LINEAMIENTOS DE ADMINISTRACION DE SEGURIDAD

Abril de 2023

CONTENIDO

INTRODUCIÓN

Teniendo en cuenta que la oficina de Tecnologías y Sistemas de Información de la Gobernación desarrolla un proyecto orientado a la implementación de las mejores prácticas de ITIL®, se presenta a continuación el documento de lineamientos, mediante el cual se gestionará la Seguridad de la información como un proceso sistemático, documentado y conocido por toda la entidad.

La Gobernación del Magdalena y en especial su oficina de Tecnologías y Sistemas de Información comprende que la información es parte fundamental de los servicios que presta, y que, para garantizar su confidencialidad, integridad y disponibilidad, es necesario adoptar estrategias que permitan establecer niveles adecuados de protección, asegurando la continuidad en la prestación de servicios a sus diferentes clientes internos.

Así mismo, es importante mencionar que el presente lineamiento se basa en los parámetros establecidos por el estándar internacional ISO/IEC 27001, el cual será una herramienta útil para el logro de los objetivos estratégicos planteados por la alta dirección de la Gobernación del Magdalena.

1. OBJETIVO

El objetivo General del Lineamiento de la Administración de Seguridad es alinear la seguridad de TI con la Seguridad de la entidad garantizando la confidencialidad, integridad y disponibilidad de la información en las actividades realizadas para gestionar servicios de TI.

1.1. Objetivos Específicos

Los objetivos específicos de la Administración de Seguridad son:

- Producir y mantener un Sistema de Prevención de Intrusos - ISP alineada con a los objetivos estratégicos de la entidad en relación con la protección y el uso efectivo de los recursos de información.

- Establecer controles de seguridad a través de la implantación de políticas, estándares, guías y procedimientos, que permitan la protección de los recursos de la información de la entidad.

- Desarrollar un plan de seguridad a través de la administración de riesgos que considere las amenazas y vulnerabilidades a los que se encuentra expuesta la entidad para proteger toda aquella información crítica.

- Garantizar que el intercambio de información entre varios involucrados sea confiable.

2. ALCANCE

El alcance de la Administración de Seguridad cubre los lineamientos de la oficina de Tecnologías y Sistemas de Información que soportan el diseño, transición y operación de los servicios establecidos en el Catálogo de Servicios de Tecnología de Información y Comunicaciones, los cuales se listan a continuación:

1. Internet.
2. Intranet.
3. Correo electrónico.
4. Diseño y publicación de páginas web.
5. Sistemas de información.
6. Video conferencia.
7. Sistema de Gestión de Correspondencia.
8. Sistema de Gestión de Talento Humano.

3. TÉRMINOS Y DEFINICIONES

Activo: Algo que tenga valor para lo organización. Los activos pueden incluir, gente, edificios, sistemas computacionales, redes, registros en papel, faxes, etc.

Amenaza: Causa potencial de un incidente no deseado que puede resultar en daño al sistema u organización. [ISO/IEC 13335-1:2004]

Confiabilidad: Garantizar que los sistemas informáticos brindan información correcta para ser utilizada en la operatoria de cada uno de los procesos.

Confidencialidad: Garantizar que toda la información está protegida del uso no autorizado, revelaciones accidentales, espionaje industrial, violación de la privacidad y otras acciones similares de accesos de terceros no permitidos.

Control: Herramienta de la gestión del riesgo, incluidas políticas, pautas, estructuras organizacionales, que pueden ser de naturaleza administrativa, técnica, gerencial o legal.

NOTA: Control es también usado como sinónimo de salvaguardia o contramedida.

Disponibilidad: Garantizar que la información y la capacidad de su procesamiento manual y automático, sean resguardadas y recuperadas eventualmente cuando sea necesario, de manera tal que no se interrumpa significativamente la marcha de los negocios.

Evento de seguridad de información: Es una ocurrencia identificada de un sistema, servicio, o red el cual indica una posible brecha de la política de seguridad de información o fallas de las salvaguardias o una situación desconocida que puede ser relevante para la seguridad. [ISO/IEC 18044-1:2004].

Exactitud: Asegurar que toda la información se encuentre libre de errores y/o irregularidades de cualquier tipo.

Gestión del riesgo: Actividades coordinadas para dirigir y controlar una organización considerando el riesgo.

NOTA: Gestión del riesgo incluye típicamente evaluación del riesgo, tratamiento del riesgo, aceptación del riesgo y comunicación del riesgo.

