InfiValle

Instituto Financiero para el Desarrollo del Valle del Cauca

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

CONTENIDO

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.

La seguridad y privacidad de la información constituyen un componente transversal de la gestión integral de riesgos del Instituto, en tanto impactan de manera directa la operación, la continuidad del negocio, el cumplimiento regulatorio, la protección del consumidor financiero y la reputación institucional.

El presente Plan de Seguridad y Privacidad de la Información establece el marco estratégico, normativo y operativo para la protección de la información. Este plan busca garantizar la confidencialidad, integridad, disponibilidad y privacidad de la información, asegurando el cumplimiento normativo, la continuidad del negocio y la confianza de clientes, reguladores y demás partes interesadas.

El presente plan se encuentra alineado con los requerimientos de las normas ISO/IEC 27001:2022 para la gestión de la seguridad de la información y ISO 22301: 2019 para la continuidad del negocio y la resiliencia organizacional, integrándose de manera consistente con el sistema de gestión de calidad ISO 9001:2015 y con los modelos de control interno y administración de riesgos adoptados por el Instituto.

GIOVANNI RAMÍREZ CABRERA
Gerente

1. DEFINICIONES

MSPI: El Modelo de Seguridad y Privacidad de la Información - MSPI, imparte lineamientos a las entidades públicas en materia de implementación y adopción de buenas prácticas, tomando como referencia estándares internacionales, con el objetivo de orientar la gestión e implementación adecuada del ciclo de vida de la seguridad de la información (Planeación, Implementación, Evaluación, Mejora Continua), permitiendo habilitar la implementación de la Política de Gobierno Digital.

Acceso a la Información Pública: Derecho fundamental consistente en la facultad que tienen todas las personas de conocer sobre la existencia y acceso a la información pública en posesión o bajo control de sujetos obligados. (Ley 1712 de 2014, art 4).

Activo: En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de ésta (sistemas, soportes, edificios, personas, etc.) que tenga valor para la organización. (ISO/IEC 27000).

Activos de Información y recursos: se refiere a elementos de hardware y de software de procesamiento, almacenamiento y comunicaciones, bases de datos y procesos, procedimientos y recursos humanos asociados con el manejo de los datos y la información misional, operativa y administrativa de cada entidad, órgano u organismo.

Archivo: Conjunto de documentos, sea cual fuere su fecha, forma y soporte material, acumulados en un proceso natural por una persona o Entidad pública o privada, en el transcurso de su gestión, conservados respetando aquel orden para servir como testimonio e información a la persona o institución que los produce y a los ciudadanos, o como fuentes de la historia. También se puede entender como la institución que está al servicio de la gestión administrativa, la información, la investigación y la cultura. (Ley 594 de 2000, art 3).

Auditoría: Proceso sistemático, independiente y documentado para obtener evidencias de auditoría y obviamente para determinar el grado en el que se cumplen los criterios de auditoría. (ISO/IEC 27000).

Autorización: Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales (Ley 1581 de 2012, art 3).

Bases de Datos Personales: Conjunto organizado de datos personales que sea objeto de Tratamiento (Ley 1581 de 2012, art 3)

Ciberseguridad: Protección de activos de información, mediante el tratamiento de las amenazas que ponen en riesgo la información que se procesa, almacena y transporta mediante los sistemas de información que se encuentran interconectados.

Ciberespacio: Es el ambiente tanto físico como virtual compuesto por computadores, sistemas computacionales, programas computacionales (software), redes de telecomunicaciones, datos e información que es utilizado para la interacción entre usuarios. (Resolución CRC 2258 de 2009).

Control: Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.

Seguridad de la información: Preservación de la confidencialidad, integridad, y disponibilidad de la información en cualquier medio: impreso o digital. (ISO/IEC 27000).

Seguridad digital: Preservación de la confidencialidad, integridad, y disponibilidad de la información que se encuentra en medios digitales.

3. OBJETIVO

Establecer las actividades contempladas en el Modelo de Seguridad y Privacidad de la Información – MSPI del Instituto, alineadas con la norma ISO/IEC 27001:2022, Sistema de Gestión de Seguridad de la Información (SGSI) y ISO 22301:2019, Continuidad del Negocio y Resiliencia Organizacional, la normativa vigente y los criterios de continuidad de la operación de los servicios, que permitan mantener la seguridad y privacidad de la información que gestionan los procesos del Instituto.

4. ALCANCE

La gestión de riesgos de seguridad de la información 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.

5. MARCO DE REFERENCIA

- Constitución Política de Colombia (Art. 15 – Habeas Data).
- Ley 1581 de 2012 – Protección de Datos Personales.
- Ley 594 de 2000, "por medio de la cual se dicta la Ley General de Archivos y se dictan otras disposiciones".
- Ley 1712 de 2014, "por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones".
- Decreto 1078 de 2015, “por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones”
- Circular Básica Jurídica (CBJ) – Superintendencia Financiera de Colombia.
- Circular Básica Contable y Financiera (CBCF).
- ISO 9001:2015 – Gestión de la Calidad.
- ISO/IEC 27001:2022 – Sistema de Gestión de Seguridad de la Información (SGSI).
- ISO 22301:2019 – Continuidad del Negocio y Resiliencia Organizacional.

6. CRONOGRAMA DE IMPLEMENTACIÓN

Actividad	Proceso Líder	Producto	Fecha de inicio	Fecha de finalización
Establecer y/o actualizar indicadores que permitan medir la eficiencia y eficacia de los controles y el nivel de implementación del MSPI	Gestión de Riesgos	Hoja de vida de indicadores de gestión de seguridad de la información	1/01/2026	28/02/2026
Actualización de la identificación, clasificación y valoración de los de Activos de Información.	Todos los procesos	Matriz de inventario activos de información actualizada en el módulo de riesgos	1/01/2026	15/07/2026
Actualización y consolidación de las políticas de Seguridad de la Información y Continuidad de Negocio	Gestión de Riesgos	Manual de Directrices y Políticas	1/01/2026	15/07/2026
Seguimiento a vulnerabilidades	Gestión de Riesgos	Informe de vulnerabilidad	1/01/2026	31/12/2026
Realizar seguimiento a los controles de las normas ISO 27001:2022 y 22301:2019.	Gestión de Riesgos	Informe de seguimiento de controles	1/02/2026	30/09/2026
Realizar seguimiento a los incidentes de seguridad de la información y continuidad del negocio y planes de acción.	Gestión de Riesgos	Informe de seguimiento Planes de Acción	1/02/2026	30/09/2026
Actualización de la Política de Protección de Datos Personales	Gestión de Riesgos	Política de Protección de Datos actualizada	4/05/2026	28/09/2026
Actualización e Identificación de los riesgos de seguridad de la información y continuidad del negocio para los activos de información identificados.	Todos los procesos	Mapas de riesgo de seguridad de la información y continuidad del negocio actualizados en el módulo de riesgos.	1/06/2026	15/07/2026

Actividad	Proceso Líder	Producto	Fecha de inicio	Fecha de finalización
Actualización de las estrategias de continuidad	Gestión de Riesgos	Propuesta estructurada y presentada	1/06/2026	15/07/2026
Actualización de reporte de bases de datos con las áreas	Gestión de Riesgos	Formatos de Recolección de Bases de Datos	15/06/2026	30/06/2026
Registro y actualización de las bases de datos en la plataforma RNBD	Gestión de Riesgos	Certificado del registro de BD que expide la SIC	15/06/2026	30/06/2026
Realizar una auditoría interna del Sistema de Seguridad de la Información y Continuidad del Negocio.	Gestión de Riesgos	Plan de Auditoria Informe de Auditoria	1/08/2026	28/08/2026
Definición y ejecución del plan de pruebas de las estrategias de Continuidad	Gestión de Riesgos	Plan y registro de pruebas de las estrategias de continuidad diseñadas	1/08/2026	15/09/2026
Realizar la publicación de la matriz de inventario de Activos de Información actualizada	Gestión de Riesgos	Publicación en la plataforma de datos Abiertos, sitio Web de Entidad y portal de datos abiertos	1/10/2026	30/10/2026