| | | |
|---|---|---|
| Gobernación del Atlántico / ATLÁNTICO LÍDER | **PLAN DE ACCIÓN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN.**<br>**PLAN DE TRATAMIENTO DE RIESGOS**<br>**CUMPLIMIENTO DE LA ESTRATEGIA DE GOBIERNO DIGITAL**<br>**SECRETARÍA TIC** | Versión: 1.0<br>Fecha: 15/12/2017 |

# PLAN DE ACCIÓN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN.

# PLAN DE TRATAMIENTO DE RIESGOS
# CUMPLIMIENTO DE LA ESTRATEGIA DE GOBIERNO DIGITAL

Secretaría de Tecnologías de la Información y las

Comunicaciones (TIC)

Gobernación del Atlántico

Barranquilla-Atlántico

2017

*TABLA DE CONTENIDO*

## OBJETIVOS

El plan de acción y tratamiento de riesgos de seguridad de la información se realiza con los siguientes propósitos:

- Exponer los resultados producto del análisis de riegos de seguridad de la información de la Gobernación del Atlántico.
- Presentar el plan de acción y tratamiento correspondiente al análisis y evaluación de riesgos realizado a la Gobernación del Atlántico, considerando los niveles de riesgo identificados y los controles aplicables para su mitigación.

## ALCANCE

El alcance de este documento comprende dos grandes aspectos; el primero presenta los resultados del análisis de riesgos de seguridad de la información de la Gobernación del Atlántico; por otra parte, el segundo aspecto contempla los lineamientos para llevar a cabo un plan de tratamiento adecuado a través de proyectos alineados a los controles del anexo A de la norma ISO/IEC 27001:2013 y las guías comprendidas en la norma ISO/27002:2013, para los riesgos identificados.

## INTRODUCCIÓN

El presente documento contiene los resultados del análisis de riesgos de seguridad de la información realizado; además, presenta un plan de tratamiento de riesgos el cual contempla aspectos como controles del anexo A de la norma ISO/IEC 27001:2013, las vulnerabilidades que se mitigan y proyectos que se encuentran alineados a los controles, con el fin de dar una mayor claridad en la implementación.

## 1. RESULTADOS DEL ANÁLISIS DE RIESGOS DE SEGURIDAD

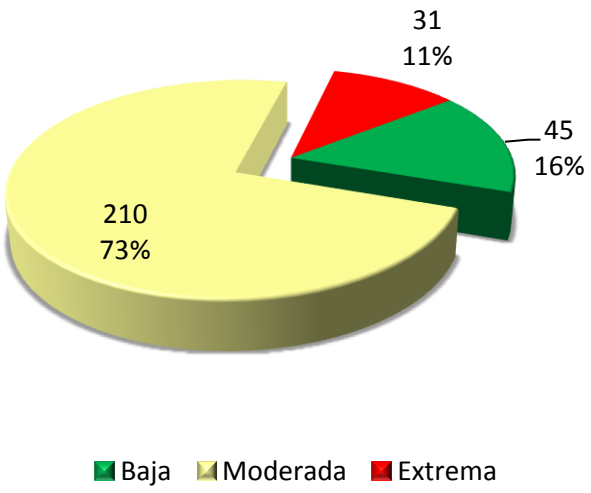
El análisis y evaluación de riesgos de seguridad de la información fue desarrollado considerando los activos de información que apoyan las actividades desarrolladas en la Secretaría de Informática y Telecomunicaciones; además, se desarrolló con el acompañamiento de personal que ejerce diferentes roles dentro de la secretaría, el cual ejecuto actividades como la valoración del impacto de los activos de información considerando la confidencialidad, integridad y disponibilidad de los mismos, estableciendo la probabilidad que una amenaza explote una vulnerabilidad y recolectando la información de los controles existentes para mitigar los riesgos.

De la información obtenida durante la fase de identificación y valoración de activos de información se obtuvo un listado final de 45 activos de información de los cuales 23 fueron sometidos al análisis y evaluación de riesgos de seguridad de acuerdo con su valor de activo.

El total de riesgos evaluados e identificados para los diferentes activos de información fueron 286, distribuidos por zona de riesgo de la siguiente manera:

| ZONA RIESGO | NO. RIESGOS |
|---|---|
| Baja | 45 |
| Moderada | 210 |
| Extrema | 31 |
| Total | **286** |

En el siguiente grafico se presenta el porcentaje correspondiente por zona de riesgo, de acuerdo con el total de riesgos identificados que se relacionan en la tabla anterior, obteniendo como resultado 11% en la zona de riesgo Extrema, 76% en la zona de riesgo Moderada y 16% en la zona de riesgo Baja.



Finalmente, la siguiente imagen presenta la distribución de riesgos de acuerdo con el mapa de calor definido por la Gobernación de Atlántico:

| PROBABILIDAD | NIVEL DE IMPACTO | | | | |
|---|---|---|---|---|---|
| | 1. Insignificante | 2. Menor | 3. Moderado | 4. Mayor | 5. Catastrófico |
| 1. Raro | | | | 13% | 0% |
| 2. Improbable | | | | 24% | 5% |
| 3. Posible | | | | 27% | 5% |
| 4. Probable | | | | 16% | 6% |
| 5. Casi seguro | | | | 3% | 2% |

## 2. PLAN DE ACCION Y TRATAMIENTO DE RIESGOS

### 2.1. ESTRUCTURA

El plan de tratamiento de riesgos de seguridad de la información se compone de los hallazgos del análisis y evaluación de riesgos, considerando los controles identificados y su relación con la mitigación de vulnerabilidades, niveles de aceptación o zonas de riesgo y tratamiento o proyectos propuestos.

Es importante mencionar que un mismo control puede mitigar diferentes vulnerabilidades, para distintos niveles de aceptación o zonas de riesgo y que diferentes proyectos pueden apoyar un mismo control en la mitigación del riesgo. Por lo tanto, en el momento de realizar la implementación de los controles de niveles de riesgos con mayor prioridad, se pueden tratar riesgos que aparecen en zonas de riesgo con menor prioridad.

A continuación, se observa la estructura de los planes de tratamiento de riesgos:

| NIVEL DE ACEPTACIÓN | CONTROL |
|---|---|
| Riesgos en zona Extrema | Control del Anexo A de la norma ISO/IEC 27001:2013 o control adicional |
| Riesgos en zona Moderada | |

| Riesgos en zona Baja | |
|---|---|
| **VULNERABILIDADES** | **PROYECTOS** |
| Vulnerabilidades asociadas a los activos de información | Listado de proyectos que apoyan el control del anexo A o control adicional, con el fin de dar tratamiento a las vulnerabilidades presentadas |

## 2.2. PLANES DE ACCION Y TRATAMIENTO

A continuación, se presenta la descripción de cada uno de los controles del Anexo A de la norma ISO/IEC 27001:2013 y los controles adicionales propuestos, para los diferentes niveles de riesgos en que resulten aplicables:

| NIVEL DE ACEPTACIÓN | CONTROL |
|---|---|
| Moderada | A.6.1.1 Roles y Responsabilidades de Seguridad de la Información |
| **VULNERABILIDADES** | **PROYECTOS** |
| • Falta de controles en la vinculación | • Implementación y seguimiento de Políticas de Seguridad<br>• Verificación y actualización de funciones y responsabilidades<br>• Generación de la organización de seguridad |

| NIVEL DE ACEPTACIÓN | CONTROL |
|---|---|
| Extrema<br>Moderada | A.6.1.2 Segregación de Funciones |
| **VULNERABILIDADES** | **PROYECTOS** |
| • Concentración de funciones | • Implementación y seguimiento de Políticas de Seguridad<br>• Verificación y actualización de funciones y responsabilidades<br>• Generación de la organización de seguridad<br>• Revisión y ajustes de perfiles en aplicaciones, servicios de red y recursos tecnológicos |

| NIVEL DE ACEPTACIÓN | CONTROL |
|---|---|
| Moderada | A.6.1.3 Contacto con las Autoridades |
| **VULNERABILIDADES** | **PROYECTOS** |
| • Incumplimiento de los lineamientos de seguridad | • Notificación a terceras partes |

| NIVEL DE ACEPTACIÓN | CONTROL |
|---|---|
| Moderada | A.6.1.4 Contacto con Grupos de Interés |
| **VULNERABILIDADES** | **PROYECTOS** |

| | |
|---|---|
| • Falta de entrenamiento en seguridad de la información | • Implementación y seguimiento de Políticas de Seguridad<br>• Vinculación a foros y grupos de interés |

| NIVEL DE ACEPTACIÓN | CONTROL |
|---|---|
| Moderada<br>Baja | A.6.2.2 Teletrabajo |
| **VULNERABILIDADES** | **PROYECTOS** |
| • Falta de controles en los servicios de conexión remota<br>• Falta de controles de acceso remoto | • Implementación y seguimiento de Políticas de Seguridad<br>• Gestión del acceso lógico<br>• Documentación y mantenimiento de procedimientos operativos |

| NIVEL DE ACEPTACIÓN | CONTROL |
|---|---|
| Moderada | A.7.1.1 Selección |
| **VULNERABILIDADES** | **PROYECTOS** |
| • Falta de controles en la vinculación | • Implementación y seguimiento de Políticas de Seguridad<br>• Controles sobre los funcionarios desde la vinculación hasta la desvinculación |

| NIVEL DE ACEPTACIÓN | CONTROL |
|---|---|
| Moderada | A.7.1.2 Términos y Condiciones del Empleo |
| **VULNERABILIDADES** | **PROYECTOS** |
| • Falta de controles en la vinculación | • Implementación y seguimiento de Políticas de Seguridad<br>• Controles sobre los funcionarios desde la vinculación hasta la desvinculación<br>• Definición y establecimiento de Acuerdos de Niveles de Operación |

| NIVEL DE ACEPTACIÓN | CONTROL |
|---|---|
| Moderada | A.7.2.2 Concientización, educación y entrenamiento en Seguridad de la Información |
| **VULNERABILIDADES** | **PROYECTOS** |
| • Falta de entrenamiento en seguridad de la información | • Implementación y seguimiento de Políticas de Seguridad<br>• Concientización y educación |

| NIVEL DE ACEPTACIÓN | CONTROL |
|---|---|
| Moderada | A.7.2.3 Proceso Disciplinario |

| VULNERABILIDADES | PROYECTOS |
|---|---|
| • Incumplimiento de los lineamientos de seguridad | • Implementación y seguimiento de Políticas de Seguridad<br>• Controles sobre los funcionarios desde la vinculación hasta la desvinculación<br>• Controles sobre los terceros<br>• Identificación y actualización de la legislación vigente |

| NIVEL DE ACEPTACIÓN | CONTROL |
|---|---|
| Moderada | A.7.3.1 Responsabilidades de Terminación |
| **VULNERABILIDADES** | **PROYECTOS** |
| • Falta de controles en la desvinculación o cambio de cargo | • Implementación y seguimiento de Políticas de Seguridad<br>• Controles sobre los funcionarios desde la vinculación hasta la desvinculación<br>• Controles sobre los terceros |

| NIVEL DE ACEPTACIÓN | CONTROL |
|---|---|
| Moderada | A.8.1.4 Devolución de Activos |
| **VULNERABILIDADES** | **PROYECTOS** |
| • Falta de controles en la desvinculación o cambio de cargo | • Implementación y seguimiento de Políticas de Seguridad<br>• Controles sobre los funcionarios desde la vinculación hasta la desvinculación<br>• Controles sobre los terceros |

| NIVEL DE ACEPTACIÓN | CONTROL |
|---|---|
| Extrema<br>Moderada | A.8.2.1 Clasificación de Información |
| **VULNERABILIDADES** | **PROYECTOS** |
| • Falta de clasificación y condiciones de manejo de la información | • Implementación y seguimiento de Políticas de Seguridad<br>• Concientización y educación<br>• Generación de la Guía de clasificación de la información y los procedimiento de manejo<br>• Clasificación de activos de información y aplicación de procedimientos de manejo |

| NIVEL DE ACEPTACIÓN | CONTROL |
|---|---|
| Moderada | A.8.2.2 Etiquetado de Información |
| **VULNERABILIDADES** | **PROYECTOS** |

| | |
|---|---|
| • Falta de clasificación y condiciones de manejo de la información | • Implementación y seguimiento de Políticas de Seguridad<br>• Clasificación de activos de información y aplicación de procedimientos de manejo<br>• Concientización y educación |

| NIVEL DE ACEPTACIÓN | CONTROL |
|---|---|
| Extrema | A.8.2.3 Manejo de activos |
| Moderada | |
| | |
| **VULNERABILIDADES** | **PROYECTOS** |
| • Falta de clasificación y condiciones de manejo de la información<br>• Falta de controles de almacenamiento y resguardo<br>• Falta de controles en el traslado<br>• Falta de controles en la disposición final | • Implementación y seguimiento de Políticas de Seguridad<br>• Clasificación de activos de información y aplicación de procedimientos de manejo<br>• Seguridad en la reutilización de los equipos<br>• Generación y verificación de las copias de respaldo |

| NIVEL DE ACEPTACIÓN | CONTROL |
|---|---|
| | A.8.3.1 Gestión de Medios Removibles |
| Moderada | |
| Baja | |
| **VULNERABILIDADES** | **PROYECTOS** |
| • Falta de controles en el uso de dispositivos de almacenamiento<br>• Falta de controles de almacenamiento y resguardo | • Implementación y seguimiento de Políticas de Seguridad<br>• Clasificación de activos de información y aplicación de procedimientos de manejo<br>• Generación y verificación de las copias de respaldo |

| NIVEL DE ACEPTACIÓN | CONTROL |
|---|---|
| | A.8.3.2 Disposición de Medios |
| Moderada | |
| | |
| **VULNERABILIDADES** | **PROYECTOS** |
| • Falta de controles en la disposición final | • Clasificación de activos de información y aplicación de procedimientos de manejo<br>• Seguridad en la reutilización de los equipos |

| NIVEL DE ACEPTACIÓN | CONTROL |
|---|---|
| | A.8.3.3 Transferencia Física de Medios |
| Moderada | |
| | |
| **VULNERABILIDADES** | **PROYECTOS** |

| | |
|---|---|
| • Falta de controles en el traslado | • Implementación y seguimiento de Políticas de Seguridad<br>• Clasificación de activos de información y aplicación de procedimientos de manejo<br>• Seguridad en el intercambio de información<br>Controles sobre los terceros |

| NIVEL DE ACEPTACIÓN | CONTROL |
|---|---|
| Moderada | A.9.2.1 Registro y cancelación de usuarios |
| **VULNERABILIDADES** | **PROYECTOS** |
| • Falta de controles de acceso a carpetas compartidas | • Implementación y seguimiento de Políticas de Seguridad<br>• Gestión del acceso lógico<br>• Revisión y ajustes de perfiles en aplicaciones, servicios de red y recursos tecnológicos<br>• Documentación y mantenimiento de procedimientos operativos |

| NIVEL DE ACEPTACIÓN | CONTROL |
|---|---|
| Moderada | A.9.2.2 Asignación de acceso a usuarios |
| **VULNERABILIDADES** | **PROYECTOS** |
| • Falta de controles de acceso a carpetas compartidas | • Implementación y seguimiento de Políticas de Seguridad<br>• Gestión del acceso lógico<br>• Revisión y ajustes de perfiles en aplicaciones, servicios de red y recursos tecnológicos<br>• Documentación y mantenimiento de procedimientos operativos |

| NIVEL DE ACEPTACIÓN | CONTROL |
|---|---|
| Moderada | A.9.2.3 Gestión de derechos de acceso privilegiados |
| **VULNERABILIDADES** | **PROYECTOS** |
| • Falta de controles de acceso a carpetas compartidas | • Implementación y seguimiento de Políticas de Seguridad<br>• Gestión del acceso lógico<br>• Revisión y ajustes de perfiles en aplicaciones, servicios de red y recursos tecnológicos<br>• Documentación y mantenimiento de procedimientos operativos |

| NIVEL DE ACEPTACIÓN | CONTROL |
|---|---|
| Moderada<br>Baja | A.9.2.4 Gestión de información de autenticación de usuarios |

| VULNERABILIDADES | PROYECTOS |
|---|---|
| • Debilidad en las contraseñas<br>• Falta de controles de acceso a carpetas compartidas | • Implementación y seguimiento de Políticas de Seguridad<br>• Gestión del acceso lógico<br>• Revisión y ajustes de perfiles en aplicaciones, servicios de red y recursos tecnológicos<br>• Documentación y mantenimiento de procedimientos operativos |

| NIVEL DE ACEPTACIÓN | CONTROL |
|---|---|
| Moderada | A.9.2.5 Revisión de los derechos de acceso de los usuarios |
| **VULNERABILIDADES** | **PROYECTOS** |
| • Falta de monitoreo de privilegios | • Implementación y seguimiento de Políticas de Seguridad<br>• Gestión del acceso lógico<br>• Revisión y ajustes de perfiles en aplicaciones, servicios de red y recursos tecnológicos<br>• Documentación y mantenimiento de procedimientos operativos |

| NIVEL DE ACEPTACIÓN | CONTROL |
|---|---|
| Moderada | A.9.2.6 Remoción o ajuste de derechos de acceso |
| **VULNERABILIDADES** | **PROYECTOS** |
| • Falta de controles en la desvinculación o cambio de cargo | • Implementación y seguimiento de Políticas de Seguridad<br>• Controles sobre los funcionarios desde la vinculación hasta la desvinculación<br>• Gestión del acceso lógico<br>• Revisión y ajustes de perfiles en aplicaciones, servicios de red y recursos tecnológicos<br>• Controles sobre los terceros |

| NIVEL DE ACEPTACIÓN | CONTROL |
|---|---|
| Moderada | A.9.3.1 Uso de la información de autenticación |
| **VULNERABILIDADES** | **PROYECTOS** |
| • Debilidad en las contraseñas<br>• Falta de controles de acceso a carpetas compartidas | • Implementación y seguimiento de Políticas de Seguridad<br>• Gestión del acceso lógico |

| NIVEL DE ACEPTACIÓN | CONTROL |
|---|---|
| Moderada | A.9.4.1 Restricción de acceso a la información |
| **VULNERABILIDADES** | **PROYECTOS** |

| | |
|---|---|
| • Falta de controles de acceso a carpetas compartidas | • Implementación y seguimiento de Políticas de Seguridad<br>• Clasificación de activos de información y aplicación de procedimientos de manejo<br>• Gestión del acceso lógico<br>• Revisión y ajustes de perfiles en aplicaciones, servicios de red y recursos tecnológicos |

| NIVEL DE ACEPTACIÓN | CONTROL |
|---|---|
| Moderada | A.9.4.2 Procedimientos de autenticación segura |
| **VULNERABILIDADES** | **PROYECTOS** |
| • Falta de controles de acceso a carpetas compartidas | • Implementación y seguimiento de Políticas de Seguridad<br>• Gestión del acceso lógico |

| NIVEL DE ACEPTACIÓN | CONTROL |
|---|---|
| Moderada | A.10.1.1 Política de Controles Criptográficos |
| **VULNERABILIDADES** | **PROYECTOS** |
| • Falta de cifrado de información | • Implementación y seguimiento de Políticas de Seguridad |

| NIVEL DE ACEPTACIÓN | CONTROL |
|---|---|
| Moderada | A.10.1.2 Administración de Llaves |
| **VULNERABILIDADES** | **PROYECTOS** |
| • Falta de cifrado de información | • Implementación de controles criptográficos |

| NIVEL DE ACEPTACIÓN | CONTROL |
|---|---|
| Extrema | A.11.1.1 Perímetro de Seguridad Física |
| **VULNERABILIDADES** | **PROYECTOS** |
| • Falta de controles de acceso físico<br>• Falta de monitoreo de acceso físico | • Implementación y seguimiento de Políticas de Seguridad<br>• Gestión de acceso físico<br>• Análisis de vulnerabilidades de las personas<br>• Gestión de incidentes<br>• Monitoreo de la gestión del acceso físico |

| NIVEL DE ACEPTACIÓN | CONTROL |
|---|---|
| Moderada | A.11.1.2 Controles de Acceso Físico |

| VULNERABILIDADES | PROYECTOS |
|---|---|
| • Falta de controles de acceso físico<br>• Falta de monitoreo de acceso físico<br>• Falta de protección de acceso físico al cableado de red o los dispositivos | • Implementación y seguimiento de Políticas de Seguridad<br>• Gestión de acceso físico<br>• Análisis de vulnerabilidades de las personas<br>• Documentación y mantenimiento de procedimientos operativos<br>• Gestión de incidentes<br>• Monitoreo de la gestión del acceso físico |

| NIVEL DE ACEPTACIÓN | CONTROL |
|---|---|
| Moderada | A.11.1.3 Seguridad de oficinas, recintos e instalaciones |
| **VULNERABILIDADES** | **PROYECTOS** |
| • Falta de controles de acceso físico<br>• Falta de monitoreo de acceso físico<br>• Falta de protección de acceso físico al cableado de red o los dispositivos | • Implementación y seguimiento de Políticas de Seguridad<br>• Gestión de acceso físico<br>• Análisis de vulnerabilidades de las personas<br>• Documentación y mantenimiento de procedimientos operativos<br>• Gestión de incidentes<br>• Monitoreo de la gestión del acceso físico |

| NIVEL DE ACEPTACIÓN | CONTROL |
|---|---|
| Extrema<br>Moderada | A.11.1.4 Protección contra amenazas externas y ambientales |
| **VULNERABILIDADES** | **PROYECTOS** |
| • Condiciones ambientales insuficientes<br>• Falta de monitoreo de las condiciones ambientales | • Implementación y seguimiento de Políticas de Seguridad<br>• Concientización y educación<br>• Establecimiento y monitoreo de condiciones ambientales para centros de datos<br>• Establecimiento y monitoreo de condiciones ambientales para sitios de archivo<br>• Documentación y mantenimiento de procedimientos operativos |

| NIVEL DE ACEPTACIÓN | CONTROL |
|---|---|
| Moderada | A.11.1.5 Trabajo en áreas seguras |
| **VULNERABILIDADES** | **PROYECTOS** |
| • Falta de controles de acceso físico<br>• Falta de monitoreo de acceso físico | • Implementación y seguimiento de Políticas de Seguridad<br>• Gestión de acceso físico<br>• Análisis de vulnerabilidades de las personas<br>• Gestión de incidentes<br>• Monitoreo de la gestión del acceso físico |

| NIVEL DE ACEPTACIÓN | CONTROL |
|---|---|
| Moderada | A.11.1.6 Áreas de carga y descarga |
| **VULNERABILIDADES** | **PROYECTOS** |
| • Falta de controles de acceso físico<br>• Falta de monitoreo de acceso físico | • Implementación y seguimiento de Políticas de Seguridad<br>• Gestión de acceso físico<br>• Análisis de vulnerabilidades de las personas<br>• Documentación y mantenimiento de procedimientos operativos<br>• Gestión de incidentes<br>• Monitoreo de la gestión del acceso físico |

| NIVEL DE ACEPTACIÓN | CONTROL |
|---|---|
| Moderada<br>Baja | A.11.2.1 Ubicación y protección de los equipos |
| **VULNERABILIDADES** | **PROYECTOS** |
| • Falta de consideraciones para la ubicación de los equipos<br>• Falta de consideraciones de seguridad para la ubicación de los equipos | • Implementación y seguimiento de Políticas de Seguridad<br>• Concientización y educación<br>• Gestión de acceso físico<br>• Análisis de vulnerabilidades de las personas<br>• Seguridad en la reutilización de los equipos<br>• Documentación y mantenimiento de procedimientos operativos<br>• Aseguramiento de plataforma: Estaciones de usuario<br>• Monitoreo de la gestión del acceso físico |

| NIVEL DE ACEPTACIÓN | CONTROL |
|---|---|
| Moderada | A.11.2.2 Utilidades de soporte |
| **VULNERABILIDADES** | **PROYECTOS** |
| • Abastecimiento de energía eléctrica inestable | • Implementación y seguimiento de Políticas de Seguridad<br>• Mantenimiento y pruebas de utilidades de soporte y equipos de computo<br>• Controles sobre los terceros |

| NIVEL DE ACEPTACIÓN | CONTROL |
|---|---|
| Moderada | A.11.2.3 Seguridad del Cableado |
| **VULNERABILIDADES** | **PROYECTOS** |
| • Falta de protección de acceso físico al cableado de red o los dispositivos | • Implementación y seguimiento de Políticas de Seguridad<br>• Controles sobre los terceros |

| NIVEL DE ACEPTACIÓN | CONTROL |
|---|---|
| Moderada | A.11.2.4 Mantenimiento de los Equipos |
| **VULNERABILIDADES** | **PROYECTOS** |
| • Falta de mantenimiento | • Implementación y seguimiento de Políticas de Seguridad<br>• Mantenimiento y pruebas de utilidades de soporte y equipos de computo<br>• Controles sobre los terceros |