Incidente de seguridad de información: Es indicado por una o varias series de eventos inesperados y no deseados que tienen una gran probabilidad de comprometer las operaciones de negocios y de amenazar la seguridad de información. [ISO/IEC TR 18044:2004]

Integridad: Asegurar que sea procesada toda la información necesaria y suficiente para la marcha de los negocios en cada uno de los sistemas informáticos y procesos transaccionales.

Legalidad: Asegurar que toda la información y los medios físicos que la contienen, procesen y/o transporten, cumplan con las regulaciones legales vigentes en cada ámbito.

Política: Dirección general y formal expresada por la gerencia.

Riesgo: Combinación de la probabilidad de un evento y sus consecuencias. [ISO/IEC Guide 73:2002]

Seguridad de la información: Preservación de la confidencialidad, integridad y disponibilidad de la información, así mismo, otras propiedades como la autenticidad, no rechazo, contabilidad y confiabilidad también pueden ser consideradas.

Tratamiento del riesgo: Proceso de selección e implementación de medidas para modificar el riesgo. [ISO/IEC Guide 73:2002]

Vulnerabilidad: Debilidad de un activo o grupo de activos que pueden ser explotados por una o más amenazas. [ISO/IEC 13335-1:2004]

4. DEFINICIÓN

Los lineamientos de Seguridad de la información complementan el procedimiento que gestiona y define los niveles de seguridad, analizando las brechas de seguridad existentes y los incidentes presentados, a partir de los cuales genera planes que permiten reducir los niveles de riesgo a los cuales está expuesta la entidad. Este lineamiento debe ser considerado como un marco de gobierno que cuenta con una política de seguridad adoptada por el más alto nivel de decisión de la entidad que orienta e imparte directrices relacionadas con la seguridad de los servicios y la información. El lineamiento de la Administración de Seguridad debe garantizar que las políticas de seguridad, Ver. **Manual de Políticas de Seguridad de la Información**, son revisadas regularmente y que refleja las necesidades de la entidad, al igual que establecer una estructura organizacional en términos de seguridad basada en roles y responsabilidades.

Así mismo, establece mecanismos que permiten proteger los activos claves de la entidad, por tanto, estos activos deben ser claramente identificados y analizados para comprender el nivel de criticidad de cada uno de ellos frente a los impactos que puedan generar a la entidad por pérdidas en la confidencialidad, integridad y

disponibilidad de estos. El resultado del análisis de los activos debe generar una clasificación de seguridad adecuada de estos activos.

El lineamiento de Administración de Seguridad debe garantizar que se realiza un análisis y valoración de riesgos asociados a cada uno de los activos identificados, lo cual permite establecer cuáles son los controles que deben desplegarse para reducir los niveles de riesgo calculados. Así mismo, las actividades necesarias para desplegar estos controles deben ser plasmadas en un plan de seguridad que contemple un análisis detallado de costo-beneficio de implementación de controles.

La implementación de los controles debe ser realizada a través de un procedimiento adecuado de cambios y liberaciones, garantizando que las pruebas requeridas son ejecutadas al igual que los procedimientos necesarios para operación son elaborados y formalmente establecidos. Es importante mencionar que existe una relación estrecha tanto con los lineamientos de incidentes y de monitoreo, dada la necesidad de gestionar de forma adecuada de los incidentes de seguridad que puedan presentarse.

4.1 Flujograma

El objetivo de este apartado es mostrar el flujo de actividades del lineamiento de Administración de Seguridad, los cuales están alineados a las mejores prácticas de la Administración de Servicios de ITIL® y MOF.

Ver Procedimiento de Administración de Seguridad.

4.1.1 Consideraciones claves en las actividades

La información deberá clasificarse de acuerdo a lo establecido en la **Guía para la calificación de la información**

4.2 Metodología para análisis de riesgos

A continuación, se muestran las actividades de cada una de las etapas para identificar con claridad la situación de cada uno de los activos de la Gobernación del Magdalena: su valor, vulnerabilidades, y cómo están protegidos frente a las amenazas a las cuales están expuestos; con lo cual, una vez analizados los riesgos, se elaborará el plan de tratamiento que al ser implementado y monitoreado asegure niveles de riesgo aceptables para la entidad.

