InfiValle

Instituto Financiero para el Desarrollo del Valle del Cauca

Plan de Seguridad y Privacidad de la Información

23 de abril de 2024

Contenido

1. INTRODUCCIÓN 3
2. DEFINICIONES 4
3. OBJETIVOS 6
3.1 Objetivo General 6
3.2 Objetivos Específicos 6
4. ALCANCE 7
5. MARCO DE REFERENCIA 8
6. CRONOGRAMA DE IMPLEMENTACIÓN DEL PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 9

1. INTRODUCCIÓN

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.

2. 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. 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.

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 su Manual para el Tratamiento de Riesgos de Seguridad de la Información.

5. MARCO DE REFERENCIA

5.1. **Ley 1712 de 2014:** Para la Implementación de la Estrategia de Gobierno en Línea, entidades del orden nacional; Modelo de Seguridad de la Información para la Estrategia de Gobierno en Línea.

5.2. **Ley estatutaria 1581 de 2012:** Por la cual se dictan disposiciones generales para la protección de datos personales.

5.3. **Norma técnica colombiana NTC - ISO/IEC 27001:** Estándar para la seguridad de la información.

6. CRONOGRAMA DE IMPLEMENTACIÓN DEL PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Actividad	Responsable	Producto	Fecha de inicio	Fecha de finalización
Etapa 1: Diagnóstico				
Aplicar el formato para la identificación de la línea base de seguridad en los procesos directivos (5), profesionales(11), asesores (3)	Gestión de Riesgos Apoyos Gestión de TIC Gestión Documental Comunicaciones	Identificación nivel de madurez del MSPI	01/07/2024	31/07/2024
Etapa 2: Planeación				
Establecer el plan de seguridad y privacidad de la información	Gerencia Gestión de Riesgos Gestión de TIC Planeación	Actualizar el alcance del Modelo de Seguridad y Privacidad de la Información - MSPI con base en las necesidades y expectativas de sus partes interesadas.	01/07/2024	31/07/2024
	Gerencia Gestión Riesgos Planeación Talento Humano	1. Actualización del Manual y Política de seguridad y privacidad de la información - MSPI. 2. Actualización de los Procesos y procedimientos de SI normalizados 3. Actualización Roles y Responsabilidades de SI 4. Actualización Integración del Modelo de Seguridad y Privacidad de la Información - MSPI con el proceso de Gestión Documental	01/08/2024	31/08/2024
	Gestión Riesgos Subgerencia Administrativa Comunicaciones	Plan de comunicaciones y capacitación	01/09/2024	30/09/2024
Etapa 3: Implementación				
Definición de los controles de seguridad: De acuerdo al plan para el tratamiento de los riesgos, seleccionar los controles mediante una declaración de aplicabilidad basados en el Anexo A ISO27001	Todos los procesos	Actualización de la declaración de aplicabilidad	01/07/2024	30/07/2024
Definición de indicadores de gestión Establecer indicadores que permitan medir la eficiencia de los controles y el nivel de implementación del MSPI	Gestión de Riesgos Gestión de TIC	Hoja de vida de indicadores de gestión de seguridad de la información	01/07/2024	30/07/2024
Política de Protección de Datos Personales Revisión de la normatividad vigente	Gestión de Riesgos	Actualización de la Política de Protección de Datos Personales	01/07/2024	31/08/2024

Actividad	Responsable	Producto	Fecha de inicio	Fecha de finalización
Política de Seguridad Digital	Gestión de Riesgos Gestión de TIC	Formular la política de seguridad digital para identificar los riesgos a los que están expuestos en el entorno digital y como protegerse, prevenir y reaccionar ante los delitos y ataques cibernéticos. Fomentar una cultura para crear consciencia de que el manejo del riesgo es nuestra responsabilidad Pregunta 176 FURAG 2022 - Cumplimiento de la Ley 1581 del 2021	01/09/2024	31/12/2024
Etapa 4: Evaluación del desempeño				
Plan de auditorías Establecer una serie de auditorías internas/externas que permitan hacer monitoreo y seguimiento al MSPI junto con las acciones de mejora definidas en búsqueda de la certificación	Gestión de Riesgo Planeación Control Interno	Plan de auditorias Auditoria de certificación Icontec ISO 27001	01/11/2024 01/12/2024	30/11/2024 31/12/2024
Etapa 5: Mejora continua				
Planes de mejora continua	Todos los procesos	Planes de mejora	Permanente	