscribir el correspondiente plan de mejoramiento, a más tardar el 25 de octubre 2021, que contenga las acciones de mejora que permitan corregir las debilidades identificadas en el proceso auditor.

Atentamente,

RAFAEL FAJARDO MOVILLA
Secretaría de Control Interno

Copia: Dr. Raúl Lacoutere Daza – Secretario General
Ing. Adriana Martínez Muñoz – Líder TI Secretaria General