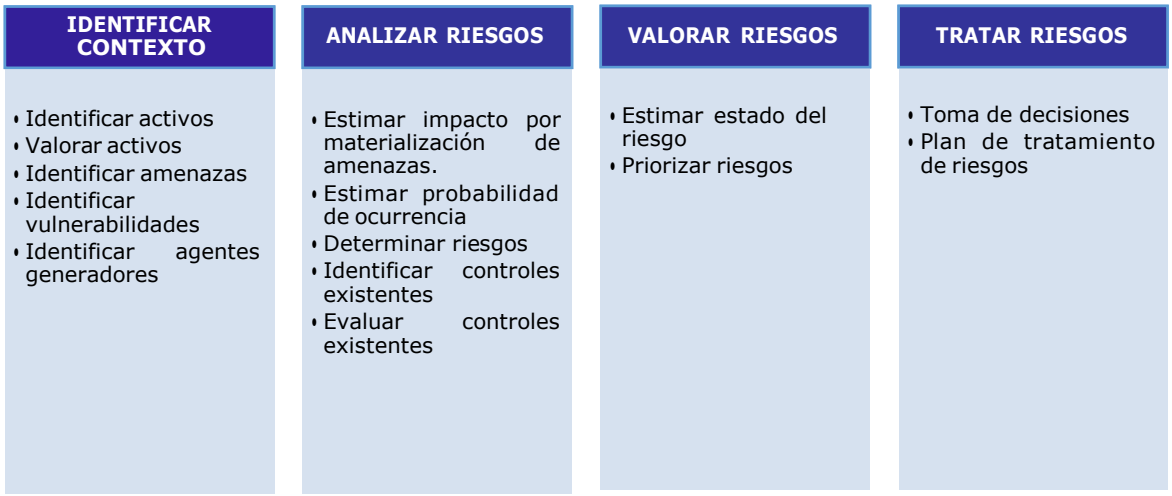

Ilustración 1. Etapas de la Gestión de Riesgos

Identificar Contexto

Objetivo: Conocer los eventos potenciales, que ponen en riesgos los activos y, establecer los efectos creados por su ocurrencia.

a) <u>Identificación de activos</u>

Un activo es: "Es cualquier elemento al cual se le asigna un valor y por lo tanto requiere protección. Los activos pueden ser: infraestructura tecnológica, documentos electrónicos y físicos, personas", lo cual puede entenderse igualmente como aquello que requiere la organización para el cumplimiento de sus objetivos.

Tipos de activo		
Tipo		**Descripción**
Infraestructura	Infraestructura física	Centro de datos, oficinas.
	Tecnología Hardware	Servidores, dispositivos de comunicaciones, computadoras de escritorio, laptops, impresoras, copiadoras, faxes, teléfonos, grabadoras de CD/DVD.
	Tecnología Software	Aplicaciones comerciales, aplicaciones desarrolladas en casa y open source.
información	Electrónica	Información importante para el negocio (bases de datos) e información de soporte (procesos, políticas, procedimientos, guías y estándares) en medios electrónicos.
	Papel	Información importante para el negocio (reportes) e información de soporte (procesos, políticas, procedimientos, guías, contratos, información de clientes y estándares) en papel.
Gente	Dueños de información	Nivel directivo dueño de la información que asigna permisos para leer utilizar y modificar la información.
	Usuarios	Personal que utiliza la información para el desempeño de su trabajo diario y que da soporte a los sistemas de información.
Servicios		Correo electrónico, Acceso a red privada virtual (VPN).

Tabla 1. Tipos de activos

b) Valoración de activos

Una vez identificados los activos se realizará la valoración de cada uno de ellos en términos de valor para la entidad según las siguientes dimensiones:

- Disponibilidad
- Confidencialidad
- Integridad

La valoración por dimensiones de cada uno de los activos nos permite establecer que activos son más valiosos para la entidad y por tanto deben ser protegidos.

Valoración De Activo
MB: muy bajo

B: bajo
M: medio
A: alto
MA: muy alto

Tabla 2. Valoración de activos

c) Identificación de amenazas

Una vez valorados los activos es necesario identificar las amenazas a las cuales está expuesto cada activo; es importante que esta consideración se realice sin tener en cuenta los controles establecidos.

Las amenazas son resultados de actos deliberados o mal intencionados que pueden afectar nuestros activos, sin embargo, existen eventos naturales o accidentales que deben ser considerados por su capacidad de generar incidentes no deseados.

