Gestión de la seguridad de la información & datos personales:

Un proceso holístico que abarque desde la planeación hasta la evaluación de la seguridad de la información

Gestión de la seguridad de la información & datos personales: 3 procedimientos principales

1

Planeación de la gestión de la seguridad de la información

Establecer la estrategia de la gestión de seguridad de la información de la Agencia a través de la definición y actualización de sus componentes, tales como: Objetivos y alcance, políticas, guías metodológicas y planes de acción

2

Operación de la gestión de la seguridad de la información

Asegurar la gestión de seguridad de información a través de la ejecución de los planes de acción, la implementación de controles aplicables y la atención de requerimientos, con el fin de proteger la información de la Agencia y mantener los niveles de riesgo dentro de los límites de tolerancia establecidos

3

Evaluación de la gestión de la seguridad de la información

Efectuar el análisis, evaluación y divulgación del desempeño de la gestión de la seguridad de la información en la Agencia de acuerdo con lo definido en su plan de gestión y lo realizado en la operación, con el fin de identificar el grado de cumplimiento de los objetivos planteados

Gestión de la seguridad de información & de datos personales

Procedimiento 1: Planeación de la gestión de la seguridad de la información

Objetivo

Establecer la estrategia de la gestión de seguridad de la información de la Agencia a través de la definición y actualización de sus componentes, tales como: Objetivos y alcance, políticas, guías metodológicas y planes de acción

Actividad	Descripción
Analizar el contexto interno y externo de la Agencia	• Internos y externos que pueden tener impacto en la gestión de la seguridad de la información. • Interno: Misión y visión, objetivos y metas, estrategia, riesgos, indicadores, lineamientos y políticas. • Externo: Evaluación de tendencias, mejores prácticas del sector, marco regulatorio, competencia y clientes.
Definir y actualizar la metodología para la implementación de la seguridad de la información	• Conjunto a los equipos del *Chief Information Security Officer* y el equipo técnico definir los parámetros, criterios, protocolos o técnicas requeridas para garantizar la seguridad y protección de los datos
Definir y actualizar los componentes de seguridad de información	• Conjunto a los equipos del *Chief Information Security Officer* y el equipo técnico definir las políticas, objetivos y alcance, estrategia, planes de acción
Divulgar los componentes de Seguridad de la Información	• Crear y ejecutar una estrategia de comunicación para todos los empleados de AAD para explicar la importancia de la seguridad de la información en la agencia y sus respectivos componentes

Gestión de la seguridad de información & de datos personales

Procedimiento 2: Operación de la gestión de la seguridad de la información

Objetivo

Asegurar la gestión de seguridad de información a través de la ejecución de los planes de acción, la implementación de controles aplicables y la atención de requerimientos, con el fin de proteger la información de la Agencia y mantener los niveles de riesgo dentro de los límites de tolerancia establecidos

Actividad	Descripción
Ejecutar planes de acción	• Ejecutar los planes de acción definidos en procedimiento 1 • Presentar estado de avance del plan de acción y potenciales obstáculos en caso de ser necesario
Gestión de activos	• Clasificar los activos de la agencia según su nivel de criticidad para el negocio con el fin de proporcionar un manejo adecuado de los mismos
Gestión de riesgos	• Clasificar los potenciales riesgos a enfrentar respecto a la seguridad de la información y datos personales • Gestionar adecuadamente los riesgos de la agencia cumpliendo con los indicadores y estándares establecidos
Gestión de incidentes	• Resolver cualquier incidente de seguridad de la información y datos personales de una manera efectiva recopilando toda la información necesaria para identificar la causa raíz del incidente
Captura de información de base de datos personales	• Asegurar procesos de captura de datos personales de una manera segura y acorde a los criterios de seguridad definidos
Administración de Base de Datos Personales	• Garantizar la gestión de datos personales de una manera segura y acorde a los criterios de seguridad definidos
Integración de Datos	• Integrar datos de una manera segura cumpliendo con las políticas y criterios de seguridad definidos
Inventario de Base de Datos Personales	• Mantener un inventario actualizado de las bases de datos personales acorde a los criterios de seguridad definidos
Realizar reporte de gestión	• Reporte de la gestión y los resultados obtenidos en la resolución de la necesidad

Gestión de la seguridad de información & de datos personales

Procedimiento 3: Evaluación de la gestión de la seguridad de la información

Objetivo

Efectuar el análisis, evaluación y divulgación del desempeño de la gestión de la seguridad de la información en la Agencia de acuerdo con lo definido en su plan de gestión y lo realizado en la operación, con el fin de identificar el grado de cumplimiento de los objetivos planteados.

Actividad	Descripción
Recibir y consolidar la información de la gestión	• Reportes de gestión generados en el Procedimiento 2.
Evaluar la gestión de la seguridad de la información	• Garantizar y realizar una evaluación proactiva de la seguridad de la información dentro de la agencia • Análisis y evaluación integral de la gestión de la seguridad de la información de la Agencia. Ejemplos de criterios: – Analizar las necesidades de seguridad de información recibidas según el tipo de gestión (requerimientos, planes de acción para la atención de iniciativas y proyectos, incidentes, controles) – Revisar la adecuada aplicación de la política, planes de acción, guía metodológica de gestión de Seguridad de la información – Analizar los resultados y efectividad de la resolución de la necesidad
Elaborar y avalar informe de resultados	• Informe con recomendaciones a los Procedimientos 1 y 2
Divulgar informe de resultados	• Comunicar proactivamente los resultados de la evaluación respecto a la seguridad de la información en la agencia a todas las partes interesadas