ALCALDÍA MAYOR DE CARTAGENA DE INDIAS

FONDO DE VIVIENDA DE INTERÉS SOCIAL Y REFORMA URBANA DISTRITAL

CORVIVIENDA

PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

2021

CARTAGENA DE INDIAS

FONDO DE VIVIENDA DE INTERES SOCIAL Y REFORMA URBANA DISTRITAL- CORVIVI
Dir.: Manga 3ª Avenida, Calle 28 #21-62
Email: atencionalusuario@corvivienda.gov.co
wwww.corvivienda.gov.co
Tel: 301 4793336 - 301 4793290

TABLA DE CONTENIDO

INTRODUCCIÓN

De acuerdo a la Dirección de Gestión y Desempeño Institucional, la implementación de la gestión del riesgo, es necesario que cada entidad haga un análisis de las estrategias, la formulación de objetivos y la implementación de esos objetivos en la toma de decisiones cotidiana, lo que permitirá una identificación del riesgo adecuada a las necesidades de cada organización, con un enfoque preventivo que permita la protección de los recursos, alcanzar mejores resultados y mejorar la prestación de servicios a sus usuarios aspectos fundamentales frente a la generación de valor público, eje fundamental en el quehacer de todas las organizaciones públicas.

Es por ello que, basado en la quinta versión de la Guía para la administración del riesgo y el diseño de controles en entidades públicas, se diseña una hoja de ruta la cual se desarrollara durante el año 2021.

2. ALCANCE

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

3. OBJETIVO GENERAL

Diseñar e implementar el Sistema de Gestión de Riesgos de Seguridad y Privacidad de la Información, con el fin de minimizar, mitigar o transferir los riesgos a los cuales se expone la información, además de velar por el cumplimiento de los requerimientos legales, regulatorios y contractuales de la entidad.

3.1. Objetivos Específicos:

- Establecer los principios básicos y el marco general de actuación para el control y la gestión de los riesgos de seguridad y privacidad de la información a los que se enfrenta la entidad.
- Realizar de identificación de los riesgos de seguridad y privacidad de la información en la Entidad.
- Efectuar valoración de los riesgos identificados mediante la aplicación de herramientas y técnicas que permitan la elaboración de planes para mitigar, minimizar o transferirlos.

4. ACTIVIDADES

A continuación, se describen las actividades que se ejecutarán junto con los respectivos entregables, en aras de cumplir con los objetivos propuestos respecto a la Seguridad y Protección de la Información – SPI en la Institución:

ACTIVIDAD	DESCRIPCIÓN		ENTREGABLE	
Política de Administración de Riesgos	1	Lineamientos de la Política de Riesgos	1	Documento "Política de Administración de Riesgos SPI"
	2	Marco Conceptual Para el Apetito del Riesgo		
Identificación del Riesgo	1	Análisis de Objetivos Estratégicos y de los Procesos	1	Documento "Mapa de Riesgos SPI de la Entidad"
	2	Identificación de los Puntos de Riesgo		
	3	Identificación de Áreas de Impacto		
	4	Identificación de Áreas de Factores de Riesgo		
	5	Descripción del Riesgo		
	6	Clasificación del Riesgo		
Valoración del Riesgo	1	Análisis de Riesgos	1	Documento "Análisis, Evaluación y Estrategias para la mitigar, minimizar y/o transferir los riesgos SPI de la Institución"
	2	Evaluación de Riesgos		
	3	Estrategias Para Combatir el Riesgo		
	4	Herramientas Para la Gestión del Riesgo	2	Documento "Diseño de Herramientas para la Gestión, Monitoreo y Revisión de los riesgos SPI"
	5	Monitoreo y Revisión		

Lineamientos Sobre los Riesgos Relacionados Con Posibles Actos de Corrupción	1	Disposiciones Generales	1	Documento "Lineamientos Generales acerca de los riesgos de Corrupción en SPI"
	2	Generalidades Acerca de los Riesgos de Corrupción		
	3	Identificación del Riesgo de Corrupción	2	Documento "Identificación, Valoración y Estrategias de Mitigación de los riesgos de corrupción en SPI"
	4	Valoración del Riesgo		

Fuente: Elaboración propia basado en la Guía para la administración del riesgo y el diseño de controles en entidades públicas. V5

5. 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 Sistema de Gestión de Riesgos 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**

6. 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 Guía para la administración del riesgo y el diseño de controles en entidades públicas Versión 5:

- **Activo:** En el contexto de seguridad digital son elementos tales como aplicaciones de la organización, servicios web, redes, Hardware, información física o digital, recurso humano, entre otros, que utiliza la organización para funcionar en el entorno digital.
- **Apetito de riesgo:** Es el nivel de riesgo que la entidad puede aceptar, relacionado con sus Objetivos, el marco legal y las disposiciones de la Alta Dirección y del Órgano de Gobierno. El apetito de riesgo puede ser diferente para los distintos tipos de riesgos que la entidad debe o desea gestionar.
- **Capacidad de riesgo:** Es el máximo valor del nivel de riesgo que una Entidad puede soportar y a partir del cual se considera por la Alta Dirección y el Órgano de Gobierno que no sería posible el logro de los objetivos de la Entidad.
- **Causa:** todos aquellos factores internos y externos que solos o en combinación con otros, pueden producir la materialización de un riesgo.
- **Causa Inmediata:** Circunstancias bajo las cuales se presenta el riesgo, pero no constituyen la causa principal o base para que se presente el riesgo.
- **Causa Raíz:** Causa principal o básica, corresponde a las razones por la cuales
- se puede presentar el riesgo.
- **Confidencialidad:** Propiedad de la información que la hace no disponible o sea divulgada a individuos, entidades o procesos no autorizados.
- **Consecuencia:** Los efectos o situaciones resultantes de la materialización del riesgo que impactan en el proceso, la entidad, sus grupos de valor y demás partes interesadas.
- **Control:** Medida que permite reducir o mitigar un riesgo.
- **Disponibilidad:** Propiedad de ser accesible y utilizable a demanda por una entidad.
- **Factores de Riesgo:** Son las fuentes generadoras de riesgos.
- **Impacto:** las consecuencias que puede ocasionar a la organización la materialización del riesgo.
- **Integridad:** Propiedad de exactitud y completitud.
- **Nivel de riesgo:** Es el valor que se determina a partir de combinar la probabilidad de ocurrencia de un evento potencialmente dañino y la magnitud del impacto que este evento traería sobre la capacidad institucional de alcanzar los objetivos. En general la fórmula del Nivel del Riesgo poder ser Probabilidad * Impacto, sin embargo, pueden relacionarse las variables a través de otras maneras diferentes a la multiplicación, por ejemplo, mediante una matriz de Probabilidad – Impacto.

- **Plan Anticorrupción y de Atención al Ciudadano:** Plan que contempla la estrategia de lucha contra la corrupción que debe ser implementada por todas las entidades del orden nacional, departamental y municipal.
- **Probabilidad:** se entiende la posibilidad de ocurrencia del riesgo. Estará asociada a la exposición al riesgo del proceso o actividad que se esté analizando. La probabilidad inherente será el número de veces que se pasa por el punto de riesgo en el periodo de 1 año.
- **Riesgo:** Efecto que se causa sobre los objetivos de las entidades, debido a eventos potenciales. Los eventos potenciales hacen referencia a la posibilidad de incurrir en pérdidas por deficiencias, fallas o inadecuaciones, en el recurso humano, los procesos, la tecnología, la infraestructura o por la ocurrencia de acontecimientos externos.
- **Riesgo de Corrupción:** Posibilidad de que, por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado.
- **Riesgo de Seguridad de la Información:** Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000).
- **Riesgo Inherente:** Nivel de riesgo propio de la actividad. El resultado de combinar la probabilidad con el impacto, nos permite determinar el nivel del riesgo inherente, dentro de unas escalas de severidad.
- **Riesgo Residual:** El resultado de aplicar la efectividad de los controles al riesgo inherente.
- **Tolerancia del riesgo:** Es el valor de la máxima desviación admisible del nivel de riesgo con respecto al valor del Apetito de riesgo determinado por la entidad.
- **Vulnerabilidad:** Representan la debilidad de un activo o de un control que puede ser explotada por una o más amenazas.

Elaborado por,

Equipo de Sistemas

Autentica,

ADM. CARLOS FERNÁNDEZ BARCENAS

JEFE OFICINA ASESORA DE PLANEACIÓN