Las amenazas a la cuales están expuestos los diferentes activos pueden ser según su origen las siguientes:

Origen	Amenaza
Condiciones Naturales	Incendios, inundaciones, sismos, tormentas.
Condiciones externas	Aspectos regulatorios, caída de energía, campos electromagnéticos, contaminación, crisis financieras, daño de agua, excesivo calor, excesivo frio, explosiones, perdida de proveedores, problemas de transporte, sobrecargas.
Condiciones internas	Campos electromagnéticos, contaminación, daños en los equipos, escapes, fallas en la red, fallas en líneas telefónicas, fallas mecánicas, falta de insumos, fugas, humedad, mala publicidad, pérdida de acceso, perdida de proveedores, polvo, problemas de transporte, registros errados, sobrecargas, suciedad, vibraciones.

Entorno Social	Motines, protestas, sabotaje, vandalismo, bombas, violencia laboral, terrorismo.
Actos deliberados	Abuso privilegios de acceso, análisis de tráfico, ataque físico a los equipos, bombas lógicas, código malicioso, destrucción de información, divulgación de información, errores en código, espías (spyware),extorsión, Espionaje industrial, fallas de hardware, fallas de software, fallas en la red, fallas en líneas telefónicas, gusanos, incendios, ingeniería social, interceptación de información, manipulación de programas, perdida de datos, robo de información, suplantación de identidad, troyanos, usos no autorizados, Virus.
Actos accidentales	Destrucción de información, Incendios, pérdida de claves, perdida de dispositivos.
Humano	Epidemias, huelgas, indisponibilidad de personal, perdida de personal clave.

Tabla 3. Listado de amenazas según su origen

d) Identificación de vulnerabilidades

Debe identificarse la forma como cada una de las amenazas podría materializarse, es decir, que vulnerabilidades permiten que las amenazas se conviertan en situaciones de riesgo reales.

Algunas vulnerabilidades pueden ser:

- Ausencia de políticas
- Configuraciones no seguras
- Empleado actual descontento
- Empleado antiguo descontento
- Empleado deshonesto (sobornado o víctima de chantaje)
- Empleado desinformado
- Empleado negligente
- Errores de configuración.
- Errores de mantenimiento.
- Errores del administrador.
- Errores en código.
- Exposición a materiales peligrosos.
- Fallas de usuarios.
- Manuales de uso no documentados
- Medidas de protección de acceso inadecuadas
- Medidas de protección física inadecuadas

- Procesos o procedimientos no documentados.
- Usuario desinformado.
- Tecnología inadecuada.
- Debilidad o inexistencia de controles.
- Condiciones de locales inadecuadas o no seguras.
- Identificación de agentes generadores

Los agentes generadores se entienden como todos los sujetos u objetos tienen la capacidad de originar una situación de riesgo; se pueden clasificar en:

- Personas
- Materiales
- Instalaciones
- Entorno

Analizar Riesgos

Objetivo: Establecer la probabilidad de ocurrencia de los riesgos y el impacto de sus consecuencias, calificándolos y evaluándolos, a fin de determinar la capacidad de la organización para su aceptación o manejo.

La calificación del riesgo se logra a través del producto de la estimación de la frecuencia y de la gravedad de los efectos causados por la materialización del riesgo. La primera representa el número de veces que se ha presentado o puede presentarse el riesgo, y la segunda se refiere a la magnitud de sus efectos.

a) Estimar impacto por materialización de amenazas

El impacto es la medida de daño causado por un incidente en el supuesto de que ocurra, afectando así, el valor de los activos. Esta pérdida de valor la denominamos degradación del activo.

La medición del impacto la realizaremos utilizando la siguiente matriz:

VALORACION DEL ACTIVO	DEGRADACION DEL ACTIVO				
	5%	25%	50%	75%	100%
MA: muy alto	M	A	A	MA	MA
A: alto	B	M	A	A	MA

M: medio	B	M	M	A	A
B: bajo	MB	B	M	M	A
MB: muy bajo	MB	MB	B	B	M

Tabla 4. Matriz de estimación del impacto sobre activos.

b) Estimar probabilidad de ocurrencia

Una vez valorado el impacto es necesario establecer la probabilidad de ocurrencia (materialización de las amenazas), que puedan causar daño a nuestros activos.

La probabilidad de ocurrencia puede determinarse de forma:

Cualitativa: a partir del análisis de las amenazas, teniendo en cuenta sus características, origen y agentes generadores; este método lo utilizaremos cuando no existan antecedentes de ocurrencia de incidentes que nos permitan determinar con un nivel adecuado de certeza su posibilidad de ocurrencia.

Cuantitativo: a partir de los datos históricos que posea la compañía relacionados con la frecuencia de ocurrencia de las amenazas identificadas. La frecuencia se considera como numero de ocurrencias de la amenaza en un año, Este método nos permite tener un mayor grado de certeza en los resultados obtenidos del análisis de riesgos.

c) Determinar riesgos

Conociendo el impacto de las amenazas sobre los activos es posible determinar el nivel de riesgo potencial, teniendo en cuenta la frecuencia de ocurrencia de los incidentes generados por las amenazas.

Debe tenerse en cuenta que el riesgo crece con el impacto y con la frecuencia.
Para determinar el nivel de riesgo utilizaremos los resultados obtenidos sobre impacto y probabilidad, así:

IMPACTO					
	MA: muy alto	Zona de riesgo moderado	Zona de riesgo importante	Zona de riesgo inaceptable	Zona de riesgo inaceptable
	A: alto	Zona tolerable del riesgo	Zona de riesgo moderado	Zona de riesgo importante	Zona de riesgo inaceptable

M: medio	Zona tolerable del riesgo	Zona de riesgo moderado	Zona de riesgo importante	Zona de riesgo importante
B: bajo	Zona aceptable de riesgo	Zona tolerable del riesgo	Zona de riesgo moderado	Zona de riesgo moderado
MB: muy bajo	Zona aceptable de riesgo	Zona aceptable de riesgo	Zona tolerable del riesgo	Zona tolerable del riesgo
	Poco frecuente	Normal	Frecuente	Muy frecuente

FRECUENCIA

Tabla 5. Matriz para determinación de riesgos**.**

d) Identificar controles existentes

En los pasos anteriores no se han tomado en consideración los controles existentes. Se miden, por tanto, los impactos y riesgos a que estarían expuestos los activos si no se protegieran en absoluto.

Los controles existentes son las medidas o contramedidas que se tienen implementados para reducir los riesgos de procedimientos, mecanismos, controles tecnológicos, etc. Las medidas adoptadas pueden estar orientadas a:

- Prevenir que el incidente se presente (Reduciendo la frecuencia de la amenaza).
- Limitar la posible degradación de los activos (Reducir las consecuencias) o detectar inmediatamente el ataque para evitar que la degradación avance; algunos controles se limitan a permitir la pronta recuperación del sistema cuando la amenaza lo destruye.

Para identificar los controles existentes puede utilizarse como referencia el anexo A del estándar ISO/IEC 27001.

e) Evaluar controles existentes

Una vez identificados los controles existentes es necesario evaluar su efectividad frente a los riesgos que se pretenden mitigar.

Para medir la efectividad de los controles utilizaremos los siguientes criterios:

Criterio	Nulo	Excelente
El control está formalmente establecido.	SI	NO
El control está perfectamente desplegado, configurado y mantenido.	SI	NO
Existen procedimientos claros de uso del control y en caso de incidencias.	SI	NO
Los usuarios están formados y concienciados sobre la aplicación del control.	SI	NO
El control es funcional desde el punto de vista teórico y operacional.	SI	NO

Tabla 6. Criterios para valoración de controles existentes

Valoración De Riesgos

Objetivo: Determinar el nivel o grado de exposición de la organización a los impactos del riesgo, estimando las prioridades para su tratamiento, así mismo, en esta etapa se identifican los mayores riesgos a los cuales está expuesta la entidad para emprender acciones inmediatas de respuesta ante ellos a través de la implementación de objetivos de control, controles, eliminación del riesgo, su transferencia, la aceptación de los efectos causados por su ocurrencia, o buscar la forma de compartir el riesgo con un tercero.

a) Estimar estado real del riesgo

El estado actual del riesgo se establece considerando los controles existentes, orientados a prevenir que el incidente se presente o limitar la posible degradación de los activos.

b) Priorizar riesgos

El estado real del riesgo nos muestra el grado de exposición de la entidad frente a las amenazas evaluadas, allí es posible distinguir entre los Riesgos aceptables, tolerables, moderados, importantes o inaceptables, y establecer la prioridad de las acciones requeridas para su tratamiento.

Las acciones deberán priorizarse así:

Estado real del riesgo (Zona de riesgo)	Prioridad	Tiempo de ejecución de acciones
Inaceptable	Muy Alta	Inmediata
Importante	Alta	De 0 a 3 meses
Moderado	Media	De 3 a 6 meses
Tolerable	Baja	De 6 a 12 meses
Aceptable	Muy baja	De 6 a 12 meses

Tabla 7. Priorización de riesgos y ejecución de actividades

Gestión de Riesgos

Objetivo: Estructurar los criterios orientadores en la toma de decisiones respecto al tratamiento de los riesgos, en esta etapa se establece las guías de acción necesarias para coordinar y administrar los eventos que pueden comprometer la confidencialidad, integridad y disponibilidad de los activos de la entidad.

Así mismo se identifican las opciones para tratar y manejar los riesgos que basadas en la valoración, permiten tomar decisiones adecuadas acerca de si se acepta, se evita, se reduce, se comparte un riesgo o se transfiere legalmente el impacto.

a) Toma de decisiones

Una vez ejecutadas las etapas de análisis y valoración, y con base en los resultados obtenidos en la determinación real de riesgos, es necesario tomar decisiones aplicando los siguientes criterios:

- Si el riesgo se ubica en la Zona de Riesgo Aceptable, permite a la Organización aceptarlo, es decir, el riesgo se encuentra en un nivel que puede asumirse sin necesidad de tomar otras medidas de control diferentes a las que se poseen.

Si el riesgo se ubica en la Zona de Riesgo Inaceptable es aconsejable eliminar la actividad que genera el riesgo en la medida que sea posible, de lo contrario se deben implementar controles orientados a reducir la frecuencia del riesgo y disminuir el impacto por degradación de activos, o compartir el riesgo si es posible a través de pólizas de seguros u otras opciones que estén disponibles.

- Si el riesgo se sitúa en cualquiera de las otras zonas (riesgo tolerable, moderado o importante) se deben tomar medidas para llevar los Riesgos a la Zona Aceptable, en lo posible.

Debe entenderse y aceptarse que en los casos en los cuales se comparte la pérdida ocasionada por un riesgo a través de los contratos de seguros, se asume la parte del riesgo que el seguro no cubre.

Siempre que el riesgo sea calificado impacto muy alto la GOBERNACIÓN diseñará planes de emergencia, contingencia y recuperación, para protegerse en caso de su ocurrencia, los cuales serán orientados y controlados por el Comité de Seguridad establecido.

Las medidas tomadas frente a cada uno de los riegos deben ser conocidas y aceptadas formalmente por el Comité de Seguridad.

"Cualquier nivel de impacto y/o riesgo es aceptable si lo conoce y acepta formalmente el Comité de Seguridad".

Para seleccionar los controles frente a los riesgos establecidos, deberá realizarse un análisis costo-beneficio para evitar implementación de controles con costos superiores al costo de los riesgos reales.

b) Plan de tratamiento de riesgos

Una vez seleccionado los controles que serán implementados para mitigación de riesgos es necesario elaborar un plan que garantice un efectivo despliegue de los mismos.

La elaboración del plan de tratamiento de riesgos será responsabilidad del responsable del lineamiento de Seguridad de la Información y la aprobación de los mismos del Comité de Seguridad de la Gobernación del Magdalena.

El plan de tratamiento de riesgos debe incluir lo siguiente:

- Los controles para implantar o mejorar
- La relación de riesgos a mitigar
- Las personas responsables de su implementación.
- Estimación de recursos necesarios:
    - ✓ Económicos

- ✓ Humanos
- ✓ Físicos

- Relación de tareas y subtareas a ejecutar con sus respectivos responsables.
- Plan de capacitación a todos los involucrados en la implementación de controles.
- Indicadores de eficiencia y eficacia de los controles a implementar o mejorar.

4.3 Descripción de roles

A continuación, se presenta la descripción de los principales roles de la Administración de Seguridad. Por cada uno de los roles se proporciona la siguiente información:

- **Objetivo:** Propósito general del rol descrito.
- **Responsabilidades:** Descripción de las actividades principales del rol.
- **Competencias:** Descripción del conocimiento técnico o profesional necesario para desempeñar el rol descrito.
- **Habilidades:** Descripción de cualidades y destrezas que complementan la competencia del rol descrito.

COMITÉ DE SEGURIDAD DE LA INFORMACIÓN	
Objetivo	La conformación del Comité tiene por objeto la planeación, formulación y la evaluación de las políticas de seguridad de la información, procesos, procedimientos y metodologías específicas de seguridad de la información para el adecuado uso y administración de los activos de información de LA OFICINA DE RECURSOS FÍSICOS DE LA GOBERNACIÓN DEL MAGDALENA
Responsabilidaddes	• Promover la mejora continua del Sistema de Gestión de Seguridad de la Información SCSI de la Gobernación del Magdalena. • Realizar el seguimiento y/o verificación de la implementación de los requisitos, controles e indicadores del Sistema de Gestión de Seguridad de la Información SCSI de la Oficina de recursos Físicos de la Gobernación del Magdalena.

