FONDECUN

FONDO DE DESARROLLO DE PROYECTOS DE CUNDINAMARCA

PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 2023

CUNDINAMARCA ¡REGIÓN Que Progresa!

Gobernación de Cundinamarca

Sede Administrativa
Av. Carrera 10 No. 28-49 Torre A, Piso 21
Teléfonos: 243 2328 / 243 2806

www.fondecun.gov.co
@fondecun

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

Contenido

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

1. INTRODUCCIÓN

La gestión de los riesgos de seguridad de la información son aquellos procesos que reducen las pérdidas y brindan protección de la información, permitiendo conocer las debilidades que afectan durante todo el ciclo de vida del servicio.

Es importante que dentro de las organizaciones el plan de tratamiento de riesgos de Seguridad y Privacidad de la información este orientado estratégicamente al desarrollo de una cultura de carácter preventivo, donde cada usuario entienda los riesgos y las afectaciones que se puede presentar permitiendo tomar medidas que disminuyan la materialización de estos.

Para el tratamiento de riesgos se debe contar con un plan de gestión de riesgos para garantizar la continuidad del negocio, planeando acciones que disminuyan la afectación de los procesos, por este motivo, se ha visto la necesidad de desarrollar la identificación, análisis, tratamiento, evolución y monitoreo de riesgo de seguridad de la información.

Teniendo en cuenta Política de Gobierno Digital como una de las dimensiones del Modelo Integrado de Planeación y Gestión – MIPG, la implementación del Modelo de Seguridad y Privacidad de la Información – MSPI, y la guía para la administración del riesgo del Departamento Administrativo de la Función Pública, se define el plan de tratamiento de riesgos relacionados con la información institucional con enfoque en la seguridad informática frente a ciberamenazas sobre activos de tecnologías de información y de las comunicaciones con el fin de garantizar la seguridad en términos de integridad, confiabilidad y disponibilidad.

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

2. OBJETIVO

Definir las acciones necesarias para el adecuado tratamiento de los riesgos a los que están expuestos los activos de información, definiendo los lineamientos y metodología a seguir para el análisis, valoración y tratamiento de riesgos de Seguridad, alineados con las políticas de seguridad y privacidad de la información, que permitan una adecuada toma de decisiones para disminuir la probabilidad que se materialice una amenaza, así como permitir la recuperación del sistema.

2.1. OBJETIVOS ESPECIFICOS

- Gestionar los eventos de seguridad de la información para detectar y tratar con eficiencia, acorde a las necesidades de la entidad.
- Proteger los activos de información de acuerdo a su clasificación y criterios de Confidencialidad, Integridad y Disponibilidad.
- Dar a conocer la importancia y la necesidad de una correcta gestión del riesgo de seguridad de la información.
- Definir los principales elementos a proteger en la entidad.
- Identificar las principales amenazas en la entidad.
- Proponer soluciones para minimizar los riesgos a los que está expuesto cada activo.
- Fortalecer y apropiar conocimiento referente a la gestión de riesgos Seguridad y Privacidad de la información, Seguridad Digital y Continuidad de la Operación.

3. ALCANCE

El plan de tratamiento de riesgos proporcionara una metodología que será aplicada para realizar una eficiente gestión de riesgos de Seguridad y Privacidad de la Información, en todos los activos de información frente a ciberamenazas teniendo en cuenta las capacidades y recursos disponibles, permitiendo sostener los procesos de la entidad, y prevenir incidentes que puedan afectar el logro de los objetivos.

4. DOCUMENTOS RELACIONADOS

- Política General de Seguridad y Privacidad de la Información.
- Manual de Políticas de Seguridad y Privacidad de la Información.
- Norma ISO 31000:2009
- Inventario de activos de información

5. METODOLOGÍA DE GESTION DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

Se implementara una metodología de Gestión de Riesgos de Seguridad de la Información basada en la norma ISO 31000 y en la guía de Gestión del Riesgo Seguridad y Privacidad de la Información de MinTic, como se ilustra a continuación.

Proceso Gestión del Riesgo ISO 31000

6. METODOLOGIA

El Plan de Tratamiento de Riesgos contempla la definición de las actividades a desarrollar en aras de mitigar los riesgos sobre los activos, estas actividades se estructuraron de la siguiente manera, siguiendo las recomendaciones de la Guía de Gestión de Riesgos de Seguridad y Privacidad de la Información (MinTIC:2016)2

Gestión	Actividades	Tareas	Responsable de la Tarea	Fechas Programación Tareas	
				Fecha Inicio	Fecha Final

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

Gestión de Riesgos	Levantamiento de activos de información	Actualizar activos de información	Líder gestión tecnológica	01/03/2023	30/05/2023
	Sensibilización	Consientizar la importancia de las buenas practicas de seguridad y Herramientas de Gestión de Riesgos	Líder gestión tecnológica	01/03/2023	15/12/2023
	Identificación de Riesgos de Seguridad y Privacidad de la Información	Identificación, Análisis y Evaluación de Riesgos	Líder gestión tecnológica	02/05/2023	30/06/2023
	Adquisición de Controles de Seguridad Informática frente a Ciberamenazas	Adquirir controles de seguridad frente a amenazas informaticas	Líder gestión tecnológica	01/03/2023	15/06/2023
	Monitoreo y Revisión	Generación, presentación y reporte de indicadores	Líder gestión tecnológica	01/06/2023	31/12/2023

Identificación de riesgos

En esta etapa los encargados de Riesgos buscaran identificar los principales riesgos críticos a los que está expuesta la entidad, en los activos de información y que pudieran afectar el cumplimiento de los

objetivos y/o estrategias definidas, la identificación puede ser a través de reuniones, encuestas, bases de datos o matrices de riesgo de ejercicios previos.

Una vez Identificados los riesgos críticos, estos se deben documentar en una matriz de riesgos, clasificándolos por tipo de riesgo estratégico, Imagen, financieros, operacional, tecnológicos y cumplimiento.

Valoración de los riesgos

La valoración de los riesgos de Seguridad y Privacidad de la Información, se realizará acorde a la metodología para la administración de riesgos mencionada en la Guía para la administración del riesgo y el diseño de controles en entidades públicas emitida por el Departamento Administrativo de la Función Pública.

Mapas de riesgos y planes de tratamiento

De acuerdo con los riesgos identificados y la valoración de los riesgos inherentes, así como de los riesgos residuales se presenta el mapa de riesgos producto de la aplicación de los controles identificados a los riesgos inherentes, así como de los controles sobre los riesgos residuales identificados, en el que se identifican el conjunto de riesgos frente a la probabilidad de ocurrencia y el impacto de la materialización.

7. RECURSOS

Para gestión de riesgos de Seguridad y Privacidad de la Información, el Fondo de Desarrollo de Proyectos de Cundinamarca cuenta con:

RECURSOS	VARIABLE
Humanos	Personal capacitado e idóneo para la gestión del riesgo de seguridad digital. El area de tecnologias TIC, es responsable de las políticas, estrategias y procedimientos en la Entidad en lo concerniente a la seguridad y privacidad de la información lo cual contribuye a la mejora continua.

Técnicos	Guía para la administración del riesgo del Departamento Administrativo de la Función Pública (DAFP). Guia de gestion del riesgo - Seguridad y Privaciad de la Información - MinTic Herramienta para la gestión de riesgos (Matriz de Riesgos SGSI)
Logísticos	Aspectos de mejora continua, monitoreo y auditorías. Gestión de recursos para realizar socializaciones, transferencia de conocimientos y seguimiento a la gestión de riesgos.
Financieros	Recursos para la adquirir con oportunidad y calidad técnica los bienes y servicios requeridos; recursos humanos, técnicos.

8. DEFINICIONES

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.

Aceptación de riesgo: Decisión de asumir un riesgo

Amenaza: es un ente o escenario interno o externo que puede hacer uso de una vulnerabilidad para generar un perjuicio o impacto negativo en la institución (materializar el riesgo).

Confidencialidad: propiedad de la información que la hace no disponible, es decir, divulgada a individuos, entidades o procesos no autorizados

Control: acciones o mecanismos definidos para prevenir o reducir el impacto de los eventos que ponen en riesgo, la adecuada ejecución de las actividades y tareas requeridas para el logro de objetivos de los procesos de una entidad

Dueño del riesgo sobre el activo: Persona o entidad con la responsabilidad de rendir cuentas y la autoridad para gestionar un riesgo.

Evaluación del riesgo: Proceso de comparar el riesgo estimado contra criterios de riesgo dados, para determinar la importancia del riesgo.

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

Gestión del riesgo: proceso efectuado por la alta dirección de la entidad y por todo el personal para proporcionar a la administración un aseguramiento razonable con respecto al logro de los objetivos.

Probabilidad: es la posibilidad de la amenaza aproveche la vulnerabilidad para materializar el riesgo.

Impacto: son las consecuencias que genera un riesgo una vez se materialice.

Riesgo: es un escenario bajo el cual una amenaza puede explotar una vulnerabilidad generando un impacto negativo al negocio evitando cumplir con sus objetivos.

Vulnerabilidad: es una falencia o debilidad que puede estar presente en la tecnología, las personas o en las políticas y procedimientos.

Elaboró y consolidó: Nelson Reina- Profesional con funciones de Gestión tecnológica y de la información