



InfiValle

Instituto Financiero para el Desarrollo del Valle del Cauca

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

31 de enero de 2025

PRESENTACIÓN

INFIVALLE en concordancia con el cumplimiento de sus objetivos estratégicos de seguridad de la información y consiente de la obligación que tiene para asegurar la confidencialidad, integridad y disponibilidad de la misma, ha establecido como marco de gobierno la implementación del MSPI y los lineamientos de gestión relacionados en la ISO 27001.

Para INFIVALLE es importante que estas herramientas actúen integralmente y den respuesta al tratamiento de riesgos de seguridad de la información con el cierre efectivo de las brechas identificadas y minimizando el impacto a causa de la materialización de alguno de ellos.

Original Firmado
GIOVANNI RAMÍREZ CABRERA
Gerente



Contenido

PRESENTACIÓN 2

2. DEFINICIONES..... 4

3. OBJETIVOS 5

3.1. Objetivo general..... 5

3.2. Objetivos específicos..... 5

4. ALCANCE 6

5. MARCO DE REFERENCIA 7

**6. CRONOGRAMA DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DE LA
INFORMACIÓN Y PRIVACIDAD DE LA INFORMACIÓN..... 8**



2. DEFINICIONES

- **Riesgo:** es un escenario bajo el cual una amenaza puede explotar una vulnerabilidad generando un impacto negativo al negocio evitando cumplir con sus objetivos.
- **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).
- **Vulnerabilidad:** es una falencia o debilidad que puede estar presente en la tecnología, las personas o en las políticas y procedimientos.
- **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.
- **Control o Medida:** 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.

3. OBJETIVOS

3.1. Objetivo general

Establecer un marco de operación para la gestión integral de los riesgos de seguridad de la información desde su identificación hasta el diseño de un plan adecuado para su tratamiento, que le permita asegurar el cumplimiento de sus objetivos estratégicos y la conservación de la confidencialidad, integridad y disponibilidad de la información.

3.2. Objetivos específicos

- Reducir el impacto que pudiese ocasionar la materialización de los riesgos de seguridad de la información a través de la aplicación de controles para su tratamiento.
- Generar en el instituto un marco de gobierno que permita el fortalecimiento y apropiación del conocimiento bajo una cultura organizacional con pensamiento basado en riesgos de seguridad de la información.
- Responder a las necesidades y expectativas de las partes interesadas externas e internas, requisitos legales y reglamentarios aplicables.

4. ALCANCE

La gestión de riesgos de seguridad de la información para INFIVALLE enmarca todos los procesos estratégicos, misionales, de apoyo y soporte, de evaluación y seguimiento con base en la actual cadena de valor, incluyendo funcionarios, contratistas, sistemas de información y terceros que manejen información institucional.

Así mismo, el tratamiento del riesgo tendrá en cuenta los riesgos que se encuentren en los niveles Alto y Extremos acorde a los lineamientos establecidos en las políticas para el tratamiento de Riesgos de Seguridad de la Información.

5. MARCO DE REFERENCIA

INFIVALLE establece la metodología para el tratamiento de los riesgos de seguridad de la información y ciberseguridad que comprende todo el ciclo de gestión desde su redacción, implementación, hasta el seguimiento y mejora continua de los controles diseñados a partir de los activos de información inventariados.

Las medidas de tratamiento del riesgo consideradas en el manual se determinan de acuerdo al apetito de riesgo definido por el instituto, estas son:

- **Aceptar:** Determinación de asumir el riesgo conociendo los efectos de su posible materialización.
- **Mitigar:** Implementación de acciones que mitigan el nivel de riesgo. No necesariamente un control adicional.
- **Transferir:** Estrategias de tercerización de procesos o traslado de riesgo a través de seguros o pólizas. La responsabilidad económica recae sobre el tercero, pero no se transfiere la responsabilidad sobre el tema reputacional.
- **Evitar:** Determinación de no asumir la actividad que genera el riesgo.



6. CRONOGRAMA DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN Y
PRIVACIDAD DE LA INFORMACIÓN

ACTIVIDAD	TAREA	RESPONSABLE	FECHA INICIO	FECHA FINALIZACIÓN
Sensibilización	Socialización de las políticas y manuales para la gestión de riesgos de seguridad de la información, sus controles y capacitación a todas las partes interesadas	Gestión del riesgo	01/02/2025	30/04/2025
Valoración del riesgo	Revisión de los riesgos y controles de seguridad de la información	Todos los procesos	01/05/2025	31/08/2025
Tratamiento del riesgo	formulación de planes para el tratamiento y mitigación de los riesgos según la metodología			
Seguimiento y monitoreo	monitoreo de planes diseñados para el tratamiento de los riesgos y verificación de la eficacia de los controles			
Monitoreo riesgos residuales	Evaluación del estado de los riesgos residuales	Gestión del Riesgo	Permanente	
Monitoreo y revisión	Monitoreo eficacia controles	Gestión del Riesgo	Permanente	
	Monitoreo planes de acción	Planeación y calidad		
	Seguimiento al cumplimiento del Sistema la gestión de riesgos de seguridad de la información	Control interno		