| NIVEL DE ACEPTACIÓN | CONTROL |
|---|---|
| Moderada<br>Baja | A.11.2.5 Retiro de activos |
| **VULNERABILIDADES** | **PROYECTOS** |
| • Falta de controles en el traslado | • Implementación y seguimiento de Políticas de Seguridad<br>• Seguridad en la reutilización de los equipos<br>• Seguridad de los equipos fuera de las instalaciones<br>• Documentación y mantenimiento de procedimientos operativos |

| NIVEL DE ACEPTACIÓN | CONTROL |
|---|---|
| Moderada | A.11.2.6 Seguridad de los equipos y activos fuera de las instalaciones |
| **VULNERABILIDADES** | **PROYECTOS** |
| • Falta de controles en el traslado | • Implementación de controles criptográficos<br>• Seguridad de los equipos fuera de las instalaciones |

| NIVEL DE ACEPTACIÓN | CONTROL |
|---|---|
| Moderada | A.11.2.7 Disposición o reutilización segura de los equipos |
| **VULNERABILIDADES** | **PROYECTOS** |
| • Falta de controles en la disposición final | • Implementación y seguimiento de Políticas de Seguridad<br>• Seguridad en la reutilización de los equipos |

| NIVEL DE ACEPTACIÓN | CONTROL |
|---|---|
| Moderada | A.11.2.8 Equipos desatendidos |
| **VULNERABILIDADES** | **PROYECTOS** |
| • Falta de controles de bloqueo | • Implementación y seguimiento de Políticas de Seguridad<br>• Gestión del acceso lógico |

| NIVEL DE ACEPTACIÓN | CONTROL |
|---|---|
| Moderada | A.12.1.1 Procedimientos operativos documentados |
| **VULNERABILIDADES** | **PROYECTOS** |
| • Falta de documentación | • Implementación y seguimiento de Políticas de Seguridad<br>• Documentación y mantenimiento de procedimientos operativos |

| NIVEL DE ACEPTACIÓN | CONTROL |
|---|---|
| Moderada<br>Baja | A.12.1.2 Gestión del Cambio |
| **VULNERABILIDADES** | **PROYECTOS** |
| • Falta de controles sobre la gestión del cambio | • Implementación y seguimiento de Políticas de Seguridad<br>• Documentación y mantenimiento de procedimientos operativos<br>• Gestión del cambio |

| NIVEL DE ACEPTACIÓN | CONTROL |
|---|---|
| Moderada<br>Baja | A.12.1.3 Gestión de la Capacidad |
| **VULNERABILIDADES** | **PROYECTOS** |
| • Falta de planes de capacidad | • Implementación y seguimiento de Políticas de Seguridad<br>• Documentación y mantenimiento de procedimientos operativos<br>• Gestión de la capacidad |

| NIVEL DE ACEPTACIÓN | CONTROL |
|---|---|
| Moderada<br>Baja | A.12.2.1 Protección contra código malicioso |
| **VULNERABILIDADES** | **PROYECTOS** |
| • Falta de software de antivirus | • Implementación y seguimiento de Políticas de Seguridad<br>• Concientización y educación<br>• Documentación y mantenimiento de procedimientos operativos<br>• Análisis de vulnerabilidades técnicas<br>• Definición de estándares de seguridad<br>• Aseguramiento de plataforma: Redes, servidores, bases de datos<br>• Aseguramiento de plataforma: Estaciones de usuario |

| NIVEL DE ACEPTACIÓN | CONTROL |
|---|---|
| | A.12.3.1 Copias de seguridad de la Información |

| | |
|---|---|
| Moderada | |
| | |
| **VULNERABILIDADES** | **PROYECTOS** |
| • Falta de copias de seguridad | • Implementación y seguimiento de Políticas de Seguridad<br>• Generación y verificación de las copias de respaldo |

| **NIVEL DE ACEPTACIÓN** | **CONTROL** |
|---|---|
| | A.12.4.1 Registros de eventos |
| Moderada | |
| | |
| **VULNERABILIDADES** | **PROYECTOS** |
| • Falta de generación y monitoreo de registros de auditoría | • Implementación y seguimiento de Políticas de Seguridad<br>• Gestión de Registros de auditoría |

| **NIVEL DE ACEPTACIÓN** | **CONTROL** |
|---|---|
| | A.12.4.2 Protección de los registros de auditoría |
| Moderada | |
| | |
| **VULNERABILIDADES** | **PROYECTOS** |
| • Falta de generación y monitoreo de registros de auditoría | • Implementación y seguimiento de Políticas de Seguridad<br>• Gestión de Registros de auditoría |

| **NIVEL DE ACEPTACIÓN** | **CONTROL** |
|---|---|
| | A.12.4.3 Registros de administradores y operadores |
| Moderada | |
| | |
| **VULNERABILIDADES** | **PROYECTOS** |
| • Falta de generación y monitoreo de registros de auditoría | • Implementación y seguimiento de Políticas de Seguridad<br>• Gestión de Registros de auditoría |

| **NIVEL DE ACEPTACIÓN** | **CONTROL** |
|---|---|
| | A.12.4.4 Sincronización de reloj |
| Moderada | |
| Baja | |
| **VULNERABILIDADES** | **PROYECTOS** |
| • Falta de sincronización con reloj de tiempo | • Implementación y seguimiento de Políticas de Seguridad<br>• Gestión de Registros de auditoría<br>• Aseguramiento de plataforma: Redes, servidores, bases de datos |

| **NIVEL DE ACEPTACIÓN** | **CONTROL** |
|---|---|
| | A.12.5.1 Instalación de software en los sistemas operativos |
| Moderada | |

| VULNERABILIDADES | PROYECTOS |
|---|---|
| • Falta de actualización de versiones o parches | • Documentación y mantenimiento de procedimientos operativos<br>• Gestión del cambio |

| NIVEL DE ACEPTACIÓN | CONTROL |
|---|---|
| Moderada<br>Baja | A.12.6.1 Gestión de vulnerabilidades técnicas |
| **VULNERABILIDADES** | **PROYECTOS** |
| • Configuración débil y/o por defecto | • Implementación y seguimiento de Políticas de Seguridad<br>• Análisis de vulnerabilidades técnicas |

| NIVEL DE ACEPTACIÓN | CONTROL |
|---|---|
| Moderada<br>Baja | A.12.6.2 Restricciones en la instalación de software |
| **VULNERABILIDADES** | **PROYECTOS** |
| • Falta de actualización de versiones o parches<br>• Falta de controles sobre el software descargado de Internet | • Implementación y seguimiento de Políticas de Seguridad<br>• Gestión del acceso lógico<br>• Revisión y ajustes de perfiles en aplicaciones, servicios de red y recursos tecnológicos |

| NIVEL DE ACEPTACIÓN | CONTROL |
|---|---|
| Moderada<br>Baja | A.13.1.1 Controles de Red |
| **VULNERABILIDADES** | **PROYECTOS** |
| • Falta de controles sobre el software descargado de Internet<br>• Puertos abiertos | • Implementación y seguimiento de Políticas de Seguridad<br>• Documentación y mantenimiento de procedimientos operativos<br>• Definición de estándares de seguridad<br>• Aseguramiento de plataforma: Redes, servidores, bases de datos<br>• Segmentación de red a nivel de comunicaciones (routers, switch) y configuración de dispositivos de seguridad (Firewall, IDS, IPS)<br>• Definición de la arquitectura técnica de seguridad<br>• Revisión y ajuste de los dispositivos de seguridad (Firewall, IDS, IPS)<br>• Verificación y ajustes sobre la arquitectura técnica de seguridad<br>• Estrategia de migración IPv4 a IPv6 |

| NIVEL DE ACEPTACIÓN | CONTROL |
|---|---|
| Moderada | A.13.2.4 Acuerdos de confidencialidad o no divulgación |

| VULNERABILIDADES | PROYECTOS |
|---|---|
| • Falta de controles en la vinculación | • Implementación y seguimiento de Políticas de Seguridad<br>• Concientización y educación<br>• Controles sobre los funcionarios desde la vinculación hasta la desvinculación<br>• Controles sobre los terceros |

| NIVEL DE ACEPTACIÓN | CONTROL |
|---|---|
| Moderada | A.14.2.2 Procedimientos de control de cambios en sistemas |
| **VULNERABILIDADES** | **PROYECTOS** |
| • Falta de controles sobre la gestión del cambio | • Implementación y seguimiento de Políticas de Seguridad<br>• Control de versiones de código fuente de los sistemas de información<br>• Documentación y mantenimiento de procedimientos operativos<br>• Gestión del cambio |

| NIVEL DE ACEPTACIÓN | CONTROL |
|---|---|
| Moderada | A.16.1.1 Responsabilidades y procedimientos |
| **VULNERABILIDADES** | **PROYECTOS** |
| • Falta de gestión de incidentes de seguridad | • Implementación y seguimiento de Políticas de Seguridad<br>• Concientización y educación<br>• Documentación y mantenimiento de procedimientos operativos<br>• Gestión de incidentes |

| NIVEL DE ACEPTACIÓN | CONTROL |
|---|---|
| Moderada | A.16.1.2 Reporte de los eventos de seguridad de la información |
| **VULNERABILIDADES** | **PROYECTOS** |
| • Falta de gestión de incidentes de seguridad | • Implementación y seguimiento de Políticas de Seguridad<br>• Concientización y educación<br>• Gestión de incidentes |

| NIVEL DE ACEPTACIÓN | CONTROL |
|---|---|
| Moderada | A.16.1.3 Reporte de las debilidades de seguridad de la información |
| **VULNERABILIDADES** | **PROYECTOS** |
| • Falta de gestión de incidentes de seguridad | • Implementación y seguimiento de Políticas de Seguridad<br>• Concientización y educación<br>• Gestión de incidentes |

| NIVEL DE ACEPTACIÓN | CONTROL |
|---|---|
| Moderada | A.16.1.4 Evaluación y decisión de los eventos de seguridad de la información |
| **VULNERABILIDADES** | **PROYECTOS** |
| • Falta de gestión de incidentes de seguridad | • Implementación y seguimiento de Políticas de Seguridad<br>• Documentación y mantenimiento de procedimientos operativos<br>• Gestión de incidentes |

| NIVEL DE ACEPTACIÓN | CONTROL |
|---|---|
| Moderada | A.16.1.5 Respuesta a los incidentes de seguridad de la información |
| **VULNERABILIDADES** | **PROYECTOS** |
| • Falta de gestión de incidentes de seguridad | • Implementación y seguimiento de Políticas de Seguridad<br>• Documentación y mantenimiento de procedimientos operativos<br>• Gestión de incidentes |

| NIVEL DE ACEPTACIÓN | CONTROL |
|---|---|
| Moderada | A.16.1.6 Aprendizaje de los Incidentes de Seguridad de la Información |
| **VULNERABILIDADES** | **PROYECTOS** |
| • Falta de gestión de incidentes de seguridad | • Implementación y seguimiento de Políticas de Seguridad<br>• Concientización y educación<br>• Gestión de incidentes |

| NIVEL DE ACEPTACIÓN | CONTROL |
|---|---|
| Moderada | A.16.1.7 Recolección de Evidencia |
| **VULNERABILIDADES** | **PROYECTOS** |
| • Falta de gestión de incidentes de seguridad | • Documentación y mantenimiento de procedimientos operativos<br>• Gestión de incidentes |

| NIVEL DE ACEPTACIÓN | CONTROL |
|---|---|
| Extrema<br>Moderada | A.17.1.1 Planear la seguridad de la información en la continuidad del negocio |
| **VULNERABILIDADES** | **PROYECTOS** |

| | |
|---|---|
| • Continuidad y/o contingencia sin consideraciones de seguridad | • Implementación y seguimiento de Políticas de Seguridad<br>• Ajustes al Plan de Continuidad de Negocio incluyendo consideraciones de seguridad<br>• Contingencia tecnológica |

| NIVEL DE ACEPTACIÓN | CONTROL |
|---|---|
| Moderada | A.17.1.2 Implementar la seguridad de la información en la continuidad del negocio |
| **VULNERABILIDADES** | **PROYECTOS** |
| • Continuidad y/o contingencia sin consideraciones de seguridad | • Implementación y seguimiento de Políticas de Seguridad<br>• Ajustes al Plan de Continuidad de Negocio incluyendo consideraciones de seguridad<br>• Contingencia tecnológica |

| NIVEL DE ACEPTACIÓN | CONTROL |
|---|---|
| Moderada | A.17.1.3 Verificar, revisar y evaluar la seguridad de la información en la continuidad del negocio |
| **VULNERABILIDADES** | **PROYECTOS** |
| • Continuidad y/o contingencia sin consideraciones de seguridad | • Implementación y seguimiento de Políticas de Seguridad<br>• Ajustes al Plan de Continuidad de Negocio incluyendo consideraciones de seguridad<br>• Contingencia tecnológica |

| NIVEL DE ACEPTACIÓN | CONTROL |
|---|---|
| Extrema<br>Moderada | A.17.2.1 Disponibilidad de instalaciones de procesamiento de información |
| **VULNERABILIDADES** | **PROYECTOS** |
| • Falta de instalaciones para continuidad y/o contingencia | • Implementación y seguimiento de Políticas de Seguridad<br>• Contingencia tecnológica |

| NIVEL DE ACEPTACIÓN | CONTROL |
|---|---|
| Baja | A.18.1.2 Derechos de propiedad intelectual |
| **VULNERABILIDADES** | **PROYECTOS** |
| • Falta de control de licenciamiento | • Implementación y seguimiento de Políticas de Seguridad<br>• Gestión del licenciamiento del software |

| NIVEL DE ACEPTACIÓN | CONTROL |
|---|---|
| Moderada | A.18.1.3 Protección de registros |
| **VULNERABILIDADES** | **PROYECTOS** |

| | |
|---|---|
| • Falta de controles de almacenamiento y resguardo<br>• Falta de controles en la disposición final | • Clasificación de activos de información y aplicación de procedimientos de manejo |

| NIVEL DE ACEPTACIÓN | CONTROL |
|---|---|
| Moderada | A.18.2.2 Cumplimiento con políticas y estándares de seguridad |
| **VULNERABILIDADES** | **PROYECTOS** |
| • Configuración débil y/o por defecto | • Implementación y seguimiento de Políticas de Seguridad<br>• Definición de estándares de seguridad<br>• Identificación y actualización de la legislación vigente |

| NIVEL DE ACEPTACIÓN | CONTROL |
|---|---|
| Moderada | A.18.2.3 Revisión del cumplimiento técnico |
| **VULNERABILIDADES** | **PROYECTOS** |
| • Configuración débil y/o por defecto | • Análisis de vulnerabilidades técnicas |

| NIVEL DE ACEPTACIÓN | CONTROL |
|---|---|
| Extrema<br>Moderada | Planes de apoyo al personal |
| **VULNERABILIDADES** | **PROYECTOS** |
| • Coacción<br>• Insatisfacción o circunstancias personales | • Apoyo al personal durante su permanencia |

# 3. PROYECTOS

## 3.1. IMPLEMENTACIÓN Y SEGUIMIENTO DE POLÍTICAS DE SEGURIDAD

### 3.1.1. DESCRIPCIÓN

Tiene el objetivo de llevar a cabo la actualización, implementación y posterior seguimiento a las políticas de seguridad de la información definidas para la Gobernación del Atlántico, con el fin de obtener el compromiso de todos los funcionarios, contratistas, proveedores y terceros frente a la seguridad de la información.

### 3.1.2. ACTIVIDADES A DESARROLLAR

A continuación, se presentan las actividades a desarrollar durante la ejecución de este proyecto:

- Revisar y ajustar la política global de seguridad de la información, las políticas específicas y sus normativas de apoyo.

- Documentar las sanciones aplicables debido al no cumplimiento de las políticas de seguridad de la información.
- Aprobar las políticas y normativas de seguridad de la información ajustadas.
- Divulgar e implementar las políticas y normativas de seguridad de la información una vez aprobadas.
- Dar seguimiento al cumplimiento de las políticas y normativas de seguridad de la información, con el fin de verificar su acatamiento y aceptación por parte de los funcionarios, contratistas y proveedores de la Gobernación.
- Revisar periódicamente las políticas y normativas de seguridad de la información y, realizar ajustes de ser necesario, con el fin de garantizar que son adecuadas y funcionales para la Gobernación del Atlántico.

## 3.2. GENERACIÓN DE LA ORGANIZACIÓN DE SEGURIDAD

### 3.2.1. DESCRIPCIÓN

Este proyecto Tiene como propósito establecer los roles y responsabilidades encargados de la seguridad de la información en Gobernación del Atlántico desde el nivel directivo hasta el operativo.

### 3.2.2. ACTIVIDADES A DESARROLLAR

A continuación, se presentan las actividades a desarrollar durante la ejecución de este proyecto:

- Verificar si existe un comité o grupo responsable de la seguridad de la información que cuente con funciones explicitas respecto a la generación de los lineamientos en seguridad de la información, aprobación de la documentación y estrategias generadas para la operación del Sistema de Gestión de Seguridad de la Información (SGSI).
- Fortalecer y reasignar funciones al grupo de trabajo encargado de liderar los aspectos tácticos y operativos relacionados con la seguridad de la información.
- Fortalecer las funciones relacionadas con mantener la seguridad de la información en el ciclo de vida de la gestión de proyectos.
- Dar a conocer a las áreas o grupos de trabajo con responsabilidad indirecta sobre temas relacionados con seguridad de la información sus responsabilidades, de acuerdo con lo establecido por la norma ISO/IEC 27001:2013. Estas áreas son, pueden ser entre otras: Talento Humano y la Seguridad Física, Control Interno (en relación con las auditorias y revisiones al SGSI).
- Documentar formalmente la organización de seguridad de la información en la Gobernación del Atlántico y divulgar las responsabilidades a los comités, áreas o grupos de trabajo involucrados.

## 3.3. VERIFICACIÓN Y ACTUALIZACIÓN DE FUNCIONES Y RESPONSABILIDADES

### 3.3.1. DESCRIPCIÓN

Este proyecto tiene como propósito verificar y actualizar las funciones y responsabilidades de los funcionarios, contratistas y personal provisto por terceros, en donde además de las funciones y responsabilidades del cargo, se incluyan aspectos relacionados con la seguridad de la información de acuerdo con las políticas y normativas de seguridad de la información existentes y considerando aspectos como la información de eventos de seguridad y la protección de los activos de información contra el acceso, divulgación, modificación y destrucción no autorizados.

### 3.3.2. ACTIVIDADES A DESARROLLAR

A continuación, se presentan las actividades a desarrollar durante la ejecución de este proyecto:

- Verificar que las funciones y responsabilidades de funcionarios, contratistas y terceros se encuentran alineadas con las políticas de seguridad de la información, considerando la revisión y actualización periódica de las mismas.

- Realizar una revisión y de ser necesario actualización a la normativa y procedimientos de seguridad de la información respecto a los roles y responsabilidades del personal, considerando la posible concentración de funciones.

- Comprobar que las responsabilidades de la alta dirección se encuentren definidas de acuerdo con su compromiso con el Sistema de Gestión de Seguridad de la Información.

- Divulgar los roles y responsabilidades de funcionarios, contratistas y terceros con la seguridad de la información de la Gobernación del Atlántico.

## 3.4. REVISIÓN Y AJUSTES DE PERFILES EN APLICACIONES, SERVICIOS DE RED Y RECURSOS TECNOLÓGICOS

### 3.4.1. DESCRIPCIÓN

Tiene como objetivo asegurar que todo el personal con acceso a los sistemas de información, servicios de red, y cualquier recurso de la plataforma tecnológica de la Gobernación del Atlántico, cuente con un perfil acorde a las labores y funciones que desempeña.

### 3.4.2. ACTIVIDADES A DESARROLLAR

A continuación, se presentan las actividades a desarrollar durante la ejecución de este proyecto:

- Revisar los perfiles y roles de acceso lógico de usuarios o grupos de usuarios, de acuerdo con las funciones de cargo y las políticas de seguridad de la información en cada uno de los sistemas de información existentes, servicios de red y recursos tecnológicos, con fin de ratificar o de ser necesario ajustar, los perfiles y roles de acuerdo con los cambios detectados durante la revisión.

- Llevar a cabo cuando resulte necesario, el ajuste de los roles y perfiles de usuarios, siguiendo los procedimientos definidos para tal fin. Se recomienda generar evidencia documentada de acuerdo de este tipo de cambios, de acuerdo con los formatos o registros existentes.

- Evaluar en conjunto con el área de Recursos Humanos y los Jefes de área, posibles ajustes o actualizaciones sobre las labores y funciones del personal en base a las revisiones y ajustes de perfiles y roles de acceso lógico.

## 3.5. NOTIFICACIÓN A TERCERAS PARTES

### 3.5.1. DESCRIPCIÓN

Su propósito es establecer criterios para el contacto con terceras partes cuando así lo requiera la aplicación de los controles del Sistema de Gestión de Seguridad de la Información.

### 3.5.2. ACTIVIDADES A DESARROLLAR

A continuación, se presentan las actividades a desarrollar durante la ejecución de este proyecto:

- Establecer el rol responsable del contacto con terceros o autoridades en caso que exista un compromiso a la confidencialidad, integridad o disponibilidad de los activos de información de la Gobernación del Atlántico.

- Definir lineamientos que establezcan cuando y como se deben reportar eventos de seguridad de la información a terceros.

- Actualizar el listado de contactos, en busca de tener en cuenta organismos de control, empresas de servicios públicos, servicios de emergencia y proveedores críticos para continuidad de las operaciones.

## 3.6. CONTROLES SOBRE LOS FUNCIONARIOS DESDE LA VINCULACIÓN HASTA LA DESVINCULACIÓN

### 3.6.1. DESCRIPCIÓN

Busca que los funcionarios y contratistas de la Gobernación del Atlántico, conozcan la importancia de la seguridad de la información, y de sus funciones y responsabilidades con ella desde el momento de su vinculación, durante su permanencia y hasta el momento de su desvinculación.

### 3.6.2. ACTIVIDADES A DESARROLLAR

A continuación, se presentan las actividades a desarrollar durante la ejecución de este proyecto:

- Identificar desde el proceso de vinculación de personal el tipo de información y el nivel de clasificación al que el funcionario o contratista tendrá acceso y los posibles riesgos derivados.

- Establecer controles adicionales de acuerdo con el nivel de clasificación de la información a la que el colaborador tendrá acceso, en la medida en que la regulación lo permita, los controles podrían ser estudios de seguridad, pruebas de polígrafo, entre otros; estos controles deben ejecutarse en el momento de la vinculación y repetirse de manera periódica.

- Definir métricas para evaluar la efectividad de los lineamentos existentes para la entrega de información, derechos de acceso, puestos de trabajo y bienes, durante la desvinculación o cambio de cargo de funcionarios y contratistas, en busca de establecer posibles oportunidades de mejora.

- Establecer que en el proceso de desvinculación de personal, se debe notificar a los funcionarios y contratistas que las responsabilidades frente a la seguridad de la información de la Gobernación del Atlántico continúan existiendo.

## 3.7. CONCIENTIZACIÓN Y EDUCACIÓN

### 3.7.1. DESCRIPCIÓN

Llevar a cabo una concienciación y educación realizada por personal interno o externo, con el fin que todos los funcionarios, contratistas, proveedores y terceros de la Gobernación del Atlántico tomen conciencia frente a la importancia de la seguridad de la información dentro de sus actividades y, como sus acciones contribuyen a optimizar la seguridad de la información.

### 3.7.2. ACTIVIDADES A DESARROLLAR

A continuación, se presentan las actividades a desarrollar durante la ejecución de este proyecto:

- Elaborar un programa de concienciación de seguridad de la información; dicho programa debe considerar que en cada periodo de concienciación y educación se cubran grupos objetivo y temarios específicos, iniciando por grupos de usuario final, hasta alcanzar grupos con conocimientos en seguridad de la información y la Alta Dirección de la Gobernación.

- Desarrollar el programa de concienciación de seguridad de la información para el periodo en vigencia, a través de la realización de charlas, folletos, fondos de pantalla, pendones u otra herramienta que se considere, para posteriormente medir su efectividad en cada uno de los grupos objetivo que reflejen los niveles conciencia en seguridad de la información.

- Revisar periódicamente el nivel de conciencia de los funcionarios, contratistas, proveedores y terceros, a través de métricas, con el fin de identificar la necesidad de reforzar las charlas, sesiones de trabajo, talleres y herramientas utilizadas.

## 3.8. APOYO AL PERSONAL DURANTE SU PERMANENCIA

### 3.8.1. DESCRIPCIÓN

Tiene como objetivo establecer las actividades necesarias para proteger al personal de la Gobernación del Atlántico en caso de coacción, amenaza o extorsión durante su vigencia laboral.

### 3.8.2. ACTIVIDADES A DESARROLLAR

A continuación, se presentan las actividades a desarrollar durante la ejecución de este proyecto:

- Establecer y documentar un plan de acción ante casos de coacción, amenaza o extorsión al personal; dicho plan debe considerar el contacto con las autoridades correspondientes.
- Divulgar a todo el personal el plan de acción establecido.
- Conformar un grupo interdisciplinario de apoyo para atender casos de coacción, amenaza o extorsión reportados, aplicando el plan de acción establecido por la Gobernación.
- Instruir al personal responsable sobre cómo se debe aplicar el plan de acción y de ser posible llevar cabo simulacros de ejecución.

