PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Alcaldía Distrital de Cartagena de Indias

TABLA DE CONTENIDO

INTRODUCCIÓN

Reconociendo la importancia de la información y apoyados en su significado, como el conjunto organizado de datos generados, obtenidos, transformados o controlados que constituyen un mensaje sin importar el medio en que se contenga (digital y no digital); nace la necesidad de definir normativas y buenas prácticas para su tratamiento general dentro de la entidad.

Mediante este plan se indicarán las medidas que implementará la Alcaldía Distrital de Cartagena de Indias, para garantizar la seguridad y privacidad de la información que se maneja, según lo establecido en el decreto 1008 del 14 de junio de 2018; por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del decreto 1078 de 2015, decreto único reglamentario del sector de Tecnologías de la Información y las Comunicaciones.

2. ALCANCE

El Modelo de Seguridad y Privacidad de la Información que se generará mediante este plan se aplicará para todo activo de información integrado en los procesos de la entidad, los cuales incluyen: funcionarios, contratistas, sistemas de información, equipo de cómputo, servidores y todo lo que se incluya en el inventario de activos de información del modelo en la entidad.

3. OBJETIVO GENERAL

Establecer un plan que permitirá la construcción, implementación y puesta en marcha de un Modelo de Seguridad y Privacidad de la información por medio del cual se manifiesta la posición de la Alcaldía Distrital de Cartagena de Indias con respecto a la importancia que tienen los activos de información para el funcionamiento de la entidad a beneficio de todas las partes interesadas.

3.1 Objetivos específicos

- ✓ Elevar los índices de transparencia como entidad pública del territorio colombiano.
- ✓ Crear las políticas y procedimientos en materia de seguridad y privacidad de la información.
- ✓ Mejorar los tiempos y la calidad de respuesta en los procesos de la entidad.
- ✓ Generar una cultura de seguridad y privacidad de la información en los funcionarios, contratistas y ciudadanos.
- ✓ Minimizar los riesgos asociados con los activos de información.
- ✓ Garantizar la continuidad del negocio frente a incidentes.

4. PRINCIPIOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

✓ Proteger la información generada, procesada o resguardada por los procesos de negocio y activos de información que hacen parte de estos.
✓ Proteger la información creada, procesada, transmitida o resguardada por sus procesos de negocio, con el fin de minimizar impactos financieros, operativos o legales debido a un uso incorrecto de esta. Para ello es fundamental la aplicación de controles de acuerdo con la clasificación de la información de su propiedad o en custodia.
✓ Proteger su información de las amenazas originadas por parte del personal.
✓ Proteger las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos.
✓ Controlar la operación de sus procesos de negocio garantizando la seguridad de los recursos tecnológicos y las redes de datos.
✓ Implementará control de acceso a la información, sistemas y recursos de red.
✓ Garantizar que la seguridad sea parte integral del ciclo de vida de los sistemas de información.
✓ Garantizar a través de una adecuada gestión de los eventos de seguridad y las debilidades asociadas con los sistemas de información una mejora efectiva de su modelo de seguridad.
✓ Garantizar la disponibilidad de sus procesos de negocio y la continuidad de su operación basada en el impacto que pueden generar los eventos.
✓ Garantizar el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas.
✓ Definir, implementar, operar y mejorar de forma continua un modelo de seguridad y privacidad de la información, soportado en lineamientos claros alineados a las necesidades de las partes interesadas, y a los requerimientos regulatorios que le aplican a su naturaleza.

5. ACTIVIDADES

A continuación, se describen las actividades que se ejecutarán junto con los respectivos entregables, en aras de cumplir con los objetivos propuestos:

FASE	ACTIVIDADES	ENTREGABLE/RESULTADO
FASE DE DIAGNÓSTICO	Determinar el estado actual de la gestión de seguridad y privacidad de la información al interior de la entidad.	Documento del diagnóstico.
	Identificar el nivel de madurez de seguridad y privacidad de la información en la entidad	

	Identificar vulnerabilidades que sirvan como insumo para la fase de planificación.	
FASE DE PLANIFICACIÓN	Identificar el alcance y objetivos de seguridad y privacidad de la información	Documento con la política de seguridad de la información.
	Política de seguridad y privacidad de la información	
	Roles y responsabilidades de seguridad y privacidad de la información.	
	Políticas de seguridad y privacidad de la información	Manual con las políticas y procedimientos de seguridad y privacidad de la información.
	Procedimientos de seguridad de la información.	
	Inventario de activos de información.	Documento con la metodología para identificación, clasificación y valoración de activos de información.
		Matriz con la identificación, valoración y clasificación de activos de información.
	Identificación, valoración y tratamiento de riesgo.	Documento con el plan de tratamiento de riesgos.
		Documento con la declaración de aplicabilidad.
		Matriz de riesgos
	Plan de comunicaciones.	Documento con el plan de comunicación, sensibilización y capacitación para la entidad.
FASE DE IMPLEMENTACIÓN	Planificación y control operacional.	Documento con la estrategia de planificación y control operacional, revisado y aprobado por la alta Dirección.
	Implementación del plan de tratamiento de riesgos.	Informe de la ejecución del plan de tratamiento de riesgos aprobado por el dueño de cada proceso.
	Indicadores de gestión.	Documento con la descripción de los indicadores de gestión de seguridad y privacidad de la información.
FASE DE EVALUACIÓN DE DESEMPEÑO	Plan de revisión y seguimiento, a la implementación del MSPI.	Documento con el plan de seguimiento y revisión del MSPI revisado y aprobado por la alta Dirección.