	• Aprobar las medidas y Políticas de Seguridad de la Información y sus modificaciones, en relación con los activos de la información para la Gobernación del Magdalena. • Adoptar las medidas y acciones a que haya lugar, de conformidad con los resultados de los diagnósticos del estado de la seguridad de la información para la Oficina de Recursos físicos de la GOBERNACIÓN DEL MAGDALENA con el fin de tomar y establecer las medidas necesarias. • Establecer mecanismos necesarios para prevenir situaciones de riesgo o incidentes de seguridad física o virtual que puedan generar pérdidas patrimoniales o afectar los recursos de información de la entidad. • Aprobar el uso de metodologías específicas para garantizar confiabilidad, disponibilidad e integridad de la seguridad de la información. • Revisar y aprobar los proyectos de seguridad de la información y servir de facilitadores para su implementación.
Competencias	• Toma de decisiones • Liderazgo • Compromiso institucional
Habilidades	• Administrativas • Conocimiento de la organización de la Oficina de Tecnologías y Sistemas de Información

EQUIPO DE RESPUESTA A INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	
Objetivo	Establézcase como órgano consultivo del Comité de Seguridad de la Información.

Responsabilidades	• Emitir concepto sobre los aspectos necesarios para garantizar la seguridad de la Información. • Proponer los temas, la información y los indicadores que el Comité de Seguridad de la Información determine que habrán de considerarse de interés de la Entidad. • Asesorar y proponer acciones para orientar y mejorar la Seguridad de la Información de la Gobernación del Magdalena. • Coordinar con la Oficina de Tecnologías de la Información y Sistemas, la definición de proyectos y medidas de seguridad de la Información. • Realizar el registro detallado e informar oportunamente la ocurrencia de eventos e incidentes de seguridad de la información, con el fin que la oficina de Tecnologías y Sistemas de información tome las acciones correspondientes. • Establecer contacto con diferentes organismos especializados en materia de seguridad de la información, de acuerdo al marco de cooperación nacional definido en el CONPES 3854 de 2016.
Competencias	• Ingeniería de Sistemas o carreras afín • Conocimiento y experiencia en tecnologías de información • Conocimientos en Administración de Proyectos • Conocimiento en administración de riesgos • Conocimientos sobre fundamentos de ITIL ®v3.
Habilidades	• Administrativas • Capacidad de trabajo en equipo • Conocimiento administrativo de la Gobernación del Magdalena • Conocimientos y práctica en sistemas de información

4.4 Matriz RACI

Una tarea muy importante es realizar un mapeo de los roles y las responsabilidades, así como su intervención en cada una de las actividades con motivo de conocer quién toma parte en cada actividad y con qué nivel de participación. Este mapeo se lleva a cabo con una matriz llamada RACI, donde cada letra que forma su nombre es una responsabilidad específica en la actividad.

A continuación, se muestra la nomenclatura a utilizar dentro de la tabla RACI definida para el lineamiento de Administración de Seguridad.

	RESPONSABILIDAD	DESCRIPCIÓN
R	Responsable	Responsable de ejecutar la actividad.
A	Accountable	Encargado del cumplimiento y la calidad en la ejecución de la actividad.
C	Consulted	Aporta conocimiento y/o información para que el responsable ejecute la actividad.
I	Informed	Rol que debe ser informado una vez que la actividad ha finalizado,

A continuación, se muestra la tabla RACI definida para el lineamiento de Administración de Seguridad. Dicha tabla está conformada por los siguientes rubros:

- **No.:** Número correspondiente a la secuencia de actividades de la función del Punto Único de Contacto o el lineamiento de Administración de Incidentes.
- **Actividad:** Nombre de la actividad.
- **Roles**: Nombre de los roles participantes en el lineamiento de Administración de Incidentes, y de Administración de Servicios, implementados en la Oficina de Tecnologías y Sistemas de Información.