## 3.9. GENERACIÓN DE LA GUÍA DE CLASIFICACIÓN DE LA INFORMACIÓN Y LOS PROCEDIMIENTOS DE MANEJO

### 3.9.1. DESCRIPCIÓN

El objetivo es generar los lineamientos para llevar a cabo el proceso de clasificación de información, de acuerdo con su grado de sensibilidad e importancia, definiendo guías de clasificación y un conjunto de procedimientos de manejo de la información para la Gobernación del Atlántico.

### 3.9.2. ACTIVIDADES A DESARROLLAR

A continuación, se presentan las actividades a desarrollar durante la ejecución de este proyecto:

- Definir los criterios de seguridad de la información (confidencialidad, integridad y disponibilidad) por los cuales será clasificada la información.
- Verificar la legislación vigente en temas de clasificación de la información y, de acuerdo con ella, definir los niveles o categorías en los cuales será clasificada la información en relación con su nivel de sensibilidad.

- Generar guías o metodologías de clasificación de la información donde se presenten las categorías de clasificación de la información.

- Especificar para cada categoría de clasificación de información procedimientos de manejo que incluyan, entre otros, acceso, procesamiento, almacenamiento, transmisión, destrucción segura y etiquetado, considerando las tablas de retención documental existentes para la Gobernación.

- Divulgar las guías de clasificación de la información y procedimientos de manejo.

## 3.10. CLASIFICACIÓN DE ACTIVOS DE INFORMACIÓN Y APLICACIÓN DE PROCEDIMIENTOS DE MANEJO

### 3.10.1. DESCRIPCIÓN

El objetivo es identificar y clasificar los activos de información definidos como alcance para la Gobernación del Atlántico utilizando la normativa existente y, una vez clasificada la información, aplicar los procedimientos de manejo establecidos.

### 3.10.2. ACTIVIDADES A DESARROLLAR

A continuación se presentan las actividades a desarrollar durante la ejecución de este proyecto:

- Instruir al personal sobre la normativa existente para la clasificación de los activos de información, considerado la tipología de los activos.

- Definir un plan de clasificación de activos, con alcance, tiempos y responsabilidades.

- Clasificar y etiquetar los activos de información de acuerdo con el plan definido y de acuerdo con la normativa para la clasificación de información.

- Implantar los procedimientos de manejo establecidos para la información clasificada en cada una de las áreas o procesos.

## 3.11. GENERACIÓN Y VERIFICACIÓN DE LAS COPIAS DE RESPALDO

### 3.11.1. DESCRIPCIÓN

Busca mantener la integridad y disponibilidad de la información a través de la generación de copias de respaldo y pruebas de restauración de estas, con el fin de garantizar que la información se lograría recuperar después de un desastre o falla que afecte la plataforma tecnológica de la Gobernación del Atlántico.

### 3.11.2. ACTIVIDADES A DESARROLLAR

A continuación se presentan las actividades a desarrollar durante la ejecución de este proyecto:

- Establecer los lineamientos o mecanismos para la restricción de medios no autorizados.
- Elaborar el procedimiento de copias de respaldo junto a un formato asociado en el cual se deben consignar los registros de dichas copias.
- Divulgar y establecer el procedimiento de copias de respaldo junto con el formato asociado.
- Definir la frecuencia de generación de copias de respaldo considerando aspectos como los requisitos de seguridad de la información involucrada y la importancia de la continuidad en la operación.
- Definir el sitio de custodia externa y, de ser necesario, suscribir los contratos o convenios para dicha custodia.
- Establecer períodos para realizar pruebas de restauración de información aleatorias a partir de las copias de respaldo.
- Determinar el tiempo de retención de las copias de respaldo teniendo en cuenta la importancia de la información respaldada y los requisitos legales y de negocio que rigen la Gobernación.
- Evaluar la necesidad de instaurar controles criptográficos a las copias de respaldo, considerando los requisitos legales o de negocio aplicables.

## 3.12. GESTIÓN DEL ACCESO LÓGICO

### 3.12.1. DESCRIPCIÓN

El objetivo es establecer una gestión adecuada del acceso lógico en la plataforma tecnológica y los sistemas de información, con el fin de proteger los servicios de procesamiento y almacenamiento de información.

### 3.12.2. ACTIVIDADES A DESARROLLAR

A continuación se presentan las actividades a desarrollar durante la ejecución de este proyecto:

- Establecer lineamientos para la entrega formal de usuarios y contraseñas, y en dicha entrega dejar evidencia que los usuarios conocen y aceptan sus responsabilidades con el manejo de dicha información.
- Ajustar los controles de acceso lógico correspondientes de acuerdo con lo establecido en la normativa y políticas de seguridad de la información.
- Aplicar la normativa de control de acceso existente.

- Establecer y documentar los perfiles y roles de acceso lógico de usuarios o grupos de usuarios, considerando segregación de funciones, privilegios de descarga de software y limitación de accesos a utilidades o funcionalidades según necesidad de uso, de acuerdo con sus funciones y las políticas de seguridad de la información.

## 3.13. GESTIÓN DE ACCESO FÍSICO

### 3.13.1. DESCRIPCIÓN

El objetivo es establecer una gestión adecuada del acceso físico para las instalaciones de Gobernación del Atlántico, con el fin de proteger las áreas de almacenamiento y procesamiento de información.

### 3.13.2. ACTIVIDADES A DESARROLLAR

A continuación se presentan las actividades a desarrollar durante la ejecución de este proyecto:

- Identificar las áreas que pueden considerarse restringidas, teniendo en cuenta el tipo de información que se almacena o procesa y la sensibilidad de dicha información.

- Evaluar y ajustar los controles de acceso físico existentes, considerando aspectos como las labores correspondientes al cargo y las políticas de seguridad de la información, para las diferentes áreas, especialmente para las áreas identificadas como sensibles, con el fin de permitir acceso solo a personal autorizado.

- Implementar el procedimiento de control de acceso físico, con el fin de establecer controles sobre el acceso físico y generar registros.

- Monitorear, de manera periódica, la efectividad de los controles de acceso físico establecidos, con el objetivo de generar propuestas de mejora de acuerdo con las políticas de seguridad de la información y los análisis de riesgos realizados.

## 3.14. MONITOREO DE LA GESTIÓN DEL ACCESO FÍSICO

### 3.14.1. DESCRIPCIÓN

El objetivo de este proyecto es realizar seguimiento a la gestión del acceso físico para las instalaciones de la Gobernación del Atlántico, con el fin de verificar que se esté llevando a cabo la protección de las áreas que contienen información y servicios de procesamiento de la misma.

### 3.14.2. ACTIVIDADES A DESARROLLAR

A continuación se presentan las actividades a desarrollar durante la ejecución de este proyecto:

- Evaluar la viabilidad de la aplicación de las siguientes consideraciones:

    - Realizar inspección de los bolsos, maletas o carteras de todo el personal que acceda a las instalaciones, sin importar si es hombre o mujer, especialmente antes del acceso en áreas de carácter restringido como lo es el Data Center o las Oficinas de la Secretaría de Informática y Telecomunicaciones.

    - Establecer restricciones para el acceso de activos (USB, cd, discos duros, cámaras, celulares, entro otros) por parte de visitantes que accedan en áreas de carácter restringido como lo es el Data Center; en caso de no ser posible la restricción total, se recomienda contar con el inventario de activos antes de ingresar, con el fin de verificar su salida de las instalaciones.

    - Todos los visitantes deben contar con una credencial en un lugar visible que los identifique como tal durante su estancia en las instalaciones.

    - Garantizar que las cámaras para el monitoreo de las instalaciones se encuentran funcionales y cuentan con la resolución suficiente para identificar detalles relevantes en posibles eventos de seguridad.

    - Garantizar que el personal encargado del monitoreo de cámaras de las instalaciones es suficiente para velar por la seguridad general de las instalaciones y especial de áreas restringidas o sensibles.

- Generar campañas de divulgación de los lineamientos y procedimientos de control de acceso físico existentes, con el fin de fortalecer la conciencia del personal de seguridad y los funcionarios y terceros de la Gobernación del Atlántico sobre el cumplimiento de los controles existentes.

- Verificar el cumplimiento del personal con los controles y lineamientos de acceso físico establecidos, con el fin de reportar al personal que no dé cumplimiento o en busca de mejorar los controles existentes.

- Inspeccionar y de ser necesario tomar las medidas correctivas para que áreas sensibles como los centros de cableado y el Data Center cuenten con los controles adecuados para impedir el acceso de personal no autorizado.

## 3.15. ANÁLISIS DE VULNERABILIDADES DE LAS PERSONAS

### 3.15.1. DESCRIPCIÓN

Tiene como objetivo realizar un análisis de vulnerabilidades a través de ataques de ingeniería social para la Gobernación del Atlántico, con el fin de identificar brechas de seguridad a nivel de seguridad física, redundando en obtención de información de las personas y de la tecnología de la Gobernación.

### 3.15.2. ACTIVIDADES A DESARROLLAR

A continuación se presentan las actividades a desarrollar durante la ejecución de este proyecto:

- Realizar recopilación de información, con el fin de identificar personal susceptible de ataque, para alcanzar objetivos específicos (servidores, enrutadores, firewalls, accesos externos, entre otros) en las redes que serán objeto del análisis de vulnerabilidades a través de ataques de ingeniería social.

- Efectuar el ataque de ingeniería social utilizando estrategias y herramientas como correo electrónico, llamadas telefónicas, medios de almacenamiento abandonados y acceso a las instalaciones físicas mediante engaños, con el fin de obtener acceso a los objetivos seleccionados, aprovechando las vulnerabilidades del personal y determinando el impacto de las mismas.

- Elaborar un documento donde se informen detalladamente los resultados obtenidos durante todo el proceso de análisis de vulnerabilidades a través de ingeniería social, como las vulnerabilidades detectadas, el impacto de cada una de ellas y las medidas a tomar para su posterior remediación.

## 3.16. GESTIÓN DE INCIDENTES

### 3.16.1. DESCRIPCIÓN

Tiene como propósito que todos los incidentes relacionados con seguridad de la información se comuniquen formalmente, se analicen, se contengan, se investiguen y sean solucionados, tomando las acciones correctivas correspondientes de manera oportuna.

### 3.16.2. ACTIVIDADES A DESARROLLAR

A continuación se presentan las actividades a desarrollar durante la ejecución de este proyecto:

- Divulgar los canales existentes para el reporte de eventos de seguridad de la información.

- Educar al personal sobre los diferentes tipos de eventos que pueden ser reportados y cuando un evento puede convertirse en un incidente de seguridad de la información.

- Establecer los mecanismos que se usaran para la recolección de evidencias.

- Instaurar mecanismos para cuantificar y monitorear todos los tipos, volúmenes y costos de los incidentes de seguridad de la información.

- En la base de conocimiento existente, documentar todos los incidentes presentados y su correspondiente solución, considerando que dicha base debería ser de carácter confidencial y de acceso restringido.

## 3.17. MANTENIMIENTO Y PRUEBAS DE UTILIDADES DE SOPORTE Y EQUIPOS DE COMPUTO

### 3.17.1. DESCRIPCIÓN

El objetivo es la realización de mantenimientos y pruebas en las utilidades de soporte y equipos de cómputo de la Gobernación del Atlántico, con el fin de prevenir fallas de hardware.

### 3.17.2. ACTIVIDADES A DESARROLLAR

A continuación se presentan las actividades a desarrollar durante la ejecución de este proyecto:

- Realizar periódicamente mantenimientos preventivos y, de ser necesarios correctivos, a todas las utilidades de soporte como sistemas de extinción de incendios, UPS, aire acondicionado, plantas eléctricas y cableado estructurado; además, se deben llevar a cabo mantenimientos periódicos a los equipos de cómputo en general.

- Generar registros acorde a los mantenimientos, preventivos o correctivos realizados a las utilidades de soporte y equipos de cómputo, en donde se detalle información relacionada con el mantenimiento, como componentes involucrados, motivo de la realización, fecha y tiempo de duración del mantenimiento.

- Ejecutar periódicamente pruebas a las utilidades de soporte, con el objetivo de garantizar su óptimo funcionamiento; adicionalmente, dichas pruebas deben ser documentadas, detallando siempre los aspectos más relevantes de las mismas.

## 3.18. SEGURIDAD EN LA REUTILIZACIÓN DE LOS EQUIPOS

### 3.18.1. DESCRIPCIÓN

El objetivo es establecer medidas de control seguras para la reutilización de los equipos de cómputo, dispositivos móviles y cualquier medio electrónico que contenga o haya contenido información correspondiente a la Gobernación del Atlántico, con el fin de proteger dicha información.

### 3.18.2. ACTIVIDADES A DESARROLLAR

A continuación se presentan las actividades a desarrollar durante la ejecución de este proyecto:

- Establecer cuáles serán los mecanismos y herramientas para la eliminación de información y reutilización segura de los equipos de cómputo, dispositivos móviles y cualquier medio electrónico que contenga o haya contenido información, considerando métodos como la destrucción física, borrado o sobre-escritura segura y la protección de la información durante la vida útil del dispositivo.

- Establecer un procedimiento que defina las acciones a seguir en caso de eliminación de información o reutilización de un equipo de cómputo, dispositivo móvil y cualquier medio electrónico que contenga o haya contenido información; dicho procedimiento debe generar registros de las actividades realizadas.

## 3.19. GESTIÓN DEL CAMBIO

### 3.19.1. DESCRIPCIÓN

Definir las consideraciones que se deben tener en cuenta para controlar los cambios en los sistemas operativos, servicios de red, aplicativos y sistemas de procesamiento de información de la Gobernación del Atlántico.

### 3.19.2. ACTIVIDADES A DESARROLLAR

A continuación se presentan las actividades a desarrollar durante la ejecución de este proyecto:

- Revisar y de ser necesario ajustar el procedimiento para el control de cambios, considerando que cuente con aspectos como aprobación formal, evaluación de impactos potenciales, registro de cambios, planificación de cambios, operaciones de restauración o rollback, recursos requeridos y pruebas.

- Validar o de ser necesario establecer procedimientos de emergencia que incluyan responsabilidades de cancelación, recuperación o eventos anómalos en la realización de cambios.

- Ejecutar pruebas de seguridad posteriores a los cambios, sin importar si los cambios son regulares o de emergencia.

- Divulgar los procedimientos de control de cambios, con el objetivo de socializar ante las partes interesadas el cómo se deben llevar a cabo los nuevos cambios.

## 3.20. GESTIÓN DE LA CAPACIDAD

### 3.20.1. DESCRIPCIÓN

El objetivo es mantener la capacidad de los recursos tecnológicos en niveles adecuados, considerando aspectos como tiempos de respuesta, necesidades actuales y necesidades futuras para la Gobernación del Atlántico.

### 3.20.2. ACTIVIDADES A DESARROLLAR

A continuación se presentan las actividades a desarrollar durante la ejecución de este proyecto:

- Crear, establecer y mantener un plan de capacidad actualizado que refleje las necesidades presentes y futuras de la Gobernación.

- Verificar periódicamente el uso de los recursos, capacidad y rendimiento de la plataforma tecnológica y de los servicios provistos por esta.

- Evaluar las necesidades de capacidad frente a los servicios tecnológicos prestados y las posibilidades de almacenamiento de dichos servicios y de la información asociada (local, en la nube u otras posibilidades).

- Identificar y remediar los problemas e incidencias de rendimiento y capacidad de la plataforma tecnológica y de los servicios provistos por esta, con el fin de proveer mejoras para la Gobernación.

- Llevar a cabo la administración de la plataforma tecnológica y de los servicios provistos por esta, considerando siempre los objetivos y el impacto de estos, frente a los niveles de rendimiento y capacidad actuales.

- Realizar acciones proactivas con el objetivo de mejorar el rendimiento y la capacidad de la plataforma tecnológica y de los servicios provistos por esta.

- Generar información estadística del uso de recursos y capacidad de la plataforma tecnológica para utilizar como información de base para las proyecciones de capacidad periódicas.

## 3.21. DEFINICIÓN DE ESTÁNDARES DE SEGURIDAD

### 3.21.1. DESCRIPCIÓN

Tiene como objetivo establecer estándares de seguridad, en diferentes componentes de la plataforma tecnológica de la Gobernación del Atlántico.

### 3.21.2. ACTIVIDADES A DESARROLLAR

A continuación se presentan las actividades a desarrollar durante la ejecución de este proyecto:

- Seleccionar estándares de seguridad aplicables a la plataforma tecnológica de la Gobernación del Atlántico, tomando como referencia guías de aseguramiento elaboradas por asociaciones profesionales o institutos con reconocimiento internacional, por ejemplo NIST.

- Ajustar los estándares a las necesidades de la Gobernación del Atlántico y a las características particulares de funcionalidad de la plataforma tecnológica.

- Ejecutar los estándares y realizar pruebas en ambientes provistos para este fin a los componentes de la plataforma tecnológica involucrados.

- Implementar los estándares de acuerdo con los lineamientos de control de cambios y validar el éxito de la puesta en producción de los componentes de la plataforma tecnológica involucrados.

## 3.22. GESTIÓN DE REGISTROS DE AUDITORÍA

### 3.22.1. DESCRIPCIÓN

Tiene como objetivo la gestión de los registros de auditoria y la correlación de eventos de los diferentes componentes de la plataforma tecnológica de la Gobernación del Atlántico.

### 3.22.2. ACTIVIDADES A DESARROLLAR

A continuación se presentan las actividades a desarrollar durante la ejecución de este proyecto:

- Definir y establecer las características de la información a ser contenida en los registros de auditoria de los diferentes componentes de la plataforma tecnológica como servidores, dispositivos de seguridad y dispositivos de comunicaciones, con el fin de garantizar que los registros de auditoria puedan llegar a facilitar actividades de investigación y monitoreo.

- Establecer las herramientas o mecanismos para establecer un repositorio único que permita el análisis de los registros de auditoria previamente definidos para la plataforma tecnológica.

- Establecer el tiempo de retención y los controles de protección adecuados para la conservación de los registros de auditoria, considerando aspectos como la capacidad de los medios donde se almacenan, los tipos de eventos críticos, requerimientos de normas o estándares y los usuarios que cuentan con el perfil adecuado para acceder a ellos.

- Asignar responsabilidades para el monitoreo y revisión de los registros de auditoría.

- Elaborar e implantar procedimientos para el monitoreo, correlación y análisis de los registros de auditoria, de acuerdo con las características y tipo de componente de la plataforma tecnológica y los sistemas de información.

## 3.23. ANÁLISIS DE VULNERABILIDADES TÉCNICAS

### 3.23.1. DESCRIPCIÓN

Realizar un análisis de vulnerabilidades técnicas sobre la plataforma tecnológica de la Gobernación del Atlántico, con el fin de identificar brechas de seguridad a través de la explotación de vulnerabilidades, para que estas conlleven a una posterior reducción de dichas brechas de seguridad, reflejándose en mejoras en la eficacia y eficiencia de los controles.

### 3.23.2. ACTIVIDADES A DESARROLLAR

A continuación se presentan las actividades a desarrollar durante la ejecución de este proyecto:

- Realizar recopilación de información, con el objetivo de identificar objetivos específicos (servidores, enrutadores, firewalls, accesos externos, entre otros) en las redes que serán objeto del análisis de vulnerabilidades técnicas.

- Llevar a cabo un proceso de enumeración, con el fin de obtener y clasificar los posibles vectores de ataque.

- Verificar la adecuada segmentación de las redes parte del alcance, especialmente aquellas que resguardan activos potencialmente sensibles.

- Ejecutar un análisis de la información y resultados del proceso de enumeración, para determinar posibles brechas de seguridad o falsos positivos en los vectores de ataque definidos.

- Efectuar la explotación o ataque a los objetivos seleccionados, aprovechando las vulnerabilidades descubiertas y determinando el impacto de las mismas en los activos donde se encuentran.

- Elaborar un documento donde se informen detalladamente los resultados obtenidos durante todo el proceso de análisis de vulnerabilidades técnicas, como las vulnerabilidades detectadas, el impacto de cada una de ellas y las medidas a tomar para su posterior remediación.

## 3.24. CONTINGENCIA TECNOLÓGICA

### 3.24.1. DESCRIPCIÓN

Tiene como propósito restaurar los servicios de diferentes recursos tecnológicos de forma rápida, eficiente y con el menor costo y pérdidas posibles, tomando como insumos los resultados del análisis de riesgos y del análisis de impacto al negocio (BIA).

### 3.24.2. ACTIVIDADES A DESARROLLAR

A continuación se presentan las actividades a desarrollar durante la ejecución de este proyecto:

- Determinar los servicios de red, sistemas de información y recursos tecnológicos críticos y utilizar los resultados del análisis de riesgos para conocer las principales amenazas a la seguridad y/o operación de dichos servicios, sistemas y recursos.

- Establecer los requisitos de recuperación, a través de un Plan de Respaldo, el cual contempla los controles preventivos antes de que se materialice una amenaza identificada en el análisis de riesgos. Algunas de las principales actividades son:

    - Establecimiento del centro alterno.
    - Establecimiento de contratos de alquiler de equipos, canales alternos de comunicaciones y Acuerdos de Niveles de Servicio.
    - Verificación de la existencia y cubrimiento de las pólizas de seguro.

- Establecimiento de procedimientos de recuperación y vuelta a la normalidad, consistentes con los escenarios y estrategias de recuperación definidos.
- Actualización permanente y mantenimiento del inventario de activos.
- Mantenimientos periódicos a los equipos de cómputo y las utilidades de soporte.
- Realización de copias de respaldo tanto de información como de configuraciones.
- Garantía de custodia externa de las copias de respaldo.
- Revisiones periódicas de las copias de respaldo.
- Simulacros por desastres naturales.
- Simulacros por fallas graves de las comunicaciones o la plataforma tecnológica.

- Definir las acciones a seguir en el evento de una contingencia tecnológica, a través de un Plan de Emergencia, el cual contempla las contramedidas y controles necesarios durante la materialización de una amenaza, o inmediatamente después con el fin de mitigar los efectos adversos de la amenaza, de manera consistente con las estrategias de recuperación establecidas. Entre estas actividades se encuentran:

  - Activación del grupo encargado de la contingencia tecnológica.
  - Activación del centro alterno, canales alternos de comunicaciones y de los contratos de alquiler de equipos informáticos.
  - Gestión de los incidentes informáticos.
  - Re-direccionamiento de las comunicaciones.
  - Restauración de las copias de respaldo según la prioridad de recuperación identificada.
  - Reanudación de las operaciones desde el centro alterno

- Restablecer las operaciones normales, a través de un Plan de Recuperación, el cual contempla las medidas necesarias después de materializada y controlada la amenaza, con el fin de restaurar los servicios de red, sistemas de información y recursos tecnológicos tal y como se encontraban antes de la materialización de la amenaza. Algunas de sus actividades se relacionan a continuación:

  - Evaluación de daños.
  - Traslado de datos desde el centro alterno a las instalaciones habituales.
  - Recuperación y reanudación de las actividades.
  - Desactivación del centro alterno, canales alternos de comunicaciones y de los contratos de alquiler de equipos.
  - Reclamaciones a la compañía de seguros

- Revisar y actualizar los Planes de Contingencia Tecnológica.

## 3.25. VINCULACIÓN A FOROS Y GRUPOS DE INTERÉS

### 3.25.1. DESCRIPCIÓN

Tiene como propósito crear y mantener vínculos con foros y grupos de interés relacionados con seguridad de la

información, estándares internacionales y buenas prácticas, aplicables a la Gobernación del Atlántico.

### 3.25.2. ACTIVIDADES A DESARROLLAR

A continuación se presentan las actividades a desarrollar durante la ejecución de este proyecto:

- Identificar temas de interés relacionados con seguridad de la información, estándares internacionales y buenas prácticas aplicables a la Gobernación.

- Establecer vínculos con foros y grupos de asociaciones profesionales o entidades reconocidas, como por ejemplo ISACA, ISC2 y NIST, de acuerdo con los temas de interés planteados, con el fin de estar siempre actualizados en nuevas tecnologías, productos, estándares, marcos de referencia, buenas practicas, amenazas y vulnerabilidades.

## 3.26. DOCUMENTACIÓN Y MANTENIMIENTO DE PROCEDIMIENTOS OPERATIVOS

### 3.26.1. DESCRIPCIÓN

Tiene como propósito la elaboración, establecimiento y mantenimiento de los procedimientos operativos relacionados con las actividades necesarias para el ejercicio de los aspectos tecnológicos, físicos, administrativos y de operación de la Gobernación del Atlántico.

### 3.26.2. ACTIVIDADES A DESARROLLAR

A continuación se presentan las actividades a desarrollar durante la ejecución de este proyecto:

- Elaborar y/o ajustar la documentación correspondiente a los procedimientos de operación y configuración de los diferentes componentes tecnológicos de la plataforma tecnológica, como encendido y apagado de equipos, generación de copias de respaldo, manejo de medios, gestión de correo electrónico y procedimientos relacionados con seguridad, entre otros.