	Plan de ejecución de auditorias	Documento con el plan de ejecución de auditorías y revisiones independientes al MSPI, revisado y aprobado por la Alta Dirección.
FASE DE MEJORA CONTINUA	Plan de mejora continua	Documento con el plan de mejoramiento.
		Documento con el plan de comunicación de resultados.

6. ROLES Y RESPONSABILIDADES

Los funcionarios y contratistas de la Alcaldía Distrital de Cartagena de Indias deberán asumir siguientes roles y responsabilidades, donde se garantice la implementación, revisión y mejora continua del Modelo de Seguridad y Privacidad de la Información al interior de la Entidad.

6.1 Alcalde

- Aprobar y verificar del cumplimiento de las políticas y procedimientos de seguridad y privacidad de la información.
- Hacer que los miembros del comité directivo sean conscientes de la criticidad de los activos de información para el desarrollo de los procesos de la Entidad.
- Divulgar las responsabilidades de seguridad y privacidad de la información de la entidad con base en los lineamientos del MSPI.

6.2 Nivel directivo – Secretarios, asesores, directores y jefe de oficinas

- Liderar y apoyar de mejora continua para la aplicación del MSPI al interior de la dependencia a cargo.
- Alineación de los objetivos de la dependencia para que su cumplimiento este apoyado por el MSPI.
- Asignar y verificar el cumplimiento de las funciones y responsabilidades de seguridad y privacidad de la información para los roles definidos en la dependencia a cargo.
- Proveer los recursos necesarios para la implementación del MSPI al interior de la dependencia a cargo.
- Apoyar la capacitación y entrenamiento requerido para que los funcionarios y contratistas de la dependencia a cargo que cumplan con el MSPI.

- Aplicar el proceso disciplinario ante los incidentes de seguridad y privacidad de la información originada por un funcionario o contratista de la dependencia a cargo.

6.3 Líder de seguridad y privacidad de la información – Jefe de oficina asesora de informática (Establecido en el Decreto 1409 de 2018)

- Liderar y apoyar la mejora continua para la aplicación del MSPI al interior de la Alcaldía.
- Asignar dentro de su equipo de trabajo quien servirá como oficial de seguridad y privacidad de la información.
- Apoyar las actividades relacionadas con el MSPI.

6.4 Oficial de seguridad y privacidad de la información

- Apoyar en definir y actualizar el inventario de los activos de información.
- Realizar análisis de riesgos de seguridad y privacidad de la información con base en lo establecido en el MSPI.
- Apoyar en definir del plan de tratamiento de los riesgos de seguridad y privacidad de la información.
- Velar por la ejecución del plan de tratamiento de los riesgos de seguridad y privacidad de la información.
- Definir, actualizar y difundir las políticas, procedimientos y formatos del MSPI.
- Definir y generar las métricas de seguridad y privacidad de la información establecida en el MSPI.
- Propender una cultura de seguridad y privacidad de la información al interior de la entidad.

Lo anterior es responsabilidad del oficial de seguridad y privacidad de la información, pero debe contar con la participación de todos los funcionarios y contratistas de la Alcaldía Distrital de Cartagena de Indias.

6.5 Mesa de trabajo de seguridad y privacidad de la información

- Validar la documentación propia del MSPI dentro de la dependencia que representa.
- Fomentar dentro de su dependencia la práctica de directrices de seguridad y privacidad de información.
- Apoyar la identificación y actualización del inventario de activos de información y riesgos de estos.

- Apoyar la identificación e implementación de controles para la mitigación de riesgos de seguridad y privacidad de información.
- Participar en las jornadas de implementación, mantenimiento y mejora del MSPI.

6.6 Funcionarios y contratistas

Todos los funcionarios y contratistas vinculados a la Alcaldía tendrán la responsabilidad de velar por la confidencialidad, integridad, disponibilidad y privacidad de la información que maneje, así mismo debe reportar los incidentes de seguridad, eventos sospechosos o un mal uso de los recursos que identifique.

El incumplimiento a la política general de seguridad y privacidad de la información traerá consigo, las consecuencias legales que apliquen a la normativa de la entidad, incluyendo lo establecido en las normas que competen al Gobierno Nacional y Territorial en cuanto a seguridad y privacidad de la información se refiere.

7 GLOSARIO

Para efectos de entendimiento de la presente política general seguridad y privacidad de la información, es importante tener en cuenta los siguientes términos y definiciones:

✓ **Acceso remoto**: conexión con los recursos informáticos de la entidad desde una ubicación remota a través de una red pública.
✓ **Activos de información:** son aquellos recursos con los que cuenta una empresa. Es decir, todo elemento que compone el proceso completo de comunicación, partiendo desde la información, el emisor, el medio de transmisión y receptor.
✓ **Amenaza:** causa potencial de incidente no deseado, el cual puede resultar en daño al Sistema o a la Organización. [Fuente: ISO 27000].
✓ **Brecha**: se denomina al espacio o ruta a recorrer entre un estado actual y un estado deseado.
✓ **Calidad:** es la cualidad de un conjunto de información recogida, que reúne entre sus atributos la exactitud, completitud, integridad, actualización, coherencia, relevancia, accesibilidad y confiabilidad necesarias para resultar útiles al procesamiento, análisis y cualquier otro fin que un usuario quiera darles.
✓ **Confidencialidad:** propiedad que impide la divulgación de información a individuos, entidades o procesos no autorizados, asegurando el acceso a la información únicamente a aquellas personas que cuenten con la debida autorización.

✓ **Conservación:** mantener y cuidar la información para que no pierda sus características y propiedades con el paso del tiempo.

✓ **Disponibilidad:** característica, cualidad o condición de la información de encontrarse a disposición de quienes deben acceder a ella, ya sean personas, procesos o aplicaciones.

✓ **Dispositivo móvil:** son todos los equipos tecnológicos que acceden a Internet, tales como: portátiles, teléfonos IP, celulares, TV, tabletas, entre otros.

✓ **Entrenamiento**: proceso utilizado para enseñar habilidades, que permitan a una persona ejecutar funciones específicas asignadas su cargo u objeto contractual.

✓ **Equipos de cómputo:** se reconoce como los portátiles o computadores de escritorios que se le asigna a un funcionario o contratista de la entidad.

✓ **Estándar:** regla que especifica una acción o respuesta que se debe seguir a una situación dada. Los estándares son orientaciones obligatorias que buscan hacer cumplir las políticas. Los estándares son diseñados para promover la implementación de las políticas de alto nivel de la entidad antes de crear nuevas políticas.

✓ **Información:** conjunto organizado de datos generados, obtenidos, adquiridos, transformados o controlados que constituyen un mensaje sin importar el medio que lo contenga (digital y no digital).

✓ **Ingeniería social:** técnica que utilizan las personas para obtener información, acceso o privilegios en sistemas de información, permitiendo que algún acto perjudique o exponga a la persona o entidad.

✓ **Integridad:** propiedad que busca mantener los datos libres de modificaciones no autorizadas. A grosso modo, la integridad es mantener con exactitud la información tal cual fue generada, sin ser manipulada ni alterada por personas o procesos no autorizados.

✓ **Monitoreo**: verificación, supervisión, observación crítica o determinación continua del estado con el fin de identificar cambios con respecto al nivel de desempeño exigido o esperado.

✓ **MSPI:** Modelo Seguridad y Privacidad de la Información.

✓ **Política:** declaración de alto nivel que describe la posición de la entidad sobre un tema específico.

✓ **Privacidad de la información:** es el aspecto que se ocupa de la capacidad que una organización o individuo tiene para determinar qué datos pueden ser compartidos con terceros.

✓ **Procedimiento:** define específicamente como las políticas, estándares, mejores prácticas y guías que serán implementadas en una situación dada.

✓ **Propietario del activo:** persona o cargo que administra, autoriza el uso, regula o gestiona el activo de información. El propietario del activo aprueba el nivel de protección requerido frente a confidencialidad, integridad y disponibilidad.

✓ **Riesgo:** efecto de la incertidumbre sobre los objetivos. Un efecto es una desviación de aquello que se espera, sea positivo, negativo o ambos. Los objetivos pueden tener aspectos diferentes (económicos, de imagen, medio ambiente) y se pueden aplicar a niveles diferentes (estratégico, operacional, toda la organización). [Fuente: ISO 31000]

✓ **Sensibilización**: es un proceso que tiene como objetivo principal impactar sobre el comportamiento de una población o reforzar buenas prácticas sobre algún tema en particular.

✓ **Seguridad de la información:** preservación de la confidencialidad, integridad y disponibilidad de la información. NTC-ISO/IEC 27001.

✓ **Teletrabajo:** En Colombia, el teletrabajo se encuentra definido en la Ley 1221 de 2008 como: "Una forma de organización laboral, que consiste en el desempeño de actividades remuneradas o prestación de servicios a terceros utilizando como soporte las tecnologías de la información y comunicación -TIC- para el contacto entre el trabajador y la empresa, sin requerirse la presencia física del trabajador en un sitio especifico de trabajo".

✓ **TIC:** Tecnologías de la Información y Comunicaciones.

✓ **Vulnerabilidad:** debilidad identificada sobre un activo y que puede ser aprovechado por una amenaza para causar una afectación sobre la confidencialidad, integridad y/o disponibilidad de la información.

8 VIGENCIA Y CONTROL DE CAMBIOS

FECHA	AUTOR	VERSION	CAMBIOS
30 de enero 2020	Oficina Asesora de Informática	1.0	Versión inicial.