Actividad	Usuario/Cliente	Oficina de Tecnologías y Sistemas de Información	Equipo de respuesta a incidentes de seguridad de	Comité de Seguridad	Administrador Talento humano	Administrador control Interno disciplinario	Administrador incidentes	Administración de configuraciones	Administración de Cambios	Administración de Niveles de Servicio	Administración de
ENTRADA DE LINEAMIENTO	R	A/I	A/I							R	

Requerimientos de seguridad identificados											
ENTRADA DE LINEAMIENTO Brecha potencial de seguridad	R	A/I	A/I								
ENTRADA DE LINEAMIENTO Incidente de seguridad detectado	R						A				
Registrar y revisar requerimiento	C	A/R	A/R								
Ajustar y mantener las políticas de seguridad		A/R	A/R	C					C		
Identificar CI's a proteger	R	A	A					R			
Clasificar CI's	R	A	A					C			
Realizar gestión de riesgos de seguridad	R	A	A								
Generar plan de Tratamiento de riesgos	C	A/R	A/R	C	C				C	C	
Evaluar plan de tratamiento de riesgos		C	C	A/R					C	C	
Es aprobado				A/R					C		
Riesgos aceptados				A/R					C	C	

Firmar cartas de aceptación de riesgos				A/R							
Actividad	**Usuario/Cliente**	**Administrador de Seguridad**	**Administrador de Seguridad**	**Comité de Seguridad**	**Administrador Talento humano**	**Administrador control disciplinario interno**	**Administrador incidentes**	**Administración de configuraciones**	**Administración de Cambios**	**Administración de Niveles de Servicio**	**Administración de**
Implementar y probar plan de tratamiento de riesgos	R	A	A						R		R
Promover capacitación en seguridad de información		R	R	A	R						
Realizar acuerdos e inducción sobre seguridad de información.		R	R	A	R						
Desarrollar procedimientos requeridos	R	A/R	A/R	C	R				C		
Desarrollar lineamientos de monitoreo de seguridad.		A/R	A/R						C		
Desarrollar procedimientos respuesta a incidentes	I	A/R	A/R				R		C		

Revisar y auditar controles y procedimientos implementados		A/R	A/R				C				
¿Existen problemas de seguridad?		A/R	A/R								
Revisar si existió violación a políticas de seguridad		A/R	A/R		C	C					
¿Se requiere Informar violación a la política?		A/R	A/R	C		I					
Tomar acciones disciplinarias	I	I/C	I/C	I/C	C	A/R					
¿Se requiere cambios en políticas ó procedimientos?	I	A/R	A/R	C			C		C		
Registrar incidente	C/ I	I	I				A				
Gestionar incidente de seguridad	C/ I	I	I				A/ R				
Proveer asistencia cuando se requiera		A	A				R				
Resolver y cerrar incidente de seguridad	I	C	C				A/ R				

4.5 Consideraciones clave

Las Consideraciones Clave de la Administración de Seguridad son las condiciones, capacidades y actitudes fundamentales para el éxito de la implementación y operación de la disciplina en el ambiente productivo de la organización. A continuación, se presentan dichas consideraciones:

- El establecimiento de una adecuada política de seguridad de la información, clara y consensuada alineada a los requerimientos de la entidad.

- Garantizar un adecuado apoyo de la Alta Dirección de la entidad en la implementación de la Seguridad de la información y respaldo a las políticas definidas.

- Definir políticas, procedimientos y controles aplicables a la organización desde el punto de vista funcional y operativo.

- Comprender que la seguridad no es responsabilidad de la Oficina de Tecnologías y Sistemas de Información sino de toda la organización.

- Establecer y aplicar un plan sostenible de concientización sobre los requisitos de seguridad.

- Garantizar que no se presente el mal uso y abuso de los sistemas de información que afectan a la intimidad y los valores éticos.

- Mitigar riesgos asociados a peligros externos de los hackers, que conduce a la negación de servicio y

- Generar al interior de la entidad un grado adecuado de compromiso con los lineamientos de administración de seguridad.

- Realizar una evaluación y gestión de riesgos relacionada con Gestión de la disponibilidad.

5. MARCO LEGAL

Se puede consultar en el – Mapa de procesos – Tecnología de Información y Comunicaciones – Normograma o en el campo de documentos asociados cuando se consulta el documento.

6. REQUISITOS TÉCNICOS

- Libros de ITIL® v3, en específico Diseño del Servicio (Service Design).

- Marco de Trabajo Operativo de Microsoft (MOF).
- Estándar ISO/IEC 27001.

7. DOCUMENTOS ASOCIADOS

Se puede consultar en el – Mapa de procesos – Documentos y formatos o en el campo de documentos asociados cuando se consulta el documento.

8. RESPONSABLE DEL DOCUMENTO

José Ramón Iglesias. Grupo de Gobierno Digital.