DEPARTAMENTO ADMINISTRATIVO

DE LA DEFENSORÍA DEL ESPACIO PÚBLICO

Manual de roles y responsabilidades de seguridad de la información

Código: 127-MANGI-02

Vigencia desde: 19/03/2019

Versión: 1

ALCALDÍA MAYOR DE BOGOTÁ D.C.

BOGOTÁ MEJOR PARA TODOS

CONTENIDO

1. INTRODUCCIÓN

El Modelo de Seguridad y Privacidad de la Información - MSPI el cual hace parte de la política de gobierno digital establece una serie de actividades y recursos con el propósito de implementar medidas que contribuyan con la seguridad de la información del DADEP. En tal sentido, se hace relevante planificar, implementar y controlar los procesos necesarios para dar cumplimiento a los requisitos de seguridad de la información.

Establecer el gobierno de seguridad de la información es una actividad estratégica de la cual hace parte toda la entidad. Allí se deben definir y asumir funciones, roles y responsabilidades dentro del personal a distintos niveles de la estructura organizacional de modo que logren los objetivos y metas que contribuyan con la confidencialidad, integridad y disponibilidad de la información.

2. OBJETIVO

Identificar roles de los funcionarios y/o contratistas para establecer funciones al interior del DADEP enfocados a la ejecución de actividades que propendan por la seguridad de los activos de información de la entidad

2.1 OBJETIVOS ESPECÍFICOS

- Tomar conciencia sobre la importancia de la seguridad de la información al interior de la entidad.
- Trabajar de manera proactiva acerca de la seguridad de la información.
- Gestionar de manera adecuada los riesgos, eventos o incidentes de seguridad que afecten los activos de información.

3. ALCANCE

El alcance de la guía de roles y responsabilidades de seguridad de la información está dada por la definición de funciones y actividades a realizar acerca de la administración y gestión de la seguridad de la información. Para esto, son asignadas responsabilidades a los distintos niveles organizacionales con la finalidad de contribuir con entornos de seguridad eficientes y efectivos.

4. DEFINICIONES Y SIGLAS

Para la adecuada gestión de riesgos de seguridad de la información se debe manejar con propiedad los siguientes términos:

- Activo: En relación a la seguridad de la información, se entiende como cualquier información o elementos tecnológicos que tienen relación directa con la información (sistemas de información, servicios tecnológicos, archivos físicos, archivos digitales, infraestructura tecnológica incluso personas) que tenga valor para la organización.

- BIA: “Bussiness Impact Analysis” Análisis de impacto al negocio.

- CIO: “Chief Information Officer” Oficial/Director de tecnologías de la información

- CISO: “Chief Information Security Officer” Oficial/Director de seguridad de la información

- COLCERT: Grupo de Respuesta a Emergencias Cibernéticas de Colombia

- Confidencialidad de la información: Propiedad que determina que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados.

- CSIRT: “Computer Security Incident Response Team” Equipo de Respuesta a Incidentes de Seguridad Informática

- Disponibilidad de la información: Propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada.

- Evento de seguridad: Se entiende como cualquier evento relacionado con la seguridad de la información que pueda llegar a afectar uno o varios activos de información.

- Incidente de Seguridad Es la materialización de un evento de seguridad que afecta la integridad, disponibilidad o confidencialidad de la información.

- Integridad de la información: Propiedad de salvaguardar la exactitud y estado completo de los activos de información.

- Riesgos de seguridad de la información: Es el potencial de que una o varias amenazas se materialicen causando daños a uno o un grupo de activos de información.

5. ROLES Y RESPONSABILIDADES

La gestión de la seguridad de la información establece una serie de componentes, directrices, procesos, procedimiento y actividades encaminados a la protección de la información que apoyan el desarrollo de las funciones de la Entidad. De este modo, a través de una estrategia integral, los objetivos de la seguridad de la información deberán estar articulados con los objetivos y metas propuestos a corto, mediano y largo plazo por el **DADEP.**

Resulta importante al interior de la entidad generar una cultura organizacional con la definición de roles y responsabilidades que permita una adecuada gestión de la seguridad de la información por medio de la coordinación de esfuerzos entre los funcionarios y/o contratistas de las diferentes dependencias al interior de la entidad en función de propiciar medidas de protección sobre los datos e información de la entidad. Para tal fin, esta guía propone una serie de responsabilidades asociadas a cada cargo y roles que se deben desempeñar de la siguiente manera:

ROL	RESPONSABILIDADES
Director DADEP CEO	• Compromiso en la asignación de recursos en materia de seguridad. • Velar por el uso apropiado de los recursos de seguridad. • Aprobación de políticas, mecanismos de supervisión y métricas de seguridad. • Supervisa el cumplimiento de las obligaciones regulatorias o de Ley en temas relacionados con seguridad de la información. • Facilitar integración entre las actividades de seguridad con dueños y gestores de procesos. • Garantiza que las acciones y procedimientos de respuesta a riesgos e incidentes cumplen con los requerimientos legales y regulatorios. • Se encarga de las comunicar tanto a las partes internas como externas el impacto de la materialización de incidentes, así como las acciones de respuesta. • tomar decisiones sobre el tratamiento del riesgo. • Realiza seguimiento sobre las acciones correctivas y preventivas en torno a los riesgos, incidentes y problemas de la seguridad de la información.
Oficial de Seguridad de la Información CISO	• Alinea objetivos de seguridad de la información con los objetivos propuestos por el DADEP • Desarrolla y mantiene la gestión de la seguridad de la información. • Gestiona de manera activa los riesgos e incidentes que afecten la seguridad de la información. • Contribuye en la definición de medidas proactivas y reactivas para controlar los niveles de riesgo. • Coordina los recursos asociados para la seguridad de la información. • Asume responsabilidad sobre el plan de respuesta a incidentes. • Prepara informes sobre la respuesta a incidentes que afectan la seguridad. • Reporta incidentes ante el COLCERT y el CAI virtual cuando el incidente sea crítico o cause impacto considerable para la Institución. • Mantiene comunicación con entidades externas que gestionen incidentes de seguridad COLCERT, CAI virtual, CSIRT Gobierno

