ALCALDÍA MAYOR DE CARTAGENA DE INDIAS
FONDO DE VIVIENDA DE INTERÉS SOCIAL Y REFORMA URBANA DISTRITAL
CORVIVIENDA

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN
2021

CARTAGENA DE INDIAS

TABLA DE CONTENIDO

INTRODUCCIÓN

En consecuencia a 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, el Fondo de Vivienda de Interés Social y Reforma Urbana – Corvivienda, procede a definir normativas y buenas prácticas para el tratamiento de la información dentro de la entidad.

Mediante este plan se indicarán las medidas que se implementará que pretende garantizar la seguridad y privacidad de la información que maneja la institución.

2. ALCANCE

El plan que se diseñará incluirá los siguientes actores: funcionarios, contratistas, sistemas de información, equipo de cómputo, servidores y todo lo que se incluya en el inventario de activos de información de la entidad.

3. OBJETIVO GENERAL

Elaborar un plan que permita definir, implementar y controlar, un marco normativo de buenas prácticas en el buen uso de la información dando cumplimiento a lo planteado en el decreto 1008 del 14 de junio de 2018.

3.1. Objetivos Específicos:

Realizar el diagnóstico de la situación actual del Sistema de Gestión de Seguridad y Privacidad de la Información al interior de la entidad, así como detectar posibles vulnerabilidades.

Establecer alcance, roles, responsabilidades, políticas, procedimientos y demás elementos que permitan construir un marco normativo al interior de la institución.

Determinar el estado de los activos de información, identificación, valoración y tratamiento de riesgos dentro de la Entidad.

Diseñar e implementar controles para mitigar, minimizar o transferir los riesgos de Seguridad y Protección de la información en cada una de las áreas.

Evaluar el desempeño de las herramientas, políticas y controles implementados en el Sistema de Gestión de Seguridad y Privacidad de la Información

4. PRINCIPIOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Confidencialidad: Es la propiedad que impide la divulgación de información a individuos, entidades o procesos no autorizados. A grandes rasgos, asegura el acceso a la información únicamente a aquellas personas que cuenten con la debida autorización.

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

Disponibilidad: Es la característica, cualidad o condición de la información de encontrarse a disposición de quienes deben acceder a ella, ya sean personas, procesos o aplicaciones. A grandes rasgos, la disponibilidad es el acceso a la información y a los sistemas por personas autorizadas en el momento que así lo requieran.

Autenticidad: Es la propiedad que permite identificar el generador de la información. En un sistema informático se suele conseguir este factor con el uso de cuentas de usuario y contraseñas de acceso.

5. ACTIVIDADES

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

ACTIVIDAD	DESCRIPCIÓN		ENTREGABLE	
FASE DE DIAGNÓSTICO	1	Determinar el estado actual de la gestión de seguridad y privacidad de la información al interior de la entidad.	1	Documento del diagnóstico y análisis de vulnerabilidades
	2	Identificar vulnerabilidades que sirvan como insumo para la fase de planificación.		
FASE DE PLANIFICACIÓN	1	Identificar el alcance y objetivos de seguridad y privacidad de la información	1	Documento con la política de seguridad de la información.
	2	Roles y responsabilidades de seguridad y privacidad de la información.		
	3	Políticas de seguridad y privacidad de la información	2	Manual con las políticas y procedimientos de seguridad y privacidad de la información.
	4	Procedimientos de seguridad de la información.		

	5	Inventario de activos de información.	3	Documento con la metodología para identificación, clasificación y valoración de activos de información.
			4	Matriz con la identificación, valoración y clasificación de activos de información.
	6	Identificación, valoración y tratamiento de riesgo.	5	Documento con el plan de tratamiento de riesgos.
			6	Matriz de riesgos
	7	Plan de comunicaciones.	7	Documento con el plan de comunicación, sensibilización y capacitación para la entidad.
FASE DE IMPLEMENTACIÓN	1	Planificación y control operacional.	1	Documento con la estrategia de planificación y control operacional, revisado y aprobado por la alta Dirección.
	2	Implementación del plan de tratamiento de riesgos.	2	Informe de la ejecución del plan de tratamiento de riesgos aprobado por el dueño de cada proceso.
	3	Indicadores de gestión.	3	Documento con la descripción de los indicadores de gestión de seguridad y privacidad de la información.
FASE DE EVALUACIÓN DE DESEMPEÑO	1	Plan de revisión y seguimiento, a la implementación del MSPI.	1	Documento con el plan de seguimiento y revisión del MSPI revisado y aprobado por la alta Dirección.
	2	Plan de ejecución de auditorias	2	Documento con el plan de ejecución de auditorías y revisiones independientes al MSPI, revisado y aprobado por la Alta Dirección.
FASE DE MEJORA CONTINUA	1	Plan de mejora continua	1	Documento con el plan de mejoramiento.
	2		2	Documento con el plan de comunicación de resultados.

Fuente: Elaboración propia basado en la norma ISO 27001: Seguridad Informática

6. ROLES Y RESPONSABILIDADES

Los funcionarios y contratistas del Fondo de Vivienda de Seguridad Social y Reforma Urbana – "Corvivienda" 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.

RESPONSABLE	DESCRIPCIÓN	
GERENTE	1	Aprobar y verificar del cumplimiento de las políticas y procedimientos de seguridad y privacidad de la información.
	2	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.
	3	Divulgar las responsabilidades de seguridad y privacidad de la información de la entidad con base en los lineamientos del MSPI. (Modelo de Seguridad y Privacidad de la Información)
Asesores y jefe de oficinas	1	Liderar y apoyar de mejora continua para la aplicación del MSPI al interior de la dependencia a cargo.
	2	Alineación de los objetivos de la dependencia para que su cumplimiento este apoyado por el MSPI.
	3	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.
	4	Proveer los recursos necesarios para la implementación del MSPI al interior de la dependencia a cargo.
	5	Apoyar la capacitación y entrenamiento requerido para que los funcionarios y contratistas de la dependencia a cargo que cumplan con el MSPI.
	6	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.
Líder del proceso Gestión TIC	1	Liderar y apoyar la mejora continua para la aplicación del MSPI al interior de la Entidad
	2	Apoyar las actividades relacionadas con el MSPI.
	3	Apoyar en definir y actualizar el inventario de los activos de información.
	4	Realizar análisis de riesgos de seguridad y privacidad de la información con base en lo establecido en el MSPI.
	5	Apoyar en definir del plan de tratamiento de los riesgos de seguridad y privacidad de la información.
	6	Velar por la ejecución del plan de tratamiento de los riesgos de seguridad y privacidad de la información.
	7	Definir, actualizar y difundir las políticas, procedimientos y formatos del MSPI.
	8	Definir y generar las métricas de seguridad y privacidad de la información establecida en el MSPI.
	9	Propender una cultura de seguridad y privacidad de la información al interior de la entidad.
Mesa de trabajo de seguridad y privacidad de la información	1	Validar la documentación propia del MSPI dentro de la dependencia que representa.
	2	Fomentar dentro de su dependencia la práctica de directrices de seguridad y privacidad de información.

	3	Apoyar la identificación y actualización del inventario de activos de información y riesgos de estos.
	4	Apoyar la identificación e implementación de controles para la mitigación de riesgos de seguridad y privacidad de información.
	5	Participar en las jornadas de implementación, mantenimiento y mejora del MSPI.
Funcionarios y contratistas	1	Todos los funcionarios y contratistas vinculados a la Entidad 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.
	2	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.

Fuente: Elaboración propia, basado en PMBOK V6, capitulo StakeHolders

7. TÉRMINOS Y DEFINICIONES

A continuación, se listan algunos términos y definiciones de términos que se utilizarán durante el desarrollo de la gestión de riesgos de seguridad de la información, los cuales se encuentran en la Norma ISO 27001: Seguridad Informática.

- **Activo:** En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas...) que tenga valor para la organización.
- **Alcance:** Ámbito de la organización que queda sometido al SGSI.
- **Ataque:** Intento de destruir, exponer, alterar, deshabilitar, robar u obtener acceso no autorizado o hacer uso no autorizado de un activo.
- **Confidencialidad:** Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados.
- **Continuidad de la seguridad de la información:** Procesos y procedimientos para garantizar una operativa continuada de la seguridad de la información.
- **Control:** Medida por la que se modifica el riesgo. Los controles incluyen procesos, políticas, dispositivos, prácticas, entre otras acciones que modifican el riesgo. Es posible que los controles no siempre ejerzan el efecto de modificación previsto o supuesto. Los términos salvaguardan o contramedida son utilizados frecuentemente como sinónimos de control.
- **Criterio del riesgo:** Los criterios del riesgo se basan en los objetivos de la organización y el contexto externo y el contexto interno. Los criterios de riesgo pueden derivarse de estándares, leyes, políticas y otros requisitos.

- **Disponibilidad:** Propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada.
- **Evento de seguridad de la información:** Ocurrencia identificada del estado de un sistema, servicio o red de comunicaciones que indica una posible violación de la política de seguridad de la información o falla de los controles, o una situación previamente desconocida que puede ser relevante para la seguridad.
- **Fiabilidad:** Propiedad del comportamiento y de unos resultados consistentes previstos.
- **Gestión de incidentes de seguridad de la información:** Procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información.
- **Integridad:** Propiedad de la información relativa a su exactitud y completitud.
- **ISO/IEC 27001:** Norma que establece los requisitos para un sistema de gestión de la seguridad de la información (SGSI). Primera publicación en 2005; segunda edición en 2013. Es la norma en base a la cual se certifican los SGSI a nivel mundial.
- **Organización:** Persona o grupo de personas que tiene sus propias funciones con responsabilidades, autoridades y relaciones para lograr sus objetivos.
- **Profesional del sistema de gestión de seguridad de la información (SGSI):** Persona que establece, implementa, mantiene y mejora continuamente uno o más procesos del sistema de gestión de seguridad de la información.
- **Recursos de tratamiento de información:** Cualquier sistema, servicio o infraestructura de tratamiento de información o ubicaciones físicas utilizadas para su alojamiento.
- **Rendimiento:** El rendimiento puede relacionarse con hallazgos cuantitativos o cualitativos. El rendimiento puede relacionarse con la gestión de actividades, procesos, productos (incluidos servicios), sistemas u organizaciones.
- **Requisito:** Necesidad o expectativa que es establecida, generalmente de forma implícita u obligatoria.
- **Riesgo:** Efecto de la incertidumbre sobre los objetivos. Un efecto es una desviación de lo esperado: positivo o negativo. La incertidumbre es el estado, incluso parcial, de deficiencia de información relacionada con la comprensión o conocimiento de un evento, su consecuencia o probabilidad.
- **Seguridad de la información:** Preservación de la confidencialidad, integridad y disponibilidad de la información.
- **Sistema de Información:** Conjunto de aplicaciones, servicios, activos de tecnología de la información u otros componentes que manejan información.
- **Trazabilidad:** Cualidad que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sean asociadas de modo inequívoco a un individuo o entidad.
- **Vulnerabilidad:** Debilidad de un activo o control que puede ser explotada por una o más amenazas.

8. MARCO LEGAL

Con el propósito de implementar un Sistema de Gestión de Seguridad de la Información, toda organización debe obligatoriamente cumplir con todas las leyes, normas, decretos, etc. que sean aplicables en el desarrollo de sus actividades. Estas son las Leyes vigentes al día de hoy:

Derechos de Autor
Decisión 351 de la C.A.N.
Ley 23 de 1982
Decreto 1360 de 1989
Ley 44 de 1993
Decreto 460 de 1995
Decreto 162 de 1996
Ley 545 de 1999
Ley 565 de 2000
Ley 603 de 2000
Ley 719 de 2001

Propiedad Industrial
Decisión 486 de la C.A.N.
Decreto 2591 de 2000
Ley 463 de 1998
Ley 170 de 1994
Ley 178 de 1994

Propiedad Intelectual
Decisión 345 de la C.A.N.
Decisión 391 de la C.A.N.
Decisión 523 de la C.A.N.

Comercio Electrónico y Firmas Digitales
Ley 527 de 1999
Decreto 1747 de 2000
Resolución 26930 de 2000

Seguridad de la Información
Ley 1273 de 2009

Elaborado por,
Equipo de Sistemas

Autentica,

ADM. CARLOS FERNÁNDEZ BARCENAS
JEFE OFICINA ASESORA DE PLANEACIÓN