- Elaborar la documentación correspondiente a los procedimientos de operación de los elementos no tecnológicos, como el procedimiento para el control de acceso físico y demás relacionados con seguridad.

- Establecer los procedimientos de operación elaborados, con el fin de llevar a cabo las actividades propias, tanto de aspectos tecnológicos como no tecnológicos de manera consistente.

- Mantener los procedimientos de operación, a través del monitoreo de su aplicabilidad en los aspectos tecnológicos y no tecnológicos, y de ser necesario generar cambios controlados en ellos.

## 3.27. DEFINICIÓN Y ESTABLECIMIENTO DE ACUERDOS DE NIVELES DE OPERACIÓN

### 3.27.1. DESCRIPCIÓN

Tiene como propósito la definición y establecimiento de acuerdos de niveles de operación, donde se consideren los objetivos y responsabilidades del proveedor de servicios interno y los usuarios clientes de los servicios de la Gobernación del Atlántico.

### 3.27.2. ACTIVIDADES A DESARROLLAR

A continuación se presentan las actividades a desarrollar durante la ejecución de este proyecto:

- Definir el diseño de la estructura de acuerdo de nivel de operación más adecuada para satisfacer las necesidades de la Gobernación, considerando opciones como acuerdos de nivel de operación basados en áreas, procesos y servicios.

- Definir los requisitos del nivel de operación considerando aspectos como soluciones, resultados y objetivos deseados, con el fin de cumplir adecuadamente los acuerdos de nivel de operación.

- Establecer los acuerdos de nivel de operación de acuerdo al diseño y requisitos de nivel de operación seleccionados.

- Monitorear el rendimiento de los acuerdos de nivel operación con el fin de verificar el cumplimiento de los mismos y la satisfacción de los usuarios; asimismo, con los resultados obtenidos en la realización de monitoreo se pueden examinar y ajustar los niveles de operación con el objetivo de mejorar los servicios prestados a nivel interno.

## 3.28. CONTROLES SOBRE LOS TERCEROS

### 3.28.1. DESCRIPCIÓN

Tiene como objetivo mantener la seguridad de la información en los servicios de procesamiento y almacenamiento de información de la Gobernación del Atlántico a los cuales tienen acceso terceras partes o personal provisto por estas.

### 3.28.2. ACTIVIDADES A DESARROLLAR

A continuación se presentan las actividades a desarrollar durante la ejecución de este proyecto:

- Identificar los riesgos con terceras partes o con personal provisto por ellas, para la información y, los servicios de procesamiento y almacenamiento de la misma.

- Implementar los controles lógicos y físicos necesarios para proteger la información que no debe ser accesible a terceras partes o a personal provisto por ellas.

- Establecer los requisitos legales y obligaciones contractuales que se deberían tener en cuenta en las relaciones con terceras partes o personal provisto por ellas, incluyendo temas como el cumplimiento de las políticas de seguridad, acuerdos o clausulas para el intercambio de información y acuerdos o cláusulas de confidencialidad, haciéndolos extensivos a los terceros de los terceros contratados.

- Implantar y divulgar las funciones y responsabilidades frente a la seguridad de la información, que le competen al personal provisto por terceras partes, así como a sus terceros, que cuente con acceso a la plataforma tecnológica o la información contenida en ella.

- Establecer en el proceso de finalización de contrato, aspectos referentes a la entrega de bienes, información, derechos de acceso y puestos de trabajo de manera formal, por parte del personal provisto por terceras partes.

- Monitorear el cumplimiento de los Acuerdos de Niveles de Servicio con el fin de verificar el cumplimiento de los niveles de servicio acordados y la satisfacción de los usuarios frente a estos, con el objetivo de proponer mejoras sobre los mismos.

## 3.29. IDENTIFICACIÓN Y ACTUALIZACIÓN DE LA LEGISLACIÓN VIGENTE

### 3.29.1. DESCRIPCIÓN

Tiene como propósito evitar el incumplimiento de cualquier ley, de obligación estatutaria, reglamentaria o contractual y de cualquier requisito de seguridad.

### 3.29.2. ACTIVIDADES A DESARROLLAR

A continuación se presentan las actividades a desarrollar durante la ejecución de este proyecto:

- Identificar, mantener y actualizar de manera documentada, la legislación aplicable, como son los requisitos estatutarios, reglamentarios y contractuales que rigen para Gobernación, relacionada con la seguridad de la información.

- Garantizar la protección de los datos y la privacidad de la información personal de acuerdo con la legislación y reglamentos pertinentes.

- Validar la regulación de controles criptográficos frente a los acuerdos de ley y reglamentos pertinentes.

- Validar el cumplimiento técnico frente a las políticas y normas de seguridad de la información de la Gobernación.

## 3.30. SEGURIDAD EN EL INTERCAMBIO DE INFORMACIÓN

### 3.30.1. DESCRIPCIÓN

El objetivo es mantener la seguridad de la información que se intercambia tanto dentro como fuera de las instalaciones de la Gobernación del Atlántico.

### 3.30.2. ACTIVIDADES A DESARROLLAR

A continuación se presentan las actividades a desarrollar durante la ejecución de este proyecto:

- Identificar y establecer la herramienta adecuada para aplicar controles criptográficos en el intercambio de información de acuerdo a las necesidades y considerando aspectos como algoritmos de cifrado, tipo de licencia y evaluando alternativas posibles como PGP, GPG, VeraCrypt y BitLocker.

- Almacenar las llaves criptográficas y las copias de seguridad de las mismas en un repositorio central, el cual debe contar con protección contra modificación, pérdida o destrucción.

- Establecer los lineamientos para el uso adecuado de los controles criptográficos, considerando aspectos relacionados con legislación y necesidad de uso.

- Instaurar acuerdos de intercambio de información entre partes externas y la Gobernación, considerando los lineamientos de uso de los controles criptográficos y consecuencias legales por el manejo inadecuado de la información.

## 3.31. IMPLEMENTACIÓN DE CONTROLES CRIPTOGRÁFICOS

### 3.31.1. DESCRIPCIÓN

El objetivo es realizar la implementación de controles criptográficos, con el fin de proteger el almacenamiento y transmisión de información sensible, obteniendo así un fortalecimiento de la plataforma tecnológica de la Gobernación del Atlántico.

### 3.31.2. ACTIVIDADES A DESARROLLAR

A continuación se presentan las actividades a desarrollar durante la ejecución de este proyecto:

- Identificar y establecer la herramienta adecuada para aplicar controles criptográficos, considerando aspectos como algoritmos y tipos de llaves criptográficas, y evaluando alternativas como PGP o GPG.

- Almacenar las llaves criptográficas en un repositorio central, el cual debe contar con protección contra modificación, pérdida o destrucción.

- Establecer los lineamientos para el uso adecuado de los controles criptográficos.
- Llevar cabo la implementación de los controles criptográficos considerando los lineamientos para su uso.
- Definir y establecer procedimientos para la administración de llaves criptográficas, si resulta aplicable, considerando aspectos como fechas finales de uso, retiro de llaves, destrucción de llaves, usuarios autorizados para su uso, registros y auditoria, y copias de respaldo de las mismas.

## 3.32. ESTABLECIMIENTO Y MONITOREO DE CONDICIONES AMBIENTALES PARA CENTROS DE DATOS

### 3.32.1. DESCRIPCIÓN

Tiene como objetivo establecer y monitorear las condiciones ambientales y de las instalaciones donde se encuentra la plataforma tecnológica de la Gobernación del Atlántico.

### 3.32.2. ACTIVIDADES A DESARROLLAR

A continuación se presentan las actividades a desarrollar durante la ejecución de este proyecto:

- Mantener las instalaciones donde se encuentra ubicada la plataforma tecnológica de la Gobernación libre de materiales combustibles o peligrosos como cartón, papel y líquidos inflamables.
- Realizar el análisis correspondiente de los riesgos medio ambientales y geográficos del sitio donde se encuentra ubicada la plataforma tecnológica, considerando aspectos como incendios, altas temperaturas, humedad, inundaciones, contaminación por polvo, terremotos, explosiones, manifestaciones o disturbios sociales, entre otros.
- Implantar los controles medioambientales necesarios o mejorar los controles existentes y llevar a cabo las adecuaciones necesarias en los sitios de procesamiento de información o centros de datos para mitigar los riesgos identificados.
- Realizar un monitoreo periódico de las instalaciones donde se encuentra ubicada la plataforma tecnológica, con el objetivo de ratificar o ajustar consideraciones referentes a incendios, altas temperaturas, humedad, inundaciones, contaminación por polvo, materiales combustibles o peligrosos, almacenamiento de equipos de cómputo y medios, y cualquier otro aspecto que pueda afectar las condiciones de las instalaciones.

## 3.33. ESTABLECIMIENTO Y MONITOREO DE CONDICIONES AMBIENTALES PARA SITIOS DE ARCHIVO

### 3.33.1. DESCRIPCIÓN

Tiene como objetivo establecer y monitorear las condiciones ambientales y de las instalaciones donde se encuentra

la documentación física de la Gobernación del Atlántico.

### 3.33.2. ACTIVIDADES A DESARROLLAR

A continuación se presentan las actividades a desarrollar durante la ejecución de este proyecto:

- Mantener las instalaciones donde se encuentra ubicada la documentación física de la Gobernación libre de materiales combustibles y líquidos inflamables.

- Evaluar las condiciones de las instalaciones donde se encuentran ubicados los Archivos de la Gobernación y especialmente los referentes a la Secretaría de Informática y Telecomunicaciones, verificando aspectos de temperatura, humedad, ventilación, iluminación y contaminación por polvo, entre otros.

- De ser necesario, llevar a cabo las adecuaciones requeridas e implantar controles ambientales de temperatura, humedad, ventilación, iluminación y contaminación por polvo para dar cumplimiento con la normativa de manejo de archivos.

- Instalar mecanismos que permitan el monitoreo de las condiciones ambientales del Archivo, como termohigrómetros, que permiten la medición de temperatura y humedad; así mismo, se deben registrar las mediciones realizadas de manera periódica.

- Realizar mantenimientos periódicos a las instalaciones del Archivo.

## 3.34. ASEGURAMIENTO DE PLATAFORMA: ESTACIONES DE USUARIO

### 3.34.1. DESCRIPCIÓN

El objetivo es realizar el aseguramiento de la plataforma tecnológica, en el componente de estaciones de usuario; adicionalmente, apoyar la mitigación de vulnerabilidades detectadas en este componente durante la ejecución del proyecto de análisis de vulnerabilidades técnicas, obteniendo así un fortalecimiento de la plataforma tecnológica de la Gobernación del Atlántico.

### 3.34.2. ACTIVIDADES A DESARROLLAR

A continuación se presentan las actividades a desarrollar durante la ejecución de este proyecto:

- Realizar la configuración de protocolos, puertos y servicios necesarios para el desarrollo de las labores en las estaciones de usuario de la Gobernación.

- Establecer políticas de dominio y listas de acceso que rijan las configuraciones de las estaciones de usuario.

- Renombrar las cuentas de administrador y proteger o deshabilitar las cuentas de invitado en las estaciones de usuario, con el fin mitigar los riesgos relacionados con los nombres de usuario y cuentas por defecto.

- Verificar y optimizar los procesos y servicios de arranque de los sistemas operativos de las estaciones de usuario.

- Actualizar los componentes de software y los parches de seguridad de las estaciones de usuario siguiendo los lineamientos para la gestión del cambio.

- Habilitar y personalizar los mecanismos de auditoria y monitoreo de las estaciones de usuario, considerando aspectos como la generación de registros sobre las acciones de los administradores, eliminación de registros de auditoria y acceso a diferentes elementos del sistema.

- Seguir buenas prácticas y guías de aseguramiento de acuerdo con el sistema operativo con el que cuenten las estaciones de usuario.

## 3.35. ASEGURAMIENTO DE PLATAFORMA: REDES, SERVIDORES, BASES DE DATOS

### 3.35.1. DESCRIPCIÓN

El objetivo es realizar el aseguramiento de la plataforma tecnológica, en sus componentes de redes, servidores y bases de datos; adicionalmente, apoyar la mitigación de vulnerabilidades detectadas en estos componentes el análisis de vulnerabilidades técnicas, obteniendo así un fortalecimiento de la plataforma tecnológica de la Gobernación del Atlántico.

### 3.35.2. ACTIVIDADES A DESARROLLAR

A continuación se presentan las actividades a desarrollar durante la ejecución de este proyecto:

- Llevar a cabo el aseguramiento correspondiente a los componentes de red considerando aspectos como el bloqueo de puertos, fortalecimiento de las credenciales de acceso, registros de auditoria, buenas prácticas aplicables y guías de aseguramiento provistas por el fabricante de acuerdo con las características y modelo del componente de red.

- Realizar el aseguramiento correspondiente a los servidores considerando aspectos como el bloqueo de puertos, fortalecimiento de las credenciales de acceso, registros de auditoria, políticas de software, actualización de parches de seguridad, buenas prácticas y guías de aseguramiento de acuerdo con el sistema operativo y los servicios que provea el servidor.

- Efectuar el aseguramiento correspondiente a las bases de datos considerando aspectos como el uso controlado de puertos, fortalecimiento de las credenciales de acceso y métodos de autenticación, registros de auditoria, políticas de administración del motor de base de datos, almacenamiento cifrado de la información, transmisión segura de información, buenas prácticas y guías de aseguramiento de acuerdo con el motor de base de datos y los servicios que este provea.

## 3.36. SEGURIDAD DE LOS EQUIPOS FUERA DE LAS INSTALACIONES

### 3.36.1. DESCRIPCIÓN

El objetivo es establecer las medidas de control adecuadas para la movilización fuera de la instalaciones de los equipos de cómputo, dispositivos móviles y cualquier medio electrónico que contenga información correspondiente a la Gobernación del Atlántico, con el fin de proteger la información contenida en ellos.

### 3.36.2. ACTIVIDADES A DESARROLLAR

A continuación se presentan las actividades a desarrollar durante la ejecución de este proyecto:

- Realizar, en apoyo con el proyecto de concienciación y educación, la divulgación correspondiente de los riesgos a los que se ven expuestos los equipos de cómputo, dispositivos móviles y cualquier otro medio que contenga información, cuando son retirados de la Gobernación.

- Establecer los mecanismos adecuados con el fin de evitar la fuga de información en los equipos de cómputo, dispositivos móviles y cualquier otro medio que contenga información, a través del uso de controles como los criptográficos.

## 3.37. AJUSTES AL PLAN DE CONTINUIDAD DE NEGOCIO INCLUYENDO CONSIDERACIONES DE SEGURIDAD

### 3.37.1. DESCRIPCIÓN

Su objetivo es determinar e incluir los aspectos relevantes relacionados con la seguridad de la información en el Plan de Continuidad de Negocio y el Plan de Contingencia de la Gobernación del Atlántico, estableciendo los procedimientos e implantando los controles requeridos para mantener el nivel requerido de seguridad de la información durante la activación de la continuidad del negocio o la contingencia tecnológica.

### 3.37.2. ACTIVIDADES A DESARROLLAR

A continuación se presentan las actividades a desarrollar durante la ejecución de este proyecto:

- Determinar si el Plan de Continuad del Negocio y el Plan de Contingencia Tecnológica cuentan con medidas para preservar la confidencialidad, integridad y disponibilidad de la información.

- Identificar los requisitos de seguridad de la información que deben ser tenidos en cuenta en la planificación de la continuidad del negocio y recuperación de desastres.

- Incluir dentro del Análisis de Impacto del Negocio (BIA) los aspectos de seguridad de la información.

- Establecer la estructura organizacional con la autoridad, experiencia y competencia necesarias para gestionar los temas de seguridad de la información durante la activación del Plan de Continuidad de Negocio o el Plan de Contingencia Tecnológica.

- Documentar y establecer los procedimientos, instructivos o planes para mantener la seguridad de la información durante la ocurrencia de activación de los planes de continuidad de negocio o contingencia tecnológica, dando cumplimiento a los requerimientos identificados previamente.

- Establecer los controles de seguridad de la información dentro de los procesos de continuidad de negocio o de recuperación de desastres.

## 3.38. GESTIÓN DEL LICENCIAMIENTO DEL SOFTWARE

### 3.38.1. DESCRIPCIÓN

Tiene como propósito evitar el incumplimiento de las leyes relacionadas con derechos de autor y controlar el licenciamiento del software utilizado en la Gobernación del Atlántico.

### 3.38.2. ACTIVIDADES A DESARROLLAR

A continuación se presentan las actividades a desarrollar durante la ejecución de este proyecto:

- Establecer procedimientos y controles para asegurar el cumplimiento de la legislación aplicable a material con derechos de propiedad intelectual.

- Definir los responsables de monitorear las licencias utilizadas con una periodicidad establecida.

- Deshabilitar las licencias no utilizadas en el momento de dar de baja los equipos de cómputo o reasignarlos.

## 3.39. CONTROL DE VERSIONES DE CÓDIGO FUENTE DE LOS SISTEMAS DE INFORMACIÓN

### 3.39.1. DESCRIPCIÓN

Tiene como propósito establecer un mecanismo de control para mantener un historial de cambios sobre los programas de código fuente de los sistemas de información de la Gobernación del Atlántico, permitiendo su utilización para el desarrollo futuro de manera vigilada.

### 3.39.2. ACTIVIDADES A DESARROLLAR

A continuación se presentan las actividades a desarrollar durante la ejecución de este proyecto:

- Definir la herramienta de mercado para control de versiones de programas de código fuente.

- Definir si los mecanismos de almacenamiento de los programas de código fuente que deba gestionar la herramienta serán centralizados o distribuidos.

- Asignar un responsable del sistema de control de versiones y definir sus responsabilidades.

- Generar y establecer el procedimiento o instructivo para realizar cambios sobre los programas de código fuente almacenados en la herramienta seleccionada.

- Verificar con una periodicidad establecida el registro histórico de las acciones realizadas con cada programa o conjunto de programas.

## 3.40. VERIFICACIÓN Y AJUSTES SOBRE LA ARQUITECTURA TÉCNICA DE SEGURIDAD

### 3.40.1. DESCRIPCIÓN

Tiene como objetivo la verificación y ajustes sobre la arquitectura técnica de seguridad, con el fin de buscar fortalecimiento en la plataforma tecnológica de la Gobernación del Atlántico.

### 3.40.2. ACTIVIDADES A DESARROLLAR

A continuación se presentan las actividades a desarrollar durante la ejecución de este proyecto:

- Identificar las posibles falencias de la arquitectura técnica de seguridad actual a través de reportes realizados a la mesa de ayuda, incidentes de seguridad presentados y reportes que se hayan presentado producto del análisis de vulnerabilidades técnicas.

- Confirmar cuales de las posibles falencias identificas, son fallas reales de la arquitectura técnica de seguridad actual, con el fin de dar tratamiento adecuado a cada una de ellas.

- Llevar a cabo el proceso de solución de las fallas detectadas en la arquitectura técnica de seguridad, con el objetivo de cerrar posibles brechas de seguridad de la información.

- Realizar ajustes proactivos en la arquitectura técnica de seguridad, a través del aseguramiento de la plataforma, con el objetivo de no dar oportunidad a ataques relacionados con seguridad de la información.

## 3.41. SEGMENTACIÓN DE RED A NIVEL DE COMUNICACIONES (ROUTERS, SWITCH) Y CONFIGURACIÓN DE DISPOSITIVOS DE SEGURIDAD (FIREWALL, IDS, IPS)

### 3.41.1. DESCRIPCIÓN

Tiene como objetivo realizar la segmentación de red y la configuración de dispositivos de seguridad, a través de la identificación de los recursos de la plataforma tecnológica que así lo requieren, debido al servicio que proveen o a la sensibilidad de la información que almacenan y/o procesan de la Gobernación del Atlántico.

### 3.41.2. ACTIVIDADES A DESARROLLAR

A continuación se presentan las actividades a desarrollar durante la ejecución de este proyecto:

- Definir los segmentos de la red por áreas funcionales que componen la Gobernación, ayudando así a identificar y separar los perfiles de usuario que componen cada una de estas áreas.
- Definir segmentos adicionales por los cuales circulará tráfico relacionado únicamente a servicios, voz y vídeo, así como segmentos adicionales para los servidores.
- Determinar sobre cada uno de los segmentos la distribución de los recursos tecnológicos, conforme al servicio que prestan, definiendo de esta manera cuáles deben ser accedidos única y exclusivamente desde el interior de la red, y cuáles podrían recibir conexión desde el exterior de la misma, y de esta manera adecuar las necesidades de uso de la DMZ.
- Establecer dentro de la red, segmentos independientes para los ambientes de: Producción, pruebas y desarrollo.
- Establecer dentro de la red, un segmento exclusivo para todas las interfaces de administración de los elementos de red y seguridad: Firewall, routers, switches, SAN, entre otros.
- Documentar la segmentación definida de tal manera que se pueda seguir a futuro un control de cambios sobre la misma.
- Identificar la necesidad de adquisición de equipos de comunicaciones faltantes como routers o switch, con el fin de poner en marcha la segmentación definida de acuerdo con los procesos o procedimientos de control de cambios.
- Evaluar la necesidad de adquisición de dispositivos de seguridad como Firewall, IDS e IPS, con el fin de contar con controles para el filtrado de tráfico, detección de intrusos y prevención de intrusos.
- Ejecutar la puesta en marcha de los dispositivos de seguridad como Firewall, IDS e IPS, considerando aspectos como áreas con información sensible, estándares de seguridad y recomendaciones del proveedor del servicio.

## 3.42. REVISIÓN Y AJUSTE DE LOS DISPOSITIVOS DE SEGURIDAD (FIREWALL, IDS, IPS)

### 3.42.1. DESCRIPCIÓN

Tiene como objetivo la revisión de la configuración de los dispositivos de seguridad y realización de ajustes de ser necesario, a través de la identificación de los recursos de la plataforma tecnológica que así lo requieren, debido al servicio que proveen o a la sensibilidad de la información que almacenan y/o procesan de la Gobernación del Atlántico.

### 3.42.2. ACTIVIDADES A DESARROLLAR

A continuación se presentan las actividades a desarrollar durante la ejecución de este proyecto:

- Verificar en la configuración del Firewall el trafico entrante y saliente, con el fin de identificar mejoras en los filtros de tráfico; adicionalmente, se debe validar que los puertos abiertos en la configuración del Firewall estén autorizados y aun se encuentren en uso.

- Evaluar las políticas configuradas en el IDS e IPS, con el fin de definir si se cumple con los objetivos de detección y prevención de intrusos planteados.

- Realizar los ajustes identificados sobre los dispositivos de Firewall, IDS e IPS, considerando efectuar un monitoreo constante sobre los cambios realizados.

## 3.43. ESTRATEGIA DE MIGRACIÓN IPV4 A IPV6

### 3.43.1. DESCRIPCIÓN

Tiene como objetivo definir la estrategia de migración del protocolo IPv4 a IPv6, definiendo las principales actividades a desarrollar.

### 3.43.2. ACTIVIDADES A DESARROLLAR

A continuación se presentan las actividades a desarrollar durante la ejecución de este proyecto:

- Planeación IPV6: Elaborar el inventario de activos de información. Validación de la infraestructura tecnológica, para validar el grado de compatibilidad con el protocolo. Identificar la topología actual. Planear el proceso de transición de los principales servicios de tecnología (WEB, DHCP, CORREO, DNS, DIRECTORIO ACTIVO, etc.). Revisar las políticas de enrutamiento de la red.

- Implementación: Habilitar el direccionamiento en cada uno de los componentes. Desarrollar la configuración de las pruebas piloto. Realizar el montaje, ejecución y corrección de configuraciones del piloto de pruebas de IPv6. Aplicar el modelo de transición. Realizar el diseño de la topología con base en el protocolo IPv6. Validar funcionalidades de IPv6. Activar políticas de seguridad de IPv6
- Establecer el enrutamiento necesario, desde el interior en la red LAN, hacia las redes externas, coordinando con el proveedor de Internet.

- Pruebas de funcionalidad: Realizar pruebas y monitoreo de la funcionalidad de IPv6, en los sistemas, aplicaciones, servicios, entre otros. Realizar pruebas de las políticas de seguridad de IPv6. Afinamiento de la configuración del hardware.

- Actualizar el inventario de sistemas, servicios, aplicaciones, elementos de comunicación, con el nuevo protocolo de red, IPv6

## CONCLUSIONES

- Los planes de tratamiento de riesgos y los proyectos presentados en el documento se encuentran alineados con los resultados del análisis y evaluación de riesgos.

- Los resultados presentados en el numeral uno, presentan un resumen ejecutivo de los existentes en la matriz de riesgos de seguridad de la información de la Gobernación del Atlántico.

- Los planes de tratamiento de riesgos planteados en el siguiente documento no tienen dependencia unos de otros, considerando el enfoque dado a fortalecer los controles existentes a través de proyectos.