InfiValle

Instituto Financiero para el Desarrollo del Valle del Cauca

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

CONTENIDO

PRESENTACIÓN

El Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información es un documento que hace parte integral de la implementación y operación del Modelo de Seguridad y Privacidad de la Información (MSPI) del Instituto, de conformidad con los lineamientos establecidos por el Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC para las entidades públicas del orden nacional y territorial.

Este plan se elabora con base en los resultados del proceso de identificación, análisis y evaluación de riesgos de seguridad de la información y continuidad del negocio, y tiene como propósito definir las acciones de tratamiento orientadas a reducir los riesgos a niveles aceptables, de acuerdo con el apetito de riesgo institucional y los criterios de aceptación definidos por la Alta Dirección, es decir “Bajo” y “Moderado”.

Adicionalmente en este documento se contempla la aplicación de las alternativas de gestión del riesgo establecidas en el MSPI —mitigar, aceptar, transferir o evitar— mediante la implementación de controles administrativos, organizacionales, tecnológicos y físicos, alineados con ISO 27001:2022 Seguridad de la Información y ISO 22301:2019 Continuidad del Negocio, garantizando la protección de los activos de información y el adecuado tratamiento de los datos personales.

Así mismo, este documento contribuye al cumplimiento de la normativa vigente en materia de protección de datos personales, en especial la Ley 1581 de 2012, sus decretos reglamentarios y las disposiciones emitidas por la Superintendencia de Industria y Comercio, y se constituye en un insumo fundamental para el seguimiento, monitoreo y mejora continua del MSPI, así como para los procesos de auditoría interna, control interno y reporte de avance institucional.

GIOVANNI RAMÍREZ CABRERA
Gerente

1. 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.

• 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 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 o Medida: Medida que permite reducir o mitigar un riesgo.

• Disponibilidad: Propiedad de ser accesible y utilizable a demanda por una entidad.}

• Impacto: consecuencias que puede ocasionar a la organización la materialización del riesgo.

• Integridad: Propiedad de exactitud y completitud.

• Probabilidad: se entiende la posibilidad de ocurrencia del riesgo. Estará asociada a la exposición al riesgo del proceso o actividad que se esté analizando.

• Riesgo: Efecto que se causa sobre los objetivos de las entidades, debido a eventos potenciales.

• 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.

• Vulnerabilidad Representa la debilidad de un activo o de un control que puede ser explotada por una o más amenazas.

2. OBJETIVOS

- Cumplir con los requisitos legales, reglamentarios, regulatorios y de las normas técnicas colombianas en materia de seguridad de la información, continuidad del negocio, privacidad de la información, seguridad digital y protección de la información personal.

- Gestionar los riesgos de Seguridad de la Información y Continuidad del Negocio.

- 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.

- Fortalecer y apropiar conocimiento referente a la gestión de riesgos de Seguridad de la Información y Continuidad del Negocio.

3. ALCANCE

La gestión de riesgos de seguridad de la información y continuidad del negocio para INFIVALLE aplica a todo el modelo de operación por procesos (estratégicos, misionales, de apoyo y soporte, de evaluación y seguimiento y de comunicación) 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.

4. MARCO DE REFERENCIA

INFIVALLE estableció la “Metodología para el análisis de riesgos de seguridad de la información y continuidad del negocio” para el tratamiento de dichos los riesgos 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 esta Metodología 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.

5. CRONOGRAMA

ACTIVIDAD	ACTIVIDAD	RESPONSABLE	FECHA INICIO	FECHA FINALIZACIÓN
Sensibilización	Socialización de las políticas y manuales para la gestión de riesgos de seguridad de la información y continuidad, sus controles y capacitación a todas las partes interesadas	Gestión del riesgo	1/04/2026	31/08/2026
Valoración del riesgo	Revisión de los riesgos y controles de seguridad de la información y continuidad del negocio.	Todos los procesos	1/04/2026	31/08/2026
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 y continuidad del negocio.	Control interno		