	• Define metodología y establece plan para capacitaciones y fomento de la sensibilización en seguridad de la información. • Define cronograma de actividades relacionadas con la seguridad de la información. • Hace seguimiento y participa en el desarrollo de actividades de seguridad de la información. • Mantiene y hace continúo seguimientos a la política de seguridad de la información y al manual de políticas definidas que contribuyan a garantizar la disponibilidad, integridad y confidencialidad. • Establece metodologías, procesos y procedimientos relacionados con la seguridad de la información. • Responsable de dar cumplimiento de las obligaciones de Ley o regulatorias relacionadas con la seguridad de la información. • Comunica, sensibiliza y capacita a funcionarios y contratistas sobre temas que contribuyan con la seguridad de la información.
Gestor / Responsable del Proceso	• Toman decisiones sobre los asuntos relacionados a los activos de información en la identificación de riesgos o cuando ocurre un incidente de seguridad de la información. • Ofrecen entendimiento claro sobre el impacto del negocio en los procesos por medio del análisis de impacto al negocio BIA o en el plan de respuesta a incidente. • Verifica de manera continua la integridad, confidencialidad e integridad de la información productos de los procesos de su área o dependencia. • Mantiene actualizado el inventario de activos de información, así como los niveles de integridad, disponibilidad y confidencialidad. • Establece niveles y tipos de acceso de los usuarios sobre los diferentes activos de información. • Es el encargado de eliminar o solicitar la eliminación de usuarios que tienen acceso a los diferentes sistemas de información.
Jefe Oficina de Sistemas CIO	• Proporciona apoyo en la resolución de riesgos e incidentes de seguridad. • Gestionar los recursos en la medida que contribuya a la implementación de controles orientados a mitigar los riesgos velando por la protección los activos de información. • Participa y coordina funciones de la seguridad de la información.
Ingeniero de TI	• Proporcionar solución de eventos o incidentes que atenten contra la seguridad de la información. • Realizar labores de investigación sobre medidas para atender riesgos y demás factores de seguridad. • Ayuda a determinar fallos que afecten la seguridad de la información. • Proporciona información para la documentación en procesos de seguridad e incidentes. • Contribuye con la toma de evidencias digitales y con la cadena de custodia.

	• Implementa medidas para la gestión de seguridad de la información y de respuesta a incidentes. • Mantiene herramientas de Tecnologías de la Información, servicios tecnológicos y sistemas de información en condiciones óptimas de acuerdo a las políticas y mejores prácticas del DADEP. • Realiza monitoreo sobre el funcionamiento y la capacidad de los recursos tecnológicos. • Mantiene listado actualizado de usuarios sobre los recursos tecnológicos incluidos los permisos y niveles de acceso.
Gestor de Riesgos	• Trabaja en equipo junto con los dueños o gestores de proceso y la dirección sobre la gestión de riesgos. • Suministra información relacionada con el análisis de impacto al negocio. • Valora la implementación de controles como medida de protección sobre los activos. • Establece medidas para gestionar los riesgos.
Ingeniero Mesa de Ayuda	• Atiende incidentes o eventos de seguridad de la información de bajo nivel. • Apoyar la recolección de información y documentación sobre afectaciones a la seguridad de la información. • Consolidar la atención a eventos e incidentes de seguridad de la información.
Auditor	• Realiza seguimiento y evaluación a la implementación del Sistema de Gestión de Seguridad de la Información o Modelo de Seguridad y Privacidad de la Información. • Genera acciones de mejora sobre la seguridad de la información • Contribuye con la identificación de amenazas y vulnerabilidades.
Usuario	• Es responsable de velar por la preservación, protección y debido uso de los activos de información. • Reportar eventos o posibles incidentes que afecten la integridad, disponibilidad y confidencialidad de los activos de información • Debe adoptar y aplicar los controles definidos en el manual de gestión de seguridad de la información y política de seguridad de la información • Hacer uso de la información solo con propósitos autorizados y en función del desarrollo de actividades propias del DADEP.

Proyectó: Carlos Rojas Villamil, Contratista, Oficina de Sistemas
Elaboró: Carlos Rojas Villamil, Contratista, Oficina de Sistemas
Revisó: Isaías Sánchez Rivera Jefe Oficina Asesora de Planeación - Luis Fernando Arango Vargas Profesional Oficina Asesora de Planeación
Aprobó: Julio Alexander Hernández Martínez Jefe Oficina de Sistemas
Código de archivo: 140155

CONTROL DE CAMBIOS		
VERSIÓN	**FECHA**	**DESCRIPCIÓN DE MODIFICACIÓN**
1	26/03/2019	N/A