TRD_120_72_26

INSTITUTO FINANCIERO DE CASANARE

# PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

SUBGERENCIA ADMINISTRATIVA Y FINANCIERA

| Elaborado por | Revisado por | Aprobado por |
|---|---|---|
| **CARLOS ANDRÉS RUBIO BEJARANO**<br>PROFESIONAL DE APOYO CTO 52 DE 2026 - SAF | **SONIA PATRICIA RÍOS JIMÉNEZ**<br>SUBGERENTE ADMINISTRATIVO Y FINANCIERO<br><br>**JOSÉ BLADIMIR NAVARRO CALDERON**<br>TÉCNICO OPERATIVO EN SISTEMAS | **OSCAR JAVIER ARAQUE**<br>GERENTE<br><br>**COMITÉ INSTITUCIONAL DE GESTIÓN Y DESEMPEÑO**<br>ACTA Nº 4 DE 30 DE ENERO DE 2026 |

## TABLA DE CONTENIDO

## 1. INTRODUCCIÓN

La información es uno de los activos más importantes del Instituto Financiero de Casanare (IFC) y un elemento fundamental para el desarrollo de sus funciones misionales, administrativas y financieras. Protegerla adecuadamente es indispensable para garantizar la continuidad operativa, fortalecer la confianza institucional, asegurar el cumplimiento normativo y salvaguardar los derechos de los ciudadanos y demás partes interesadas que interactúan con la entidad.

El presente Plan de Seguridad y Privacidad de la Información establece los lineamientos, directrices institucionales y la Política de Seguridad y Privacidad de la Información que orientan la protección de los activos de información del IFC. Su propósito es asegurar que la confidencialidad, integridad, disponibilidad, trazabilidad y privacidad de la información sean gestionadas de manera adecuada, conforme a los habilitadores de la Política de Gobierno Digital, al Modelo Integrado de Planeación y Gestión (MIPG), a la normativa vigente y a los estándares internacionales aplicables.

Este Plan articula los componentes estratégicos, administrativos, tecnológicos y operativos necesarios para reducir riesgos, fortalecer la gestión institucional y asegurar que los sistemas, procesos, servicios y datos administrados por el IFC se gestionen de manera segura, responsable y alineada con las mejores prácticas de seguridad digital y protección de datos personales.

La implementación del Plan es de carácter obligatorio para todos los funcionarios, trabajadores oficiales, contratistas, proveedores y terceros que tengan acceso a información o recursos tecnológicos del IFC. Su cumplimiento es esencial para consolidar una cultura institucional basada en la seguridad, la privacidad, la responsabilidad demostrada y la mejora continua.

## 2. OBJETIVO

Fortalecer la seguridad y privacidad de la información del Instituto Financiero de Casanare (IFC) mediante la implementación de lineamientos, políticas, controles y buenas prácticas que permitan proteger los activos de información, gestionar los riesgos institucionales y garantizar el cumplimiento de la normativa vigente en materia de seguridad digital y protección de datos personales.

### 2.1. Objetivos específicos

1. Establecer el marco institucional de políticas, roles, responsabilidades y directrices que orientan la gestión de la seguridad y privacidad de la información en el IFC.

2. Proteger la confidencialidad, integridad, disponibilidad, trazabilidad y privacidad de la información administrada por la entidad, mediante controles técnicos, físicos, administrativos y organizacionales.

3. Implementar un enfoque basado en riesgos, alineado con el Modelo Integrado de Planeación y Gestión (MIPG), el Modelo de Seguridad y Privacidad del MinTIC y las normas ISO/IEC 27001, 27002 y 27701.

4. Fortalecer la capacidad institucional para la prevención, detección, respuesta y recuperación frente a incidentes de seguridad digital que puedan afectar los servicios o activos de información del IFC.

5. Promover la cultura de seguridad digital y protección de datos personales, mediante actividades de capacitación, sensibilización y apropiación por parte de funcionarios, contratistas y terceros.

6. Orientar la adopción de medidas de continuidad y contingencia, asegurando que los servicios críticos del IFC se mantengan protegidos ante eventos que afecten su disponibilidad.

## 3. ALCANCE

El Plan de Seguridad y Privacidad de la Información del Instituto Financiero de Casanare (IFC) aplica a todos los procesos, servicios, activos de información, recursos tecnológicos y personas que intervienen en la administración, tratamiento, custodia o uso de la información institucional.

Este Plan cubre de manera integral los componentes administrativos, tecnológicos, físicos y operativos necesarios para garantizar la confidencialidad, integridad, disponibilidad, trazabilidad y privacidad de la información que el IFC produce, recibe, almacena, procesa o transmite.

### 3.1. Sujetos de Aplicación

El cumplimiento del Plan es obligatorio para:

- ✓ Servidores Públicos
- ✓ Contratistas
- ✓ Proveedores y terceros con acceso a sistemas o información institucional
- ✓ Usuarios que administren o procesen datos en nombre del IFC

### 3.2. Alcance Operativo y Tecnológico

El Plan aplica a:

- ✓ Infraestructura tecnológica (servidores, redes, equipos de cómputo, dispositivos móviles).
- ✓ Sistemas de información, bases de datos, aplicativos y servicios en la nube.
- ✓ Información financiera, crediticia, administrativa, operativa, documental y de datos personales.
- ✓ Procesos misionales, estratégicos, de apoyo y de evaluación que involucren tratamiento de información.

### 3.3. Componentes de Seguridad Cubiertos

El Plan integra lineamientos y controles relacionados con:

- ✓ Seguridad digital y ciberseguridad.
- ✓ Protección de datos personales.
- ✓ Gestión de riesgos y continuidad del servicio en materia de seguridad.
- ✓ Gestión de incidentes de seguridad de la información.
- ✓ Seguridad física y control de accesos.
- ✓ Gestión documental asociada a información sensible o crítica.

### 3.4. Articulación Institucional

Este Plan se articula con:

- ✓ El Modelo Integrado de Planeación y Gestión (MIPG).
- ✓ El Modelo de Seguridad y Privacidad del MinTIC.
- ✓ Las políticas institucionales de gestión documental y protección de datos.
- ✓ El Plan de Continuidad del Negocio y demás instrumentos asociados.

## 4. DEFINICIONES

Para efectos del presente Plan, se adoptan las siguientes definiciones:

Activo de Información: Recurso, dato, documento, sistema o servicio que tiene valor para el IFC y que requiere protección.

Amenaza: Evento o situación con potencial de afectar negativamente un activo de información.

Vulnerabilidad: Debilidad técnica, humana, física u organizacional que puede ser aprovechada por una amenaza.

Riesgo de Seguridad de la Información: Posibilidad de que una amenaza explote una vulnerabilidad, generando impacto en la confidencialidad, integridad, disponibilidad o privacidad de la información.

Confidencialidad: Propiedad que garantiza que la información solo sea accesible por personas o sistemas autorizados.

Integridad: Propiedad que asegura que la información se mantenga completa, exacta y no alterada sin autorización.

Disponibilidad: Condición que asegura que la información y los servicios estén accesibles cuando los usuarios autorizados lo requieran.

Trazabilidad: Capacidad de registrar y verificar las acciones realizadas sobre los sistemas o los datos institucionales.

Privacidad: Conjunto de principios, derechos y obligaciones que regulan el tratamiento adecuado de los datos personales.

Dato Personal: Cualquier información asociada o que pueda asociarse a una persona natural identificada o identificable.

Dato Personal Sensible: Información cuyo uso indebido pueda generar discriminación, como datos sobre salud, orientación sexual, origen étnico, ideología política o religiosa.

Tratamiento de Datos Personales: Cualquier operación sobre datos personales, como recolección, almacenamiento, uso, circulación o supresión.

Responsable del Tratamiento: Persona natural o jurídica que decide sobre el tratamiento de datos personales dentro del IFC.

Encargado del Tratamiento: Persona natural o jurídica que realiza el tratamiento de datos por cuenta del responsable.

Incidente de Seguridad de la Información: Evento que compromete o puede comprometer la confidencialidad, integridad, disponibilidad o privacidad de la información institucional.

Control de Seguridad: Medida técnica, administrativa, física u organizacional implementada para reducir riesgos.

SGSI – Sistema de Gestión de Seguridad de la Información: Conjunto de políticas y procesos que permiten gestionar la seguridad de la información. En el IFC, este concepto se aplica conforme a los lineamientos del MinTIC y del presente Plan.

## 5. MARCO NORMATIVO

El Plan de Seguridad y Privacidad de la Información del Instituto Financiero de Casanare (IFC) se fundamenta en el conjunto de leyes, decretos, lineamientos, estándares internacionales y políticas públicas que regulan la gestión de la información, la protección de datos personales, la seguridad digital, la transparencia y el uso adecuado de las tecnologías de la información en entidades públicas.

Este marco normativo establece las obligaciones, principios y buenas prácticas que orientan la implementación del presente Plan.

### 5.1. Normatividad Colombiana Vigente

*Ley 1581 de 2012 – Protección de Datos Personales*

Establece las disposiciones generales para el tratamiento de datos personales y define los principios de seguridad, confidencialidad y responsabilidad demostrada aplicables a entidades públicas y privadas.

*Decretos Reglamentarios 1377 de 2013 y 1755 de 2015*

Desarrollan la aplicación de la Ley 1581 en aspectos como autorización, finalidades, políticas internas de tratamiento, medidas de seguridad y gestión de derechos de los titulares.

*Ley 1712 de 2014 – Ley de Transparencia y Acceso a la Información Pública*

Regula la publicidad de la información pública y establece lineamientos de acceso, disponibilidad, divulgación, clasificación y reserva, los cuales deben ser garantizados mediante medidas de seguridad de la información.

*Ley 594 de 2000 – Ley General de Archivos*

Define las obligaciones en materia de conservación, organización, integridad y custodia de documentos y archivos, fundamentales para la gestión documental y la preservación de la información institucional.
*Decreto 1078 de 2015 – Decreto Único del Sector TIC*

Compila y reglamenta la Política de Seguridad y Privacidad de la Información, disponiendo que todas las entidades públicas deben implementarla formalmente bajo los lineamientos del MinTIC.

*Decreto 2573 de 2014 – Estrategia de Gobierno Digital*

Incluye la Seguridad y Privacidad de la Información como habilitador transversal y exige a las entidades la aplicación de controles y buenas prácticas para proteger activos de información y servicios digitales.

*Decreto 1413 de 2017 – Servicios Ciudadanos Digitales*

Define obligaciones de seguridad, responsabilidad demostrada, gestión de datos y adopción de esquemas de seguridad apropiados y verificables.

*Ley 1437 de 2011 – Código de Procedimiento Administrativo y de lo Contencioso Administrativo*

Regula el uso de medios electrónicos en trámites administrativos y exige medidas de seguridad para garantizar autenticidad, integridad y disponibilidad.

### 5.2. Lineamientos Nacionales y Políticas Públicas

*Política de Gobierno Digital (MinTIC)*

Establece los lineamientos en seguridad digital, gestión de incidentes, riesgos tecnológicos, cultura de seguridad y protección de datos personales.

*Modelo de Seguridad y Privacidad de la Información (MinTIC)*

Define principios, controles, roles y procesos que estructuran el Sistema de Gestión de Seguridad de la Información en entidades públicas.

*Guía de Gestión de Incidentes de Seguridad Digital – MinTIC*

Establece el modelo para identificación, clasificación, atención, tratamiento y cierre de incidentes.

*Lineamientos del Departamento Administrativo de la Función Pública (DAFP)*

Dentro del Modelo Integrado de Planeación y Gestión (MIPG), define:

- ✓ Gestión del riesgo
- ✓ Transparencia y acceso a la información
- ✓ Gestión documental
- ✓ Seguridad digital como habilitador transversal

*Lineamientos de la Secretaría de Transparencia*

Aplicables a la prevención de riesgos de corrupción, protección de la información pública, y controles administrativos.

### 5.3. Estándares y Mejores Prácticas Internacionales

*ISO/IEC 27001 – Sistema de Gestión de Seguridad de la Información*

Norma internacional para el establecimiento, implementación, mantenimiento y mejora continua del SGSI.

*ISO/IEC 27002 – Controles de Seguridad de la Información*

Guía de buenas prácticas que define controles técnicos y administrativos recomendados.

*ISO/IEC 27005 – Gestión del Riesgo de Seguridad de la Información*

Marco para la identificación, análisis, valoración, tratamiento y seguimiento del riesgo.

*ISO/IEC 27701 – Gestión de la Privacidad de la Información*

Extensión de la 27001 para sistemas de gestión de privacidad (SGPI), alineada con la legislación de protección de datos.

*ISO 22301 – Gestión de la Continuidad del Negocio*

Norma que establece lineamientos para garantizar la resiliencia operacional y la recuperación ante interrupciones.

### 5.4. Normas internas del IFC

El Plan se articula con:

- ✓ Manual de Funciones y Competencias Laborales.
- ✓ Sistema Integrado de Planeación y Gestión.
- ✓ Programa de Gestión Documental y Tablas de Retención Documental (TRD).
- ✓ Políticas institucionales del área TIC.
- ✓ Plan de Contingencia y Continuidad del Negocio.
- ✓ Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información.

### 5.5. Responsabilidad Institucional

El cumplimiento de este marco normativo es obligatorio para:

- ✓ Directivos
- ✓ servidores públicos,
- ✓ contratistas,
- ✓ proveedores y terceros que administren o procesen información institucional.

## 6. PRINCIPIOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

El Instituto Financiero de Casanare (IFC) adopta los principios y lineamientos establecidos por la Política de Seguridad y Privacidad de la Información del MinTIC, la Ley 1581 de 2012, el Decreto 1078 de 2015, el Modelo Integrado de Planeación y Gestión (MIPG) y la normativa aplicable a la protección de datos personales, la seguridad digital y la gestión de la información pública.

Estos principios orientan las decisiones, controles y acciones que hacen parte del presente Plan de Seguridad y Privacidad de la Información, y constituyen el marco conceptual para la protección de los activos de información administrados por el IFC. Los principios adoptados son:

Confidencialidad: La información debe ser protegida contra el acceso, uso, divulgación o consulta no autorizada.

Integridad: La información debe mantenerse exacta, completa y sin alteraciones no autorizadas durante su ciclo de vida.

Disponibilidad: La información, los sistemas y los servicios tecnológicos deben estar accesibles y operativos cuando los funcionarios, contratistas o terceros autorizados los requieran.

Trazabilidad: Toda acción realizada sobre los sistemas de información debe ser registrada, auditada y verificada cuando sea necesario.

Privacidad: El tratamiento de datos personales debe realizarse conforme a los principios, derechos y obligaciones establecidos en la Ley 1581 de 2012 y sus decretos reglamentarios.

Responsabilidad Demostrada: El IFC debe implementar controles verificables que permitan demostrar el cumplimiento de las obligaciones legales y normativas en materia de seguridad y privacidad de la información.

Enfoque Basado en Riesgos: Las acciones y decisiones relacionadas con la seguridad de la información deben priorizarse con base en la identificación, valoración y tratamiento de riesgos.

Mejora Continua: Los controles, procedimientos y actividades de seguridad deben ajustarse periódicamente para responder a cambios tecnológicos, normativos u operativos.

## 7. DECLARACIÓN INSTITUCIONAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

El Instituto Financiero de Casanare (IFC), en cumplimiento del Decreto 1078 de 2015, la Política de Seguridad y Privacidad de la Información del MinTIC, la Ley 1581 de 2012, la Ley 1712 de 2014, el Modelo Integrado de Planeación y Gestión (MIPG) y las buenas prácticas internacionales establecidas en las normas ISO/IEC 27001 e ISO/IEC 27701, adopta la presente Declaración Institucional de Seguridad y Privacidad de la Información como directriz superior para la protección, administración y tratamiento adecuado de su información, así como de los datos personales confiados a la entidad.

### 7.1. Naturaleza y alcances de esta Declaración

Con el objetivo de garantizar el cumplimiento de las obligaciones legales, fortalecer la gobernanza de la seguridad y establecer lineamientos estratégicos claros para toda la organización, el IFC incorpora esta Declaración dentro del Plan de Seguridad y Privacidad de la Información, la cual:

- ✓ Actúa como política institucional provisional,
- ✓ Define los principios, compromisos y directrices de alto nivel,
- ✓ Rige para todos los servidores públicos, contratistas, proveedores y terceros,
- ✓ Permanecerá vigente hasta que el IFC expida una Política como documento independiente, si así lo determina el CIGD.

Esta figura es válida según los lineamientos del MinTIC y se utiliza cuando una entidad pública se encuentra en proceso de fortalecimiento de su gestión de seguridad digital.

### 7.2. Declaración Institucional

El IFC declara que la seguridad y privacidad de la información son pilares fundamentales para garantizar:

- ✓ La continuidad de los servicios institucionales.
- ✓ La confianza de ciudadanos, clientes, proveedores y partes interesadas.
- ✓ La transparencia, integridad y legitimidad en el ejercicio de la función pública.
- ✓ La protección de los derechos de los titulares de datos personales.
- ✓ El cumplimiento de las obligaciones legales, regulatorias y normativas.

En consecuencia, la entidad se compromete a:

1. Proteger la confidencialidad, integridad, disponibilidad y trazabilidad de los activos de información bajo su custodia.
2. Implementar y mantener controles de seguridad administrativos, físicos, tecnológicos y organizacionales acordes con los riesgos institucionales.

3. Adoptar un enfoque basado en riesgos, conforme a ISO/IEC 27001, ISO/IEC 27005 y el Modelo de Seguridad y Privacidad del MinTIC.

4. Fortalecer la cultura institucional de seguridad y protección de datos, mediante procesos de sensibilización, capacitación y responsabilidad compartida.

5. Garantizar que el tratamiento de datos personales se realice bajo criterios de legalidad, finalidad, libertad, veracidad, transparencia, acceso restringido y seguridad, conforme a la Ley 1581 de 2012 y su reglamentación.

6. Prevenir, detectar, gestionar y responder eficazmente a incidentes de seguridad digital, aplicando las guías y lineamientos del MinTIC.

7. Implementar medidas para asegurar la continuidad del negocio, la recuperación ante desastres y la resiliencia operativa.

8. Exigir a proveedores, terceros y aliados tecnológicos el cumplimiento de las obligaciones de seguridad y privacidad aplicables.

9. Garantizar el adecuado manejo, protección y clasificación de la información institucional, incluyendo la información pública, reservada y clasificada conforme a la Ley 1712 de 2014.

10. Asegurar la evaluación y mejora continua del sistema de seguridad y privacidad de la información mediante auditorías internas y externas, revisión de controles y actualización periódica del presente Plan.

### 7.3. Alcance de obligatoriedad

Esta Declaración es de cumplimiento obligatorio para:

- ✓ Servidores Públicos
- ✓ Contratistas
- ✓ Proveedores
- ✓ Terceros que tengan acceso a información o sistemas del IFC
- ✓ Aliados tecnológicos o entidades que procesen información en nombre del Instituto

El desconocimiento o incumplimiento de estas directrices podrá generar sanciones disciplinarias, contractuales, administrativas o penales, según corresponda.

## 8. ROLES Y RESPONSABILIDADES

La gestión de la seguridad y privacidad de la información en el Instituto Financiero de Casanare (IFC) requiere la participación activa y articulada de todas las áreas, funcionarios, contratistas y terceros que intervienen en el tratamiento de los activos de información.

Con el fin de garantizar la gobernanza institucional, el cumplimiento de las obligaciones normativas y la ejecución efectiva del Plan de Seguridad y Privacidad de la Información, se establecen los siguientes roles y responsabilidades:

### 8.1. Gerencia - Comité Institucional de Gestión y Desempeño

La Alta Dirección es responsable de proveer el direccionamiento estratégico, los recursos necesarios y el respaldo institucional para la implementación y sostenibilidad del Plan. Sus responsabilidades incluyen:

- ✓ Aprobar el Plan de Seguridad y Privacidad de la Información y sus actualizaciones.
- ✓ Avalar la Declaración Institucional de Seguridad y Privacidad de la Información contenida en este documento.
- ✓ Garantizar la disponibilidad de recursos humanos, tecnológicos, financieros y administrativos para implementar los controles definidos.
- ✓ Integrar la seguridad y privacidad dentro del Modelo Integrado de Planeación y Gestión (MIPG).
- ✓ Aprobar las decisiones estratégicas relacionadas con riesgos, incidentes y acciones de tratamiento.
- ✓ Hacer seguimiento anual al cumplimiento de la seguridad y privacidad a través del Comité Institucional de Gestión y Desempeño.
- ✓ Fomentar la cultura de seguridad digital en toda la organización.

### 8.2. Gestión Tecnológica / Área de Sistemas

El área de sistemas lidera la implementación técnica, operativa y administrativa de los controles de seguridad y privacidad. Entre sus responsabilidades se encuentran:

- ✓ Implementar los controles técnicos de seguridad establecidos en el Plan.
- ✓ Gestionar accesos, autenticación, permisos, roles y privilegios.
- ✓ Administrar redes, servidores, equipos, firewall, antivirus, respaldos y sistemas críticos.

- ✓ Monitorear la infraestructura tecnológica para detectar incidentes o vulnerabilidades.
- ✓ Liderar la gestión de incidentes de seguridad digital, conforme a los lineamientos del MinTIC.
- ✓ Realizar copias de seguridad, actualizaciones, parches y mantenimiento preventivo.
- ✓ Evaluar riesgos tecnológicos y participar en la matriz institucional de riesgos.
- ✓ Coordinar la seguridad en servicios delegados, soluciones cloud y proveedores tecnológicos.
- ✓ Emitir informes técnicos, diagnósticos y recomendaciones para la mejora continua.

### 8.3. Delegado o Responsable de Protección de Datos Personales (Oficial o Responsable del tratamiento)

De acuerdo con la Ley 1581 de 2012:

- ✓ Velar por el cumplimiento de la Política de Tratamiento de Datos Personales.
- ✓ Asegurar que la entidad cumpla con los principios de legalidad, finalidad, transparencia, acceso y seguridad en el tratamiento de datos personales.
- ✓ Responder solicitudes de los titulares: consultas, reclamos, actualizaciones y supresiones.
- ✓ Coordinar acciones de sensibilización y capacitación en protección de datos.
- ✓ Supervisar el manejo de bases de datos institucionales y su registro en el RNBD (si aplica).
- ✓ Verificar que terceros y encargados del tratamiento cumplan las obligaciones contractuales.
- ✓ Interactuar con el Comité Institucional en casos de incidentes de privacidad.

### 8.4. Responsables y Líderes de Proceso

Cada jefe o líder de proceso es responsable de los activos de información generados, administrados o utilizados en su proceso.

Sus responsabilidades incluyen:

- ✓ Identificar, proteger y clasificar la información del proceso a su cargo.

- ✓ Garantizar el cumplimiento de políticas, controles y lineamientos definidos en el Plan.
- ✓ Reportar incidentes, fugas o anomalías relacionadas con información o tecnología.
- ✓ Gestionar los accesos de su personal y solicitar modificaciones cuando sea necesario.
- ✓ Asegurar que contratistas y terceros bajo su coordinación cumplan las medidas de seguridad.
- ✓ Mantener actualizada la información para inventarios de activos y matrices de riesgo.
- ✓ Facilitar auditorías, verificaciones y revisiones internas.

### 8.5. Servidores públicos y contratistas del IFC

Cada **servidor público y contratista del IFC** es responsable directo del uso adecuado, responsable y seguro de la información y de los recursos tecnológicos.

Deben:

- ✓ Cumplir la Declaración Institucional de Seguridad y Privacidad y todas las políticas asociadas.
- ✓ Manejar la información conforme a los principios de confidencialidad, integridad y disponibilidad.
- ✓ Usar solo los medios tecnológicos autorizados por el área de sistemas.
- ✓ Proteger contraseñas, dispositivos y accesos asignados.
- ✓ Reportar oportunamente incidentes o acciones sospechosas.
- ✓ Evitar conductas que pongan en riesgo los activos de información.
- ✓ Cumplir capacitaciones obligatorias en seguridad digital y protección de datos.

El incumplimiento puede generar sanciones disciplinarias, contractuales o administrativas.

### 8.6. Proveedores, Encargados del Tratamiento y Terceros

Los proveedores de soluciones tecnológicas, servicios cloud, infraestructura, software, hosting o servicios tercerizados que accedan a información del IFC deben:

- ✓ Cumplir los niveles de seguridad definidos contractualmente y en este Plan.
- ✓ Implementar medidas técnicas, organizacionales y físicas equivalentes a las del IFC.
- ✓ Firmar acuerdos de confidencialidad, tratamiento de datos y protección de la información.
- ✓ Reportar incidentes de seguridad que afecten servicios o información del IFC.
- ✓ Permitir auditorías o verificaciones cuando se requieran contractualmente.
- ✓ Asegurar la destrucción segura o devolución de la información al finalizar sus servicios.

### 8.7. Comité Institucional de Gestión y Desempeño

Este comité está encargado de:

- ✓ Revisar el desempeño del Plan.
- ✓ Analizar incidentes y riesgos relevantes.
- ✓ Aprobar acciones de mejora.
- ✓ Coordinar controles estratégicos y decisiones técnicas.

### 8.8. Grupos de valor y grupos de interés

Cuando interactúan con plataformas del IFC:

- ✓ Deben utilizar los canales oficiales y seguros.
- ✓ Están sujetos a las políticas de uso del portal y tratamiento de datos personales.
- ✓ Deben garantizar la veracidad de la información suministrada.

### 8.9. Actualización de Roles y Responsabilidades

Los roles definidos en este capítulo podrán actualizarse en función:

- ✓ de cambios tecnológicos,

- ✓ reestructuraciones institucionales,
- ✓ nuevas obligaciones normativas,
- ✓ la adopción futura de un Sistema de Gestión de Seguridad de la Información formalizado.

## 9. POLÍTICAS OPERATIVAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

El Instituto Financiero de Casanare (IFC) adopta las políticas operativas definidas por los referentes institucionales y normativos aplicables, particularmente las directrices del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) y el Modelo de Seguridad y Privacidad de la Información (MSPI), las cuales hacen parte integral del presente Plan y orientan el uso, la protección, la administración y el tratamiento de los activos de información, los recursos tecnológicos, los datos personales y los servicios institucionales.

Su cumplimiento es obligatorio para todos los funcionarios, trabajadores oficiales, contratistas, proveedores y terceros que interactúen con la información o sistemas del IFC.

### 9.1. Política de Clasificación y Manejo de la Información

El IFC adoptará un modelo de clasificación de la información digital que permita identificar niveles de sensibilidad, riesgo e impacto, y que facilite la aplicación de controles tecnológicos adecuados. La presente política aplica exclusivamente a la información gestionada en medios, sistemas y repositorios digitales institucionales.

La información institucional se clasificará como:

- ✓ Pública
- ✓ De acceso restringido (uso interno)
- ✓ Privada o confidencial
- ✓ Información pública clasificada y reservada (según Ley 1712 de 2014)

Lineamientos principales

- ✓ Toda información digital debe tener un responsable asignado dentro del proceso que la genera o administra.
- ✓ Los líderes de proceso son responsables de identificar y aplicar el nivel de clasificación correspondiente.

- ✓ El Área de Sistemas apoyará la implementación de los controles tecnológicos asociados a la clasificación (permisos, accesos, repositorios seguros, trazabilidad).

- ✓ La información clasificada, confidencial o reservada deberá contar con controles estrictos de acceso, uso, almacenamiento y transmisión en medios digitales.

- ✓ Los accesos deben otorgarse bajo el principio de mínimo privilegio.

- ✓ Se deben aplicar medidas de protección acordes al nivel de sensibilidad, incluyendo:

  - ➢ restricciones de acceso,
  - ➢ control de permisos,
  - ➢ almacenamiento en repositorios autorizados,
  - ➢ uso de canales seguros para transmisión,
  - ➢ trazabilidad y registro de actividades.

- ✓ La información digital no debe ser almacenada en dispositivos o servicios no autorizados.

- ✓ La gestión documental física y las TRD continúan bajo responsabilidad del Área de Archivo y no hacen parte de esta política.

### 9.2. Política de Control de Accesos

Con base en el principio de mínimo privilegio, el IFC garantizará que los accesos a la información digital, aplicaciones y sistemas se otorguen conforme a funciones, roles y responsabilidades, asegurando que cada usuario cuente únicamente con los permisos necesarios para el desempeño de sus actividades.

- ✓ Todos los usuarios tendrán credenciales individuales, únicas y no compartidas, garantizando trazabilidad y responsabilidad sobre las acciones realizadas en los sistemas institucionales.

- ✓ El acceso será otorgado únicamente previa solicitud autorizada por el líder de proceso, quien es responsable de validar la necesidad del permiso según las funciones del usuario y la clasificación de la información definida en el punto 9.1.

- ✓ Los accesos serán revocados de inmediato cuando el usuario:
  - ➢ cambie de cargo,
  - ➢ finalice su contrato,
  - ➢ pierda la autorización,
  - ➢ cuando el líder del proceso lo solicite expresamente.
- ✓ Se utilizarán mecanismos de autenticación robustos, tales como:
  - ➢ contraseñas seguras,
  - ➢ autenticación multifactor (MFA) cuando aplique,
  - ➢ políticas de expiración y bloqueo ante intentos fallidos.
- ✓ El Área de Sistemas será responsable de ejecutar la creación, modificación y revocación de accesos, garantizando que los permisos técnicos estén alineados con lo autorizado por el proceso y con los niveles de clasificación establecidos.
- ✓ Todo acceso deberá quedar registrado, incluyendo solicitudes, cambios, revocaciones y actividades relevantes, para efectos de auditoría y trazabilidad.

### 9.3. Política de Uso Aceptable de Recursos Tecnológicos

Los funcionarios, trabajadores oficiales y contratistas deben hacer uso responsable y adecuado de:

- ✓ Equipos de cómputo
- ✓ Redes, servidores y sistemas
- ✓ Correo institucional
- ✓ Internet y aplicaciones colaborativas
- ✓ Dispositivos móviles institucionales

- ✓ Almacenamiento en la nube autorizado

Se prohíbe:

- ✓ Instalar software no autorizado
- ✓ Compartir contraseñas
- ✓ Manipular equipos, cableado, routers o switches sin autorización
- ✓ Utilizar herramientas para evadir controles de seguridad
- ✓ Descargar contenido ilegal o de riesgo

### 9.4. Política de Seguridad en Infraestructura Tecnológica

- ✓ Todos los servidores, equipos de red, bases de datos y sistemas críticos estarán bajo administración exclusiva del área TIC.
- ✓ El IFC mantendrá configuraciones seguras, actualizaciones periódicas y parches de seguridad.
- ✓ Las redes internas estarán segmentadas para asegurar la protección de servicios críticos.
- ✓ El acceso físico a servidores y equipos críticos estará restringido y controlado.

### 9.5. Política de Gestión de Incidentes de Seguridad Digital

El IFC adoptará el modelo del MinTIC para la gestión de incidentes, incluyendo:

- ✓ Identificación
- ✓ Registro
- ✓ Análisis
- ✓ Contención
- ✓ Erradicación

- ✓ Recuperación
- ✓ Notificación a partes interesadas
- ✓ Cierre y lecciones aprendidas

Todos los usuarios deben reportar incidentes inmediatamente.

### 9.6. Política de Seguridad para Datos Personales

Complementa la Política de Tratamiento y Protección de Datos Personales ya existente:

- ✓ Todo tratamiento de datos personales deberá cumplir la Ley 1581 y su reglamentación.
- ✓ Los sistemas que manejen datos personales deben implementar medidas técnicas de protección.
- ✓ Se prohibe recolectar datos sin autorización válida, salvo excepciones legales.
- ✓ Los titulares podrán ejercer sus derechos de acceso, actualización y supresión.

### 9.7. Política de Copias de Seguridad y Recuperación

- ✓ El área de sistemas realizará copias de seguridad diarias, semanales y mensuales según criticidad.
- ✓ Las copias se almacenarán en repositorios seguros y aislados.
- ✓ Se realizarán pruebas periódicas de restauración.
- ✓ Las copias deben protegerse contra modificación, pérdida o acceso no autorizado.

### 9.8. Política de Continuidad del Negocio y Recuperación ante Desastres

El IFC deberá contar con:

- ✓ Estrategias de continuidad
- ✓ Procedimientos de recuperación

- ✓ Identificación de procesos críticos
- ✓ Matriz de tiempos de recuperación (RTO/RPO)
- ✓ Planes alternos para fallas tecnológicas, físicas o cibernéticas

Esta política se articulará con el Plan de Contingencia y Continuidad del Negocio que se aprobará posterior a este Plan de Seguridad y Privacidad de la Información.

### 9.9. Política de Seguridad en el Uso del Correo Electrónico Institucional

- ✓ El correo institucional es para fines laborales y es personal e intransferible.
- ✓ Se deben evitar correos sospechosos o enlaces no verificados.
- ✓ Se prohíbe enviar información confidencial sin cifrado o sin autorización.
- ✓ El área TIC gestionará la creación, configuración y eliminación de cuentas.

### 9.10. Política de Seguridad en Internet y Navegación

- ✓ El acceso a internet estará regulado por el firewall institucional.
- ✓ Se bloquearán sitios considerados de alto riesgo o no relacionados con las funciones del IFC.
- ✓ Se prohíbe el uso de redes privadas (VPN) no autorizadas para evadir controles.

### 9.11. Política de Gestión de Dispositivos Tecnológicos y Medios Extraíbles

- ✓ Se prohíbe el uso de USB en equipos institucionales, salvo autorización formal.
- ✓ Los dispositivos externos serán revisados por el área TIC antes de conectarse.
- ✓ Los equipos móviles institucionales deben tener antivirus, cifrado y controles de acceso.

### 9.12. Política de Seguridad Física

- ✓ Las áreas donde haya equipos tecnológicos críticos tendrán acceso controlado.

- ✓ El ingreso de visitantes o proveedores deberá registrarse y supervisarse.
- ✓ Se implementarán medidas para prevenir incendios, humedad, sobrecargas y manipulaciones no autorizadas.

### 9.13. Política de Seguridad para Terceros y Proveedores

Los proveedores que administren servicios o información del IFC deben:

- ✓ Cumplir estándares de seguridad exigidos en los contratos.
- ✓ Garantizar la protección de la información bajo su custodia.
- ✓ Notificar incidentes que afecten la información o servicios.
- ✓ Firmar acuerdos de confidencialidad y tratamiento de datos.

### 9.14. Política de Actualización, Parcheo y Hardening

- ✓ Todos los sistemas deberán estar actualizados con parches de seguridad.
- ✓ Se aplicarán configuraciones seguras (hardening) a sistemas operativos, bases de datos, aplicaciones y equipos de red.
- ✓ Se realizarán auditorías periódicas para verificar cumplimiento.

### 9.15. Política de Sensibilización y Cultura de Seguridad

El IFC implementará:

- ✓ Capacitaciones obligatorias en seguridad y privacidad.
- ✓ Campañas de sensibilización periódicas.
- ✓ Buenas prácticas para prevenir incidentes.
- ✓ Lineamientos simples para usuarios no técnicos.

## 10. CONTROLES DE SEGURIDAD DE LA INFORMACIÓN

El Instituto Financiero de Casanare (IFC) implementará controles de seguridad de la información orientados a mitigar riesgos, proteger los activos institucionales y garantizar la confidencialidad, integridad, disponibilidad, trazabilidad y privacidad de los datos.

Los controles aquí definidos se basan en las buenas prácticas establecidas por ISO/IEC 27002, el Modelo de Seguridad y Privacidad del MinTIC y la normativa vigente.

### 10.1. Control de Acceso

- ✓ El acceso a los sistemas y datos institucionales debe otorgarse bajo los principios de mínimo privilegio y necesidad de conocimiento.
- ✓ Toda asignación, modificación o revocatoria de permisos debe estar formalmente autorizada y registrada.
- ✓ Se deben emplear mecanismos de autenticación robustos, incluyendo autenticación multifactor cuando sea técnicamente viable.

### 10.2. Control de Usuarios y Credenciales

- ✓ Las cuentas de usuario deben ser únicas, personales e intransferibles.
- ✓ Las contraseñas deben cumplir con los criterios de complejidad, longitud y vigencia definidos por el IFC.
- ✓ Las cuentas inactivas, temporales o no utilizadas deben deshabilitarse o eliminarse según los lineamientos del Área Tecnológica.

### 10.3. Control de Infraestructura y Plataformas Tecnológicas

- ✓ Los servidores, equipos de red, estaciones de trabajo y dispositivos móviles deben contar con configuraciones seguras y actualizaciones periódicas.
- ✓ La infraestructura tecnológica debe protegerse mediante segmentación de redes, firewalls, sistemas de monitoreo, protección antimalware y controles perimetrales.
- ✓ Toda modificación en la infraestructura o su configuración debe gestionarse mediante un proceso formal de control de cambios.

### 10.4. Control de Seguridad Física

✓ Las áreas críticas (centro de datos, cuartos técnicos, racks) deben contar con acceso restringido, supervisado y registrado.

✓ Los equipos que procesan o almacenan información sensible deben ubicarse en ambientes seguros y protegidos contra riesgos ambientales y físicos.

✓ El ingreso de personal externo a áreas críticas debe estar autorizado y acompañado.

### 10.5. Control de Copias de Seguridad

✓ El Área de Sistemas debe realizar copias de seguridad periódicas de los sistemas, aplicaciones y bases de datos institucionales.

✓ Los respaldos deben almacenarse en ubicaciones seguras, con controles de acceso y, cuando aplique, cifrado.

✓ La restauración de respaldos debe probarse con la periodicidad definida por el IFC.

### 10.6. Control de Información Sensible y Datos Personales

✓ La información clasificada como sensible, reservada, confidencial o crítica debe protegerse mediante controles apropiados, incluido el cifrado cuando sea necesario.

✓ Todo tratamiento de datos personales debe cumplir con la Ley 1581 de 2012 y las políticas internas del IFC.

✓ La transferencia o divulgación de información sensible deberá estar autorizada y documentada.

### 10.7. Control de Comunicaciones y Transferencia de Información

✓ La información transmitida a través de redes internas o externas debe protegerse con mecanismos como cifrado, conexiones seguras y protocolos confiables.

✓ Las transferencias de información a terceros deben estar respaldadas por acuerdos de seguridad y confidencialidad.

✓ El uso de servicios en la nube debe garantizar canales seguros y cumplimiento de los lineamientos institucionales.

### 10.8. Control de Software y Aplicaciones

✓ Solo se permitirá el uso de software autorizado, licenciado y aprobado por el Área Tecnológica.

✓ Las aplicaciones institucionales deben contar con controles de seguridad en su diseño, desarrollo, pruebas y operación.

✓ Los parches, actualizaciones y mejoras deben aplicarse de forma oportuna y controlada.

### 10.9. Control de Proveedores y Servicios Externos

✓ Los proveedores deben implementar medidas de seguridad acordes con los riesgos del servicio prestado.

✓ Todo contrato debe incluir cláusulas de confidencialidad, seguridad digital, protección de datos y notificación de incidentes.

✓ El IFC podrá solicitar evidencias del cumplimiento de los controles definidos.

### 10.10. Control de Monitoreo, Auditoría y Registro

✓ El IFC debe registrar eventos relevantes de seguridad en los sistemas de información.

✓ El área responsable debe monitorear continuamente los sistemas, alertas y registros generados.

✓ Los registros deben conservarse según la normativa archivística y permitir auditorías internas y externas.

### 10.11. Control de Continuidad y Recuperación

✓ Los procesos críticos deben contar con medidas que aseguren la continuidad operativa y la recuperación ante fallos.

✓ Estos controles deben alinearse con el Plan de Contingencia y Continuidad del Negocio del IFC.

✓ Se deben realizar pruebas periódicas para validar la efectividad de los mecanismos de recuperación.

### 10.12. Supervisión y Actualización de los Controles

Los controles establecidos en este capítulo son de cumplimiento obligatorio para todas las áreas, procesos, trabajadores oficiales, contratistas y terceros que utilicen activos de información del IFC.

Su implementación será supervisada por el Área Tecnológica.

Los controles deben revisarse y actualizarse cuando existan cambios normativos, tecnológicos o institucionales.

## 11. GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

La Gestión de Riesgos de Seguridad de la Información en el Instituto Financiero de Casanare – IFC se desarrolla bajo un enfoque integral, preventivo y sistemático, que permite identificar, analizar, evaluar, tratar y monitorear los riesgos que puedan afectar la confidencialidad, integridad, disponibilidad, privacidad y trazabilidad de los activos de información institucionales.

El proceso se encuentra alineado con el Procedimiento de Gestión y Administración del Riesgo, con el Modelo de Seguridad y Privacidad de la Información del MinTIC, el Modelo Integrado de Planeación y Gestión – MIPG, la Guía de Administración del Riesgo del DAFP, y con estándares internacionales como ISO/IEC 27001 e ISO/IEC 27005, garantizando un enfoque estructurado y acorde con las exigencias regulatorias y de control interno.

### 11.1. Marco Institucional

La administración del riesgo en el IFC se desarrolla bajo el marco definido en el Procedimiento de Gestión y Administración del Riesgo, el cual establece la estructura, responsabilidades y actividades necesarias para garantizar una adecuada identificación, valoración, tratamiento y monitoreo de los riesgos institucionales.

Dentro de este marco se articulan:

a) Tres líneas de defensa institucional

- ✓ Primera línea: Servidores todos los niveles. (Directivos, funcionarios, trabajadores oficiales, contratistas, proveedores y terceros)
- ✓ Segunda línea: Oficina Asesora de Planeación – Riesgos, como instancia encargada de coordinar el sistema de administración del riesgo y consolidar la información institucional.
- ✓ Tercera línea: Oficina de Control Interno, responsable de evaluar la efectividad de los controles y del sistema de administración del riesgo.

b) Línea estratégica

- ✓ Alta Dirección (Comités base MIPG)

Estas instancias definen prioridades, revisan riesgos críticos, evalúan brechas de control y orientan decisiones de nivel gerencial.

Esta estructura se integra plenamente al ámbito de seguridad y privacidad de la información, asegurando coherencia entre los riesgos tecnológicos y los riesgos institucionales generales.

### 11.2. Metodología General para la Gestión de Riesgos de Seguridad de la Información

El IFC adopta una metodología basada en buenas prácticas, integrando los lineamientos del DAFP y los principios de ISO 27005. El ciclo comprende:

1. Identificación del riesgo

Incluye la determinación de:

- ✓ Activos de información (datos, aplicaciones, sistemas, infraestructura, servicios).
- ✓ Responsables del activo.
- ✓ Vulnerabilidades técnicas, humanas, procedimentales o derivadas de terceros.
- ✓ Amenazas internas y externas (errores, ataques, fallas, desastres, accesos indebidos).
- ✓ Impactos sobre la confidencialidad, integridad, disponibilidad o privacidad.

La identificación se apoya en:

- ✓ La Matriz de Riesgos de Seguridad Digital del IFC.
- ✓ Resultados de auditorías.
- ✓ Incidentes reportados.
- ✓ Pruebas de seguridad, análisis de vulnerabilidades o revisiones técnicas.
- ✓ Cambios normativos o tecnológicos.

2. Análisis del riesgo

Se evalúan variables como:

- ✓ Probabilidad de materialización.
- ✓ Impacto operacional, financiero, reputacional, legal y de datos personales.
- ✓ Brechas de control existentes.
- ✓ Grado de exposición tecnológica e institucional.

3. Valoración y priorización

Se calcula el riesgo inherente y residual, clasificándolo en:

- ✓ Bajo
- ✓ Medio
- ✓ Alto
- ✓ Extremo

Los riesgos altos o extremos deben ser elevados a la Alta Dirección y revisados en el Comité de Riesgos.

4. Tratamiento del riesgo

El IFC puede optar por:

- ✓ Mitigar: implementar controles técnicos, administrativos o físicos.
- ✓ Transferir: suscribir seguros o delegar en terceros especializados.
- ✓ Aceptar: cuando el riesgo residual es tolerable.
- ✓ Evitar: eliminando la causa que lo origina.

Las medidas de tratamiento se documentan en la Matriz de Riesgos de Seguridad Digital y en los planes de acción correspondientes.

5. Seguimiento y monitoreo

Incluye:

- ✓ Verificación periódica del cumplimiento de controles.
- ✓ Seguimiento a planes de acción.
- ✓ Monitoreo de vulnerabilidades e incidentes.
- ✓ Revisión semestral o anual de matrices.
- ✓ Informes para el Comité de Riesgos y la Alta Dirección.

6. Mejora continua

Se ajustan los controles y el análisis del riesgo cuando:

- ✓ Se presentan incidentes.
- ✓ Se detectan nuevas amenazas.
- ✓ Se realizan cambios tecnológicos.
- ✓ Se actualiza la normatividad.
- ✓ Lo recomiendan auditorías o revisiones internas.

### 11.3. Integración con el Ciclo Institucional del Riesgo

La gestión de riesgos de seguridad y privacidad se integra de manera directa al ciclo institucional, adaptando las actividades del Procedimiento de Gestión y Administración del Riesgo a este ámbito específico:

1. Revisión y actualización de las matrices de riesgos de seguridad

Los líderes de proceso y el profesional de riesgos revisan los riesgos asociados a información, tecnología, ciberseguridad, datos personales y continuidad.

2. Gestión integral del riesgo

Se definen las actividades de seguridad y privacidad dentro de los instrumentos de planeación y seguimiento institucional.

3. Plan de trabajo de seguimiento

Establece actividades trimestrales y semestrales para revisar controles, verificar cumplimiento y actualizar los niveles de riesgo.

4. Revisión de matrices por proceso

Los líderes realizan análisis y actualización de riesgos relacionados con:

- ✓ Sistemas de información
- ✓ Tratamiento de datos personales
- ✓ Aplicativos misionales
- ✓ Infraestructura tecnológica
- ✓ Gestión documental
- ✓ Continuidad del negocio

5. Actualización de la Matriz Institucional

La Oficina de Planeación consolida los riesgos de seguridad provenientes de los procesos y los incorpora en la matriz general institucional.

6. Informes periódicos

Incluyen:

- ✓ Riesgos operacionales asociados a TI.
- ✓ Vulnerabilidades detectadas.
- ✓ Incidentes relevantes.
- ✓ Avances en los planes de tratamiento.

7. Alertas tempranas

Se monitorean señales de posible materialización de riesgos, como:

- ✓ Accesos no autorizados.

- ✓ Fallos en sistemas críticos.
- ✓ Variaciones inusuales en operaciones.
- ✓ Indicadores de ciberataques.

8. Comité de Riesgos

Los riesgos de seguridad digital se presentan y analizan para su validación, priorización y toma de decisiones.

9. Valoración de controles

La Oficina de Control Interno evalúa la efectividad de los controles existentes, verificando:

- ✓ Cumplimiento de políticas.
- ✓ Evidencias de seguimiento.
- ✓ Registro adecuado de incidentes y medidas correctivas.

10. Evaluación integral del riesgo

Se revisa:

- ✓ La metodología aplicada.
- ✓ La consistencia entre riesgo, controles y evidencias.
- ✓ La pertinencia de los niveles residuales.

11. Planes de manejo

Se generan recomendaciones para fortalecer:

- ✓ Controles deficientes.
- ✓ Procesos o procedimientos.
- ✓ Capacitación o sensibilización.

- ✓ Documentación y trazabilidad.

### 11.4. Articulación con el Plan de Tratamiento de Riesgos de Seguridad y Privacidad

Los riesgos identificados en la Matriz de Riesgos de Seguridad Digital deben tener:

- ✓ Acciones de mitigación específicas.
- ✓ Responsables claramente definidos.
- ✓ Prioridades y plazos establecidos.
- ✓ Indicadores verificables.
- ✓ Evidencias documentales de ejecución.

Este plan se revisa al menos anualmente o ante cualquier cambio significativo en la infraestructura tecnológica o normativa.

### 11.5. Responsables de la Gestión del Riesgo

- ✓ Alta Dirección: define prioridades estratégicas y aprueba decisiones críticas.
- ✓ Comité de Riesgos: valida análisis y medidas de mitigación.
- ✓ Oficina de Planeación – Riesgos: coordina el Sistema Integrado de Administración del Riesgo - SIAR.
- ✓ Líderes de proceso: identifican, evalúan y actualizan los riesgos de sus áreas.
- ✓ Área de Tecnología / Seguridad Digital: implementa controles técnicos, identifica vulnerabilidades y gestiona incidentes.
- ✓ Oficina de Control Interno: evalúa la eficacia del sistema de administración del riesgo.
- ✓ Terceros y proveedores: cumplen con los lineamientos de seguridad definidos por el IFC.

### 11.6. Evidencias y Documentación Soporte

La gestión de riesgos genera como evidencia:

- ✓ Matriz de Riesgos de Seguridad Digital.
- ✓ Matriz Institucional consolidada.
- ✓ Plan de Tratamiento de Riesgos.
- ✓ Informes de auditoría.
- ✓ Reportes de incidentes.
- ✓ Registro de vulnerabilidades.
- ✓ Actas de Comité de Riesgos.
- ✓ Informes de Control Interno.
- ✓ Evidencias de implementación de controles.

### 11.7. Mejora Continua

La gestión de riesgos es un proceso dinámico. Sus resultados se retroalimentan con:

- ✓ Lecciones aprendidas de incidentes.
- ✓ Recomendaciones del Comité de Riesgos.
- ✓ Hallazgos de auditorías internas y externas.
- ✓ Cambios tecnológicos o normativos.
- ✓ Retroalimentación de los procesos y usuarios.

El ciclo de mejora continua garantiza que los riesgos de seguridad y privacidad se gestionen de manera oportuna, efectiva y alineada con los objetivos estratégicos del IFC.

## 12. GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

La Gestión de Incidentes de Seguridad de la Información en el Instituto Financiero de Casanare – IFC constituye un proceso fundamental para garantizar la protección de los activos de información, la continuidad de la operación institucional y el cumplimiento de las obligaciones legales,

contractuales y normativas relacionadas con seguridad digital, ciberseguridad y protección de datos personales.

El IFC adopta un enfoque estructurado basado en buenas prácticas internacionales (ISO/IEC 27035), en el Modelo de Seguridad y Privacidad del MinTIC, en el Modelo Integrado de Planeación y Gestión – MIPG, y en los lineamientos internos definidos por la Alta Dirección para la atención y respuesta de incidentes que puedan afectar la integridad, confidencialidad, disponibilidad y privacidad de la información.

### 12.1. Definición de Incidente de Seguridad de la Información

Se entiende como incidente de seguridad cualquier evento, real o potencial, que:

- ✓ Afecte la operación normal de los sistemas de información.
- ✓ Comprometa la integridad, disponibilidad o confidencialidad de datos.
- ✓ Implique acceso no autorizado a información, sistemas o infraestructura.
- ✓ Genere pérdida, fuga, alteración o divulgación indebida de información.
- ✓ Vulnere datos personales o información financiera.
- ✓ Indique la materialización de amenazas internas o externas.

Ejemplos comunes incluyen:

- ✓ Ataques de phishing o spear phishing
- ✓ Malware, ransomware, intrusiones o intentos de intrusión
- ✓ Fallos críticos en plataformas o servidores
- ✓ Filtración, pérdida o manipulación de datos
- ✓ Robo o extravío de equipos
- ✓ Accesos indebidos o privilegios mal gestionados
- ✓ Fallos en servicios de terceros

- ✓ Inconsistencias o manipulaciones en procesos misionales
- ✓ Incidentes asociados a proveedores tecnológicos

### 12.2. Clasificación de los Incidentes

Para garantizar una gestión adecuada, los incidentes se clasifican según:

1. Tipo

- ✓ Técnicos: malware, ataques, fallos de infraestructura.
- ✓ Humanos: errores, negligencia, ingeniería social.
- ✓ Operativos: fallos de procesos, indisponibilidad de sistemas.
- ✓ Físicos: pérdida o robo de equipos, daños por eventos externos.
- ✓ Terceros: fallas de proveedores, incumplimientos contractuales.

2. Impacto

- ✓ Bajo: afectación mínima y controlable.
- ✓ Medio: afecta procesos pero con alternativas de operación.
- ✓ Alto: detiene procesos críticos o compromete datos sensibles.
- ✓ Crítico: afectación grave a la entidad, datos personales, sistemas financieros o imagen institucional.

3. Naturaleza

- ✓ Incidentes de seguridad digital
- ✓ Incidentes de privacidad de datos personales
- ✓ Incidentes operacionales o tecnológicos

- ✓ Incidentes asociados al SARLAFT, cuando apliquen

### 12.3. Ciclo de Gestión de Incidentes

El IFC adopta un ciclo de gestión basado en las fases internacionales de ISO 27035:

1. Preparación

Incluye:

- ✓ Políticas y controles definidos en este Plan.
- ✓ Sensibilización y formación del personal.
- ✓ Identificación de activos críticos.
- ✓ Mecanismos de monitoreo y alertas.
- ✓ Procedimientos internos de notificación.
- ✓ Contratos con proveedores con cláusulas de seguridad.

2. Detección y Reporte

Los incidentes pueden detectarse mediante:

- ✓ Sistemas de monitoreo y alertas.
- ✓ Herramientas de seguridad (antimalware, firewall, IDS/IPS).
- ✓ Auditorías y revisiones técnicas.
- ✓ Reportes de usuarios o líderes de proceso.
- ✓ Señales de fraude, manipulación o anomalías operacionales.

Todo funcionario, contratista o proveedor debe reportar inmediatamente cualquier anomalía al área encargada de tecnología/seguridad digital o al líder del proceso involucrado.

3. Registro del incidente

Todo incidente debe registrarse formalmente y contener:

- ✓ Fecha y hora.
- ✓ Descripción del evento.
- ✓ Sistemas o procesos afectados.
- ✓ Nivel de criticidad.
- ✓ Acciones iniciales.
- ✓ Evidencias recopiladas.

La evidencia debe preservarse adecuadamente para análisis posterior.

4. Análisis y clasificación

El análisis incluye:

- ✓ Identificación de causa raíz.
- ✓ Sistemas afectados y alcance del daño.
- ✓ Impacto operativo, financiero, legal y reputacional.
- ✓ Riesgo asociado a datos personales.
- ✓ Necesidad de contención inmediata.

5. Contención

Se deben ejecutar acciones rápidas para limitar el daño, tales como:

- ✓ Aislar equipos o cuentas comprometidas.
- ✓ Bloquear accesos.
- ✓ Suspender procesos o servicios afectados.
- ✓ Proteger copias de seguridad.

- ✓ Activar medidas de contingencia.

6. Erradicación

Incluye:

- ✓ Eliminación de malware o código malicioso.
- ✓ Corrección de vulnerabilidades explotadas.
- ✓ Aseguramiento de configuraciones.
- ✓ Desactivación de cuentas o permisos indebidos.
- ✓ Reparación de servicios comprometidos.

7. Recuperación

El objetivo es restablecer la operación normal garantizando que el incidente no se repita.

Actividades:

- ✓ Restauración de servicios y datos.
- ✓ Validación técnica de la operación segura.
- ✓ Pruebas de funcionalidad.
- ✓ Rehabilitación de cuentas y accesos.
- ✓ Monitoreo posterior al restablecimiento.

8. Cierre y documentación

Debe documentarse:

- ✓ Causa raíz.
- ✓ Controles afectados.

- ✓ Acciones aplicadas.
- ✓ Evidencias.
- ✓ Medidas futuras de prevención.
- ✓ Requerimientos de mejora.

9. Lecciones aprendidas y mejora continúa

El incidente debe retroalimentar:

- ✓ La Matriz de Riesgos de Seguridad Digital.
- ✓ El Plan de Tratamiento de Riesgos.
- ✓ Las políticas operativas y técnicas.
- ✓ Los procesos institucionales.
- ✓ El plan de continuidad y contingencia.
- ✓ La capacitación del personal.

### 12.4. Roles y Responsabilidades en la Gestión de Incidentes

- ✓ Área de Sistemas / Gestión Tecnológica: recepción, análisis técnico, contención y recuperación de incidentes.
- ✓ Líderes de proceso: detección temprana, reporte y colaboración con la investigación.
- ✓ Oficina Asesora de Planeación – Riesgos: análisis de impacto en el sistema de administración del riesgo.
- ✓ Alta Dirección: toma de decisiones críticas y asignación de recursos.
- ✓ Oficina de Control Interno: verificación independiente, evaluación de controles y recomendaciones.

- ✓ Contratistas y proveedores: deben cumplir con obligaciones contractuales de seguridad y colaborar en la atención del incidente.
- ✓ Usuarios en general: detección temprana y reporte oportuno de anomalías.

### 12.5. Coordinación con Otros Planes y Procedimientos Institucionales

La gestión de incidentes se articula con:

- ✓ El Plan de Continuidad y Contingencia del IFC
- ✓ El Plan de Tratamiento de Riesgos de Seguridad y Privacidad
- ✓ El Procedimiento de Gestión y Administración del Riesgo
- ✓ El Plan de Respaldo y Recuperación de Información
- ✓ Políticas operativas del numeral 9 del presente plan
- ✓ Procedimientos de proveedores o aliados tecnológicos

Cuando un incidente supera la capacidad operativa normal o compromete procesos críticos, se activa el esquema de continuidad institucional.

### 12.6. Notificación Interna y Externa

Dependiendo del tipo de incidente, se realiza notificación a:

- ✓ Alta Dirección
- ✓ Comité de Riesgos
- ✓ Oficina Asesora Jurídica (cuando se afectan datos personales o responsabilidades legales)
- ✓ Oficina de Control Interno
- ✓ Autoridades externas cuando aplique, como:
  - ➢ CeCip (Dirección de Investigación Criminal e INTERPOL)

- SIC (por incidentes de datos personales)
- MinTIC (cuando corresponda a incidentes digitales de alta criticidad)

Toda notificación debe seguir los lineamientos institucionales.

### 12.7. Evidencias y Registros

Como resultado del proceso deben mantenerse:

- ✓ Registro de incidentes
- ✓ Bitácoras o logs del evento
- ✓ Evidencias técnicas (capturas, reportes, análisis forense)
- ✓ Comunicaciones internas y actas
- ✓ Recomendaciones posteriores
- ✓ Acciones de mejora
- ✓ Validaciones de cierre

La evidencia debe protegerse para garantizar integridad, autenticidad y trazabilidad.

### 12.8. Mejora Continua

La gestión de incidentes debe revisarse cada año o después de incidentes significativos, garantizando:

- ✓ Actualización de controles y políticas
- ✓ Evaluación del desempeño del proceso
- ✓ Ajustes a los planes de tratamiento
- ✓ Inclusión de nuevos riesgos en la matriz
- ✓ Capacitación al personal según los hallazgos

La efectividad del proceso se evalúa mediante indicadores como:

- ✓ Tiempo de respuesta
- ✓ Tiempo de recuperación
- ✓ Número de incidentes repetitivos
- ✓ Grado de impacto
- ✓ Cumplimiento de procedimientos
- ✓ Calidad de las evidencias y registros

## 13. GESTIÓN DE LA CONTINUIDAD Y CONTINGENCIA DEL SERVICIO

La gestión de la continuidad y contingencia del servicio en el Instituto Financiero de Casanare – IFC tiene como propósito garantizar que los procesos esenciales de la entidad puedan continuar operando o restablecerse en el menor tiempo posible ante incidentes de seguridad, fallas tecnológicas, eventos disruptivos o situaciones externas que afecten la disponibilidad de los sistemas de información y de los servicios institucionales.

Este componente se articula directamente con la gestión de riesgos de seguridad de la información, la gestión de incidentes y, de manera principal, con el Plan de Continuidad del Negocio del IFC, el cual desarrolla en detalle las estrategias, procedimientos y responsabilidades para mantener la operación institucional ante eventos de interrupción.

### 13.1. Relación entre Seguridad de la Información y Continuidad del Servicio

La seguridad de la información es un habilitador esencial para la continuidad del servicio. En el IFC, ambas dimensiones se integran mediante:

- ✓ La identificación de riesgos tecnológicos y de seguridad que puedan interrumpir la operación.
- ✓ La inclusión de controles de seguridad dentro de los escenarios del Plan de Continuidad del Negocio.
- ✓ La consideración de los incidentes de seguridad como posibles desencadenantes de la activación del plan.

- ✓ La protección de la información durante la operación en contingencia o en ambientes alternos.
- ✓ La coordinación entre el análisis de impacto al negocio (BIA) y los riesgos de seguridad digital.

El objetivo es asegurar que, ante cualquier interrupción, la entidad pueda continuar funcionando sin comprometer la integridad, confidencialidad o disponibilidad de la información institucional.

### 13.2. Principios Generales de Continuidad aplicados a Seguridad de la Información

1. Disponibilidad garantizada: Los sistemas y datos esenciales deben permanecer accesibles durante interrupciones o ser recuperados en los tiempos establecidos por el IFC.
2. Protección de la información: La información tratada durante contingencias debe mantenerse segura y sin alteraciones.
3. Reducción del impacto: Los incidentes de seguridad deben atenderse rápidamente para evitar interrupciones prolongadas.
4. Capacidad de recuperación: Los sistemas deben tener mecanismos de respaldo y recuperación que aseguren el restablecimiento seguro.
5. Evidencia y trazabilidad: Toda acción realizada durante contingencias debe quedar debidamente registrada.

### 13.3. Activación de medidas de continuidad relacionadas con Seguridad

Las medidas de continuidad relacionadas con seguridad se activan cuando:

- ✓ Un incidente de seguridad digital afecta sistemas o datos críticos.
- ✓ Se presentan fallas técnicas que comprometen la operación.
- ✓ Se materializan riesgos de alto impacto identificados en la Matriz de Riesgos de Seguridad Digital.
- ✓ Se produce una indisponibilidad significativa de servicios tecnológicos.
- ✓ Lo determina la Alta Dirección o el área de sistemas en coordinación con los líderes de proceso.

En estos casos, la gestión de incidentes se integra con el proceso de continuidad para ejecutar acciones de restablecimiento seguro.

### 13.4. Responsabilidades en Continuidad y Contingencia (Nivel Seguridad)

- ✓ Alta Dirección: autoriza la activación de medidas excepcionales y apoya la priorización de recursos.
- ✓ Área de sistemas / Gestión Tecnológica: ejecuta acciones técnicas de recuperación y garantiza la protección de la información en ambientes alternos.
- ✓ Líderes de proceso: aplican procedimientos operativos definidos para escenarios de contingencia.
- ✓ Oficina Asesora de Planeación – Sistema de Administración de Riesgos: registra afectaciones en el sistema de administración del riesgo y evalúa impacto institucional.
- ✓ Oficina de Control Interno: realiza seguimiento a la ejecución y cumplimiento de controles relacionados con seguridad en escenarios de contingencia.
- ✓ Proveedores tecnológicos: deben cumplir con los niveles de servicio y cláusulas de continuidad pactadas contractualmente.

### 13.5. Articulación directa con el Plan de Continuidad del Negocio

El Plan de Seguridad y Privacidad se articula con el Plan de Continuidad del Negocio del IFC, el cual desarrolla de manera detallada:

- ✓ La priorización de procesos según análisis de impacto al negocio (BIA).
- ✓ Los tiempos máximos tolerables de interrupción (MTD).
- ✓ Los tiempos de recuperación tecnológica (RTO/RPO).
- ✓ Las estrategias de operación en ambientes alternos.
- ✓ Los procedimientos por proceso para escenarios de contingencia.
- ✓ La recuperación ante desastres (DRP) y restauración de sistemas.
- ✓ Los roles y responsabilidades específicos durante emergencias.

Este capítulo reafirma que los aspectos de seguridad son parte fundamental del BCP, pero no sustituye el documento, que es el instrumento rector en materia de continuidad.

### 13.6. Evidencias y Registros

Como resultado de la activación de medidas de contingencia relacionadas con seguridad deben mantenerse:

- ✓ Registros de incidentes que motivaron la activación.
- ✓ Evidencias de recuperación o restablecimiento de sistemas.
- ✓ Informes de acciones aplicadas.
- ✓ Comunicaciones internas y externas.
- ✓ Recomendaciones posteriores al evento.

La evidencia se archiva conforme a la normativa de gestión documental institucional.

### 13.7. Mejora Continua

El mecanismo de continuidad asociado a seguridad se revisa:

- ✓ Después de incidentes con impacto significativo.
- ✓ Durante la actualización anual del Plan de Continuidad del Negocio.
- ✓ A partir de recomendaciones del Comité de Riesgos y Control Interno.
- ✓ Ante cambios tecnológicos, infraestructura nueva o modernización de sistemas.

Los resultados deben retroalimentar:

- ✓ Los controles del Plan de Seguridad y Privacidad.
- ✓ Los riesgos incluidos en la Matriz de Seguridad Digital.
- ✓ El Plan de Continuidad del Negocio.

## 14. GESTIÓN DOCUMENTAL Y CUMPLIMIENTO NORMATIVO

La Gestión Documental y el Cumplimiento Normativo en el ámbito de la seguridad y privacidad de la información en el Instituto Financiero de Casanare – IFC tienen como propósito garantizar que la información institucional sea administrada, protegida, conservada y dispuesta conforme a la normativa vigente, al ciclo de vida documental y a los lineamientos de seguridad digital establecidos por la entidad.

Este componente establece los criterios que aseguran que la documentación física y electrónica relacionada con seguridad, privacidad, incidentes, riesgos, controles y continuidad cuente con integridad, autenticidad, disponibilidad y trazabilidad, y se gestione conforme a los lineamientos del Archivo General de la Nación, el Modelo de Seguridad y Privacidad de la Información y el Modelo Integrado de Planeación y Gestión – MIPG.

### 14.1. Marco Normativo Aplicable

La Gestión Documental en materia de seguridad y privacidad se rige por el marco normativo general descrito en el Capítulo 5 de este Plan. Adicionalmente, para el manejo específico de la documentación física y electrónica del IFC, aplican las disposiciones propias del sistema archivístico nacional, particularmente:

- ✓ Ley 594 de 2000 – Ley General de Archivos.
- ✓ Normativa del Archivo General de la Nación (AGN) en materia de gestión documental, preservación, conservación, organización, transferencia y disposición final.
- ✓ Decreto 2609 de 2012, relacionado con lineamientos técnicos para la gestión documental en entidades públicas.
- ✓ Tablas de Retención Documental (TRD) y demás instrumentos archivísticos institucionales definidos por el IFC.
- ✓ Lineamientos y estándares técnicos aplicables al manejo documental electrónico emitidos por el AGN y el MinTIC.

Estas normas complementan el marco general del Plan, asegurando que la documentación relacionada con seguridad y privacidad se gestione conforme al ciclo de vida documental, manteniendo su integridad, autenticidad, disponibilidad y confidencialidad.

### 14.2. Principios de la Gestión Documental aplicados a la Seguridad de la Información

1. Integridad: la información no debe ser modificada sin autorización.

2. Disponibilidad: los documentos deben estar accesibles cuando se requiera, en función del nivel de criticidad.
3. Confidencialidad: acceso permitido únicamente a personal autorizado.
4. Autenticidad: los documentos deben ser válidos y verificables.
5. Trazabilidad: todo acceso, modificación o disposición debe quedar registrado.
6. Conservación: garantizar la preservación del patrimonio documental.
7. Legalidad: adecuación a los requisitos normativos y técnicos.

### 14.3. Clasificación y Control de Documentos Relacionados con Seguridad y Privacidad

El IFC debe asegurar que la documentación relacionada con seguridad y privacidad sea clasificada conforme a:

a) Nivel de sensibilidad

- ✓ Información pública
- ✓ Información de uso interno
- ✓ Información confidencial
- ✓ Información reservada (cuando aplique legalmente)

b) Tipo de documento

- ✓ Políticas, normas y lineamientos
- ✓ Procedimientos operativos y técnicos
- ✓ Registros de incidentes
- ✓ Evidencias de auditoría
- ✓ Matrices de riesgos y planes de tratamiento
- ✓ Informes de continuidad y contingencia

- ✓ Bitácoras y trazas
- ✓ Documentos contractuales con terceros
- ✓ Registros de acceso y actividades

c) Ciclo de vida documental

- ✓ Producción
- ✓ Trámite
- ✓ Organización
- ✓ Transferencia
- ✓ Disposición final (conservación o eliminación)

La información con implicaciones de seguridad o privacidad deberá contar con esquemas de control de acceso y medidas de protección incrementadas.

### 14.4. Custodia, Conservación y Respaldo de Documentos

El IFC debe garantizar:

- ✓ Custodia física en espacios seguros y controlados.
- ✓ Custodia electrónica en sistemas de información institucionales con mecanismos de autenticación, cifrado y registro de actividades.
- ✓ Respaldo periódico de documentación electrónica crítica.
- ✓ Controles de acceso lógico según roles y privilegios definidos.
- ✓ Conservación a largo plazo según tablas de retención documental (TRD).
- ✓ Protección contra pérdida, daño, alteración o divulgación indebida.

Los documentos relacionados con incidentes, riesgos, planes o auditorías tienen carácter estratégico y deben conservarse conforme a los tiempos definidos en las TRD y la normativa del AGN.

### 14.5. Disposición Final de Documentos

La información relacionada con seguridad y privacidad debe ser dispuesta conforme a:

- ✓ Tablas de Retención Documental del IFC
- ✓ Políticas del Archivo General de la Nación
- ✓ Normativa de protección de datos personales
- ✓ Criterios de seguridad y clasificación de la información

La eliminación de documentación debe realizarse mediante métodos seguros (digitales o físicos), con registro y evidencia de la disposición final.

### 14.6. Cumplimiento Normativo en Seguridad y Privacidad de la Información

El IFC debe asegurar el cumplimiento de:

- ✓ Principios de protección de datos personales.
- ✓ Obligaciones en materia de habeas data.
- ✓ Requisitos de seguridad digital establecidos por MinTIC.
- ✓ Lineamientos de acceso a la información pública.
- ✓ Normativa sobre transparencia y reserva de la información.
- ✓ Estándares técnicos aplicables a la seguridad de datos y documentos.
- ✓ Obligaciones contractuales con proveedores tecnológicos.

El incumplimiento puede generar riesgos legales, sancionatorios, operativos o de reputación.

### 14.7. Evidencias y Registros del Cumplimiento

Como resultado de la gestión documental y normativa, deben mantenerse:

- ✓ Registros de acceso y modificación a documentos.

- ✓ Actas, informes y trazas de auditoría.
- ✓ Evidencias de capacitación al personal.
- ✓ Registros de incidentes y medidas de seguridad aplicadas.
- ✓ Bitácoras de transferencias documentales.
- ✓ Documentación de procedimientos y controles.
- ✓ Evidencias de eliminación de documentos.

Estos registros soportan el cumplimiento de obligaciones legales y sirven como evidencia ante auditorías internas y externas.

### 14.8. Mejora Continua

La gestión documental y el cumplimiento normativo en materia de seguridad y privacidad se revisan periódicamente mediante:

- ✓ Auditorías internas y externas.
- ✓ Actualización de normativa.
- ✓ Evaluación de riesgos y controles documentales.
- ✓ Revisión del Comité Institucional de Gestión y Desempeño.
- ✓ Retroalimentación del proceso de seguridad y privacidad.

Los resultados deben traducirse en ajustes a procedimientos, controles, sistemas de información y prácticas institucionales.

## 15. SEGUIMIENTO, EVALUACIÓN Y MEJORA CONTINUA

El Seguimiento, Evaluación y Mejora Continua del Plan de Seguridad y Privacidad de la Información del Instituto Financiero de Casanare – IFC constituye un componente esencial para garantizar la efectividad y vigencia del conjunto de políticas, controles, procedimientos y actividades definidas en este instrumento.

Este proceso se articula con los lineamientos del Modelo Integrado de Planeación y Gestión – MIPG, el Sistema de Control Interno, la gestión institucional del riesgo, los ciclos de auditoría, los comités de control y desempeño y los procesos de mejora continua adoptados por la entidad.

### 15.1. Lineamientos de Seguimiento

El seguimiento del Plan se realiza mediante actividades periódicas orientadas a:

1. Verificar la implementación y cumplimiento de los controles definidos.
2. Identificar brechas o desviaciones.
3. Evaluar la eficacia de los controles y medidas adoptadas.
4. Revisar la pertinencia de políticas, roles, responsabilidades y procedimientos.
5. Monitorear incidentes y vulnerabilidades relevantes.
6. Revisar avances en los planes de tratamiento de riesgos.
7. Aplicar ajustes derivados de auditorías, comité de riesgos o cambios normativos.

Estas actividades se realizarán de manera semestral.

### 15.2. Evaluación del Plan

La evaluación del Plan de Seguridad y Privacidad debe desarrollarse:

a) Una vez al año, coincidiendo con la actualización del Sistema Integral de Administración de Riesgos y del proceso de direccionamiento estratégico y planeación.

b) Después de incidentes de alta criticidad, que evidencien debilidades de controles o procesos.

c) Después de auditorías internas o externas, incluyendo:

- ✓ Auditorías basadas en riesgos
- ✓ Auditorías de gestión tecnológica
- ✓ Evaluaciones de Control Interno

d) Ante cambios tecnológicos o de infraestructura, especialmente en:

- ✓ Sistemas de información misionales.

- ✓ Plataformas de nube o servicios externos.
- ✓ Infraestructura crítica.
- ✓ Procesos institucionales altamente dependientes de TIC.

e) Ante cambios normativos, que requieran actualización de medidas, políticas o prácticas institucionales.

### 15.3. Responsables del Seguimiento y Evaluación

- ✓ Área de Sistemas / Gestión Tecnológica: monitorea controles, incidentes, vulnerabilidades y cumplimiento técnico.
- ✓ Líderes de proceso: verifican y reportan cumplimiento de responsabilidades, controles administrativos y medidas operativas.
- ✓ Oficina Asesora de Planeación – Riesgos: articula la actualización del riesgo y consolida la información para análisis institucional.
- ✓ Oficina de Control Interno: evalúa la eficacia de los controles, emite recomendaciones y verifica la implementación de acciones correctivas.
- ✓ Comité Institucional de Gestión y Desempeño (CIGD): aprueba ajustes relevantes al Plan y define prioridades estratégicas, revisa los informes de seguimiento y orienta acciones de mejora.
- ✓ Comité de Riesgos: evalúa riesgos emergentes y prioriza acciones correctivas.

### 15.4. Actualización del Plan

El Plan de Seguridad y Privacidad debe actualizarse cuando:

- ✓ Se identifiquen nuevas amenazas o vulnerabilidades.
- ✓ Se presenten incidentes graves o recurrentes.
- ✓ Se implementen nuevas tecnologías o sistemas de información.
- ✓ Se modifiquen políticas operativas o estratégicas.

- ✓ Se actualicen normativas o estándares aplicables.
- ✓ Se detecten brechas durante auditorías internas o externas.

La actualización debe quedar registrada en el control de cambios institucional.

### 15.5. Gestión de Acciones Correctivas y Preventivas

Como resultado del seguimiento y evaluación, el IFC debe:

- ✓ Definir acciones correctivas para cerrar brechas o mejorar controles.
- ✓ Establecer acciones preventivas para evitar recurrencia de incidentes.
- ✓ Asignar responsables, tiempos y recursos necesarios.
- ✓ Dar seguimiento al cumplimiento de dichas acciones.
- ✓ Documentar evidencias de ejecución.

Estas acciones deben integrarse al Sistema de Administración del Riesgo y a los planes de mejoramiento derivados de auditorías.

### 15.6. Mejora Continua

El proceso de mejora continua del Plan se fundamenta en:

- ✓ Retroalimentación obtenida de incidentes y vulnerabilidades.
- ✓ Recomendaciones del Comité de Riesgos y del Comité de Gestión y Desempeño.
- ✓ Resultados de auditorías internas y externas.
- ✓ Madurez de la gestión de seguridad institucional.
- ✓ Innovaciones tecnológicas o mejores prácticas.
- ✓ Retroalimentación del personal y de los líderes de proceso.

La mejora continua garantiza que el Plan evolucione de acuerdo con la realidad tecnológica, los riesgos emergentes y la estrategia institucional del IFC.

## 16. GESTIÓN DE PROVEEDORES Y TERCEROS EN SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

El Instituto Financiero de Casanare – IFC reconoce que la relación con proveedores, contratistas y terceros implica riesgos inherentes para la seguridad y privacidad de la información institucional. Por esta razón, es fundamental contar con lineamientos claros que garanticen que los servicios, soluciones, infraestructuras y productos tecnológicos externos cumplan con las políticas de seguridad del IFC, protejan los activos de información y prevengan incidentes derivados de accesos indebidos, fallas técnicas, vulnerabilidades o incumplimientos contractuales.

Este capítulo define el marco a través del cual se gestionan los aspectos de seguridad y privacidad en la relación contractual, técnica y operativa con terceros, asegurando un control adecuado del ciclo de vida del servicio prestado.

### 16.1. Principios de Seguridad para la Gestión de Proveedores

La gestión de terceros en el IFC debe seguir los siguientes principios:

1. Responsabilidad compartida: tanto el IFC como el proveedor son responsables de la protección de la información.

2. Cumplimiento normativo: todo proveedor debe cumplir con la normativa vigente en seguridad, protección de datos y gobierno digital.

3. Confidencialidad obligatoria: cualquier tercero con acceso a información debe firmar acuerdos de confidencialidad.

4. Seguