PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD

FONDECUN
FONDO DE DESARROLLO DE
PROYECTOS DE CUNDINAMARCA

Contáctenos
Av-cra 10 # 28-49 Torre A, Piso 21
(57) 1 - 2432328- 2432806
@fondecunoficial
www.fondecun.gov.co

TABLA DE CONTENIDO

Contáctenos
Av-cra 10 # 28-49 Torre A, Piso 21
(57) 1 - 2432328- 2432806
@fondecunoficial
www.fondecun.gov.co

1. INTRODUCCIÓN

La gestión de los riesgos de seguridad de la información es un proceso esencial que ayuda a reducir pérdidas y proteger la información en todas sus etapas. Este proceso no solo busca la protección activa frente a amenazas, sino también permite identificar las debilidades existentes, abordarlas y minimizar los impactos negativos a lo largo del ciclo de vida del servicio.

En este contexto, el plan de tratamiento de riesgos de seguridad y privacidad de la información debe tener un enfoque estratégico, orientado al desarrollo de una cultura preventiva dentro de la organización. Cada usuario debe comprender los riesgos asociados con la seguridad de la información, las posibles afectaciones y la importancia de tomar medidas preventivas que disminuyan la probabilidad de que estos riesgos se materialicen. Esto es clave para la creación de una mentalidad colectiva donde la seguridad no sea solo responsabilidad del área técnica, sino también de todos los integrantes de la entidad.

El tratamiento de riesgos debe estar respaldado por un plan de gestión de riesgos, el cual tiene como objetivo asegurar la continuidad del negocio. Este plan debe prever acciones específicas para reducir el impacto de los riesgos en los procesos esenciales de la organización, considerando no solo los riesgos de seguridad, sino también aquellos que puedan afectar la privacidad de la información.

Teniendo en cuenta la 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 ciber amenazas sobre activos de tecnologías de información y de las comunicaciones con el fin de garantizar la seguridad en términos de integridad, confiabilidad y disponibilidad.

2. 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. Estos activos se pueden clasificar así:

- ✓ Electrónicos: Bases de datos, archivos, registros de auditoría, información de archivo, aplicaciones, herramientas de desarrollo y utilidades.
- ✓ Físicos: Documentos impresos, manuscritos y hardware.
- ✓ Servicios: Servicios computacionales y de comunicaciones.
- ✓ Personas: Incluyendo sus calificaciones, competencias y experiencia.
- ✓ Intangibles: Ideas, conocimiento, conversaciones.

Contáctenos
Av-cra 10 # 28-49 Torre A, Piso 21
(57) 1 - 2432328- 2432806
@fondecunoficial
www.fondecun.gov.co

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.

Evento: Cualquier suceso identificable que requiere ser registrado y gestionado dentro del sistema de gestión de seguridad de la información de una organización. Los eventos pueden incluir incidentes de seguridad, problemas técnicos, cambios significativos, actividades planificadas, entre otros acontecimientos relevantes relacionados con la seguridad de la información.

Gestión del riesgo: Proceso sistemático e integral para identificar, evaluar y tratar los riesgos de seguridad de la información que enfrenta una organización.

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.

Riesgo aceptable: Riesgo en que la organización decide que puede convivir y/o soportar dado a sus obligaciones legales, contractuales y/o intereses propios.

Riesgo residual: El nivel de riesgo que permanece después de que se han aplicado medidas de tratamiento para mitigar o reducir los riesgos de seguridad de la información en una organización

Contáctenos
Av-cra 10 # 28-49 Torre A, Piso 21
(57) 1 - 2432328- 2432806
@fondecunoficial
www.fondecun.gov.co

3. OBJETIVOS

3.1. General

Definir y ejecutar la metodología para el tratamiento de riesgos de seguridad orientados a la preservación de la integridad, disponibilidad y confidencialidad de los activos de información institucionales, a la mitigación de la probabilidad de materialización de los mismos frente a amenazas, y al aseguramiento de la continuidad del negocio.

3.2. Objetivos Específicos

- ✓ Identificar las principales amenazas y riesgos de seguridad en la Entidad.
- ✓ Definir los principales activos de información susceptibles y críticos para garantizar la continuidad del negocio.
- ✓ Definir la metodología de análisis, evaluación, clasificación y tratamiento de riesgos de seguridad.
- ✓ 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 con 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.
- ✓ 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 las Operaciones.

4. ALCANCE

La gestión de riesgos de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación es fundamental para asegurar que los procesos de la Entidad se desarrollen sin interrupciones y con los niveles adecuados de protección, estableciendo una metodología eficiente y estructurada que permita identificar, analizar, valorar y manejar los riesgos asociados a estos ámbitos, asegurando así que la Entidad pueda continuar operando de manera eficiente, incluso en presencia de incidentes o amenazas, y cumpliendo con los objetivos establecidos.

5. DOCUMENTOS RELACIONADOS

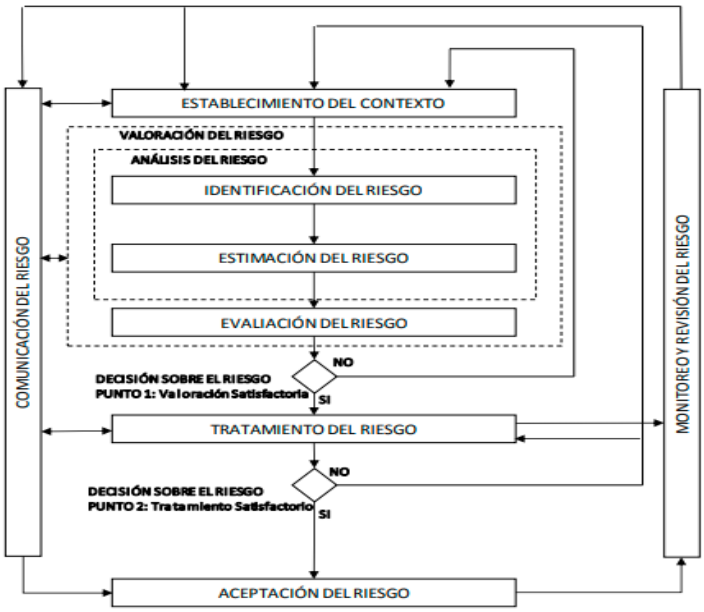
- ✓ Política General de Seguridad y Privacidad de la Información.
- ✓ Manual de Lineamientos de Seguridad Informática.
- ✓ Norma ISO 31000:2009
- ✓ Inventario de activos de información

Contáctenos
Av-cra 10 # 28-49 Torre A, Piso 21
(57) 1 - 2432328- 2432806
@fondecunoficial
www.fondecun.gov.co

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

Se implementará una metodología de Gestión de Riesgos de Seguridad de la Información basada en la norma ISO y en la guía de Gestión del Riesgo Seguridad y Privacidad de la Información del Ministerio de Tecnologías de la Información y las Comunicaciones MinTIC, como se ilustra a continuación:

Proceso Gestión del Riesgo ISO 31000



Proceso para la administración del riesgo en seguridad de la información NTC-ISO/IEC 27005

7. DESARROLLO DE LA METODOLOGÍA

La metodología de gestión de riesgos de la información le permitirá a la Entidad identificar y priorizar las acciones para la mitigación de la probabilidad de materialización de los mismos, y los mecanismos de restablecimiento con el fin de asegurar la integridad y disponibilidad de los

Contáctenos
Av-cra 10 # 28-49 Torre A, Piso 21
(57) 1 - 2432328- 2432806
@fondecunoficial
www.fondecun.gov.co
Gobernación de Cundinamarca

activos de información y la continuidad de las operaciones institucionales. Algunos aspectos relevantes que se desprenden de aplicar esta metodología son:

- ✓ Identificación de vulnerabilidades: Permite detectar las debilidades o vulnerabilidades presentes en los sistemas y procesos que podrían poner en peligro la seguridad de los activos de información.
- ✓ Evaluación del impacto: Ayuda a evaluar el impacto potencial que podría tener un evento o incidente adverso en los activos de información y en la organización en su conjunto.
- ✓ Priorización de acciones: Facilita la priorización de las acciones necesarias para proteger y mitigar los riesgos más significativos, asignando recursos de manera efectiva.
- ✓ Cumplimiento normativo: Ayuda a cumplir con los requisitos legales y regulaciones relacionadas con la protección de la información y la privacidad de los datos.

7.1. 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.

7.2. Valoración de los Riesgos

En este paso se genera una lista completa de los riesgos de cada uno de los procesos en cuanto a seguridad de la información, los riesgos a los cuales se encuentran expuestos y las causas que podrían comprometer la confidencialidad, integridad y disponibilidad de los objetivos de la Entidad, los cuales podrán ser identificados y evaluados teniendo en cuenta los criterios de evaluación definidos. En este proceso se debe realizar las siguientes actividades:

- ✓ Identificar el flujo de información de cada uno de los procesos
- ✓ Identificar las vulnerabilidades que existen en el proceso.
- ✓ Identificar las amenazas que podrían materializarse, dadas las vulnerabilidades existentes.
- ✓ Definir las escalas a utilizar

De acuerdo con los lineamientos para la gestión de riesgos digitales en Entidades públicas emitida por el DAFP, se podrán identificar los siguientes tres (3) riesgos inherentes de seguridad digital:

- ✓ Pérdida de la confidencialidad
- ✓ Pérdida de la integridad
- ✓ Pérdida de la disponibilidad

Contáctenos
Av-cra 10 # 28-49 Torre A, Piso 21
(57) 1 - 2432328- 2432806
@fondecunoficial
www.fondecun.gov.co

Para cada riesgo, se deben asociar el grupo de activos o activos específicos del proceso, y conjuntamente analizar las posibles amenazas y vulnerabilidades que podrían causar su materialización. A continuación, se mencionan un listado de amenazas y vulnerabilidades que podrían materializar los tres (3) riesgos previamente mencionados, a continuación, se describen una serie de amenazas comunes.

Deliberadas (D), fortuito (E) o ambientales (A).

Tipo	Amenaza	Origen
Daño físico	Fuego	A, D, E
	Agua	A, D, E
	Polvo, corrosión, congelamiento	A, D, E
Eventos naturales	Fenómenos climáticos	E
	Fenómenos sísmicos	E
	Fenómenos meteorológicos	E
	Inundaciones	E
Pérdidas de los servicios esenciales	Fallas en el sistema de suministro de agua o aire acondicionado	A, D, E
	Falla en equipo de telecomunicaciones	A, D, E
	Perdida de suministro de energía	A, D, E
Compromiso de la información	Interceptación de señales de interferencia comprometida	D
	Espionaje remoto	D
	Hurto de medios o documentos	D
	Recuperación de medios reciclados o desechados	D
	Datos provenientes de fuentes no confiables	D
	Manipulación con hardware	D
	Manipulación con software	D
	Divulgación	D
Fallas técnicas	Fallas del equipo	D, F
	Mal funcionamiento del equipo	D, F
	Saturación del sistema de	
	información	D, F
	Mal funcionamiento del software	D, F
	Incumplimiento en el mantenimiento del sistema de información	D, F
Acciones no autorizadas	Uso no autorizado del equipo	D, F
	Copia fraudulenta del software	D, F
	Uso de software falso o copiado	D, F
	Corrupción de los datos	D, F
Compromiso de las funciones	Error en el uso	D, F
	abuso de derechos	D
	Falsificación de derechos	D
Amenazas humanas	Pirata informático, intruso ilegal	D
	Criminal de la computación	D
	Terrorismo: Chantaje Destrucción Explotación Venganza, Ganancia política	D

Contáctenos
Av-cra 10 # 28-49 Torre A, Piso 21
(57) 1 - 2432328- 2432806
@fondecunoficial
www.fondecun.gov.co
Gobernación de Cundinamarca

Tipo	Amenaza	Origen
	Intrusos (Empleados con entrenamiento deficiente, descontentos, malintencionados, negligentes, deshonestos o despedidos)	D

7.3. Identificación de las Vulnerabilidades

Se deben identificar vulnerabilidades (debilidades) de acuerdo con los siguientes tipos:

Tipo	Vulnerabilidad
Hardware	Mantenimiento insuficiente
	Ausencia de esquemas de reemplazo periódico
	Susceptibilidad a la humedad, el polvo y la suciedad
	Susceptibilidad a las variaciones de temperatura (o al polvo y suciedad)
	Ausencia de un eficiente control de cambios en la configuración
	Susceptibilidad a las variaciones de voltaje
	Susceptibilidad a las variaciones de temperatura
	Almacenamiento sin protección
	Falta de cuidado en la disposición final
	Copia no controlada
Software	Ausencia o insuficiencia de pruebas de software
	Defectos bien conocidos en el software
	Ausencia de terminación de sesión cuando se abandona la estación de trabajo.
	Ausencia de registros de auditoría
	Asignación errada de los derechos de acceso
	Interfaz de usuario compleja
	Ausencia de documentación
	Configuración incorrecta de parámetros
	Fechas incorrectas
	Gestión deficiente de las contraseñas
	Ausencia de mecanismos de identificación y autenticación de usuarios
	Contraseñas sin protección
	Software nuevo o inmaduro
	Especificaciones incompletas o no claras para los desarrolladores
	Ausencia de control de cambios eficaz
	Descarga y uso no controlado de software
	Ausencia de copias de respaldo
Red	Ausencia de pruebas de envío o recepción de mensajes
	Líneas de comunicación sin protección
	Conexión deficiente de cableado
	Tráfico sensible sin protección
	Punto único de falla
	Arquitectura insegura de la red

Contáctenos
Av-cra 10 # 28-49 Torre A, Piso 21
(57) 1 - 2432328- 2432806
@fondecunoficial
www.fondecun.gov.co
Gobernación de Cundinamarca

Tipo	Vulnerabilidad
	Gestión inadecuada de la red
Personal	Ausencia del personal
	Entrenamiento insuficiente
	Falta de conciencia en seguridad
	Ausencia de políticas para el uso correcto de los medios de telecomunicaciones y mensajería
	Uso incorrecto de software y hardware
	Trabajo no supervisado de personal externo o de limpieza
Lugar	Uso inadecuado de los controles de acceso al edificio y los recintos
	Áreas susceptibles a inundación
	Red eléctrica inestable
	Ausencia de protección en puertas o ventanas
Organización	Ausencia de procedimiento formal para el registro y retiro de usuarios
	Ausencia de proceso para supervisión de derechos de acceso
	Ausencia de disposición en los contratos con clientes o terceras partes (con respecto a la seguridad)
	Ausencia de procedimientos de identificación y valoración de riesgos
	Ausencia de control de los activos que se encuentran fuera de las instalaciones
	Ausencia de acuerdos de nivel de servicio (ANS o SLA)
	Ausencia de acuerdos de nivel de servicio o insuficiencia de los mismos
	Ausencia de mecanismos de monitoreo para brechas en la seguridad
	Ausencia de procedimiento formal para la documentación del MSPI.
	Ausencia de procedimiento formal para la autorización de la información disponible al público
	Ausencia de planes de continuidad
	Ausencia de políticas sobre el uso de correo electrónico
	Ausencia de procedimientos para el manejo de información clasificada
	Ausencia de responsabilidad en seguridad de la información en la descripción de los cargos
	Ausencia de política formal sobre la utilización de computadores portátiles
	Ausencia de política sobre limpieza de escritorio y pantalla
	Ausencia de procedimientos para la presentación de informes sobre las debilidades en la seguridad

7.4. Análisis del Riesgo de Seguridad de la Información

En esta etapa se definen los criterios que se deben utilizar para evaluar la importancia del riesgo. Estos criterios de riesgo se estarán revisando de forma permanente, dado los cambios que pueden ocurrir en la organización.

Al definir los criterios de riesgo, se tendrán en cuenta:

✓ La naturaleza, los tipos de causas y consecuencias que pueden ocurrir y como se van a medir.

Contáctenos
Av-cra 10 # 28-49 Torre A, Piso 21
(57) 1 - 2432328- 2432806
@fondecunoficial
www.fondecun.gov.co
Gobernación de Cundinamarca

- ✓ La manera de definir la probabilidad de ocurrencia de un evento.
- ✓ La forma de determinar el nivel de riesgo.
- ✓ Niveles de riesgo aceptable para la organización.

De esta forma se procede a hacer la "calificación del riesgo", en la cual se realiza una estimación, de cuál podría ser la probabilidad de ocurrencia del riesgo y el impacto que traería éste, en caso de materializarse.

7.5. Evaluación del Riesgo

De acuerdo con la guía de gestión del riesgo, seguridad y privacidad de la información, se utilizará la "*Matriz de Calificación, Evaluación y Respuesta a los Riesgos*", obteniendo la forma de calificar los riesgos con los niveles de impacto y probabilidad.

"Matriz de Calificación, Evaluación y respuesta a los Riesgos"

PROBABILIDAD	IMPACTO				
	Insignificante (1)	Menor (2)	Moderado (3)	Mayor (4)	Catastrófico (5)
Raro (1)	B	B	M	A	A
Improbable (2)	B	B	M	A	E
Posible (3)	B	M	A	E	E
Probable (4)	M	A	A	E	E
Casi Seguro (5)	A	A	E	E	E

B: Zona de riesgo Baja: Asumir el riesgo
M: Zona de riesgo *Moderada*: Asumir el riesgo, Reducir el riesgo
A: Zona de riesgo *Alta*: Reducir el riesgo, Evitar, Compartir o Transferir
E: Zona de riesgo *Extrema*: Reducir el riesgo, Evitar, Compartir o Transferir

Fuente: Guía de Riesgos DAFP

La descripción de probabilidad de materialización de un riesgo se detalla en la siguiente tabla:

NIVEL	PROBABILIDAD		DESCRIPCIÓN
100%	Muy Alta (Casi seguro)	La actividad se realiza más de 5000 veces al año.	Cuando el evento de riesgo se produce en la totalidad de las ocasiones en que se desarrolla una actividad especifica.
80%	Alta (Probable)	La actividad se realiza entre 500 a 5000 veces al año.	Cuando el evento de riesgo se produce en la mayoría de las ocasiones en que se desarrolla una actividad específica
50%	Media (posible)	La actividad se realiza entre 25 a 500 veces al año.	El evento de riesgo se produce aproximadamente la mitad de las

Contáctenos
Av-cra 10 # 28-49 Torre A, Piso 21
(57) 1 - 2432328- 2432806
@fondecunoficial
www.fondecun.gov.co
Gobernación de Cundinamarca

			veces en que se desarrolla una actividad específica.
20%	Muy Baja (Raro)	La actividad se realiza entre 1 a 4 veces al año.	Cuando el evento de riesgo se produce en un número muy limitado y mínimo de ocasiones en que se desarrolla una actividad especifica. (poco comunes o anormales).

7.6. Evaluación de los Controles Establecidos para la Mitigación de los Riesgos

En la evaluación de los controles se tendrá en cuenta los criterios de cada uno de los riesgos identificados, iniciando por la evaluación los controles ya establecidos de la Entidad determinado la efectividad frente al riesgo, de ser necesario se reevaluará y se determinará nuevo control, en este punto se utilizará la tabla de "estructura de nuevos controles" que presenta la guía de controles de MSPI:

Política general			
Núm.	Nombre	Seleccionado / Excepción	Descripción / Justificación

Fuente: Guía – Controles del MSPI

Igualmente, se utilizarán las "Tablas para valoración de controles" que entrega la guía para la cuantificación de los controles:

PÁRAMETROS	CRITERIOS	TIPO DE CONTROL		PUNTAJES
		Probabilidad	Impacto	
Herramientas para ejercer el control	Posee una herramienta para ejercer el control.			15
	Existen manuales instructivos o procedimientos para el manejo de la herramienta			15
	En el tiempo que lleva la herramienta ha demostrado ser efectiva.			30
Seguimiento al control	Están definidos los responsables de la ejecución del control y del seguimiento.			15
	La frecuencia de la ejecución del control y seguimiento es adecuada.			25
	TOTAL			100

Fuente: Tablas para valoración de controles - DAFP

A continuación, se describen algunos componentes para apoyar la evaluación y seguimiento a los controles, y la mitigación de riesgos de seguridad:

- ✓ Planes de contingencia: Establecer planes de acción específicos para hacer frente a situaciones de emergencia y minimizar los impactos negativos en caso de ocurrir un incidente de seguridad.

Contáctenos
Av-cra 10 # 28-49 Torre A, Piso 21
(57) 1 - 2432328- 2432806
@fondecunoficial
www.fondecun.gov.co
Gobernación de Cundinamarca

- ✓ Planes de recuperación ante desastres: Implementar estrategias y procedimientos para restaurar los sistemas y operaciones de manera rápida y efectiva en caso de un desastre o interrupción grave
- ✓ Antivirus: Implementar soluciones antivirus actualizadas para detectar y eliminar malware y otras amenazas informáticas.
- ✓ Firewalls, VPN, cifrado de la información: Utilizar firewalls y redes privadas virtuales (VPN) para proteger el tráfico de datos, así como aplicar cifrado a la información sensible para garantizar su confidencialidad.
- ✓ Procedimientos: Establecer procedimientos operativos estandarizados para guiar a los usuarios institucionales en la ejecución de actividades seguras y consistentes.
- ✓ Estándares de configuración: Definir y aplicar estándares de configuración para los sistemas y dispositivos, reduciendo así posibles puntos débiles en la seguridad.

7.7. Planes de Acción y Responsables

Los planes de acción de riesgos de seguridad hacen referencia a actividades necesarias para mitigar y tratar los riegos identificados sobre los activos de información institucionales. Estos planes deben considerar los riegos residuales significativos y sus controles correspondientes. Una vez ejecutado el plan de acción se deben llevar a cabo revisiones periódicas para asegurar su efectividad teniendo en cuenta el siguiente flujo:

- ✓ Identificar y ordenar riesgos residuales.
- ✓ Establecer prioridades.
- ✓ Analizar el costo y el beneficio asociado.
- ✓ Establecer controles a implementar.
- ✓ Definir y ejecutar procedimiento de implementación.
- ✓ Evaluar y ajustar los controles.

Los responsables para la ejecución de los planes de acción deberán ser quienes administren, soporten y operen los activos de información críticos. Es así que, los riesgos identificados para un sistema en particular podrán vincularse a más de un responsable dependiendo de la complejidad y los diferentes recursos físicos y lógicos que componen o soportan tal sistema. La consideración de las diversas variables que inciden sobre los activos de información permite establecer una estrategia adecuada para mitigar los riesgos prioritarios, maximizando la eficacia de los recursos y garantizando una gestión integral de la seguridad de la Información, permitiendo la toman decisiones informadas y la respuesta efectiva ante los desafíos de seguridad identificados en el proceso de evaluación de riesgos.

8. PLAN DE IMPLEMENTACIÓN

Contáctenos
Av-cra 10 # 28-49 Torre A, Piso 21
(57) 1 - 2432328- 2432806
@fondecunoficial
www.fondecun.gov.co
Gobernación de Cundinamarca

Gestión	Actividades	Tareas	Responsable de la Tarea	Fechas Programación Tareas	
				Fecha Inicio	Fecha Final
Gestión de Riesgos	Actualizar activos de información y realizar valoración de activos	Actualizar activos de información	Líder gestión tecnológica	01/03/2025	30/11/2025
	Sensibilización	Socialización de lineamientos y la importancia de las buenas prácticas de seguridad y Herramientas de Gestión de Riesgos(dos sesiones en la vigencia 2025)		• Sesión 1: Marzo 2025 Sesión 2: Septiembre 2025	
	Evaluación de riesgos de Seguridad y Privacidad de la Información identificados	Identificación, Análisis y Evaluación de Riesgos		01/03/2025	30/12/2025
	Adquisición e implementación de Controles de Seguridad Informática frente a Ciber amenazas	Adquirir controles de seguridad frente a amenazas informáticas, Software de seguridad antivirus, actualización del firewall. Actualizar las medidas de seguridad informática y políticas de seguridad.		01/03/2025	30/12/2025
	Monitoreo y Revisión	Generación, presentación y reporte de indicadores mediante informe final consolidado.		01/08/2025	31/12/2025

9. 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 área de tecnologías 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). Guía de gestión del riesgo - Seguridad y Privacidad de la Información - Min Tic 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.

Contáctenos
Av-cra 10 # 28-49 Torre A, Piso 21
(57) 1 - 2432328- 2432806
@fondecunoficial
www.fondecun.gov.co

CONTROL DE CAMBIOS		
VERSIÓN	**FECHA**	**DESCRIPCIÓN DE LA MODIFICACION**
01	Enero 2022	Generación inicial del documento
02	Enero 2023	Actualización actividades a realizar plan de implementación.
03	Enero 2024	Actualización de metodología y plan de implementación.
04	Enero 2025	Actualización del documento por cambio de vigencia.

Contáctenos
Av-cra 10 # 28-49 Torre A, Piso 21
(57) 1 - 2432328- 2432806
@fondecunoficial
www.fondecun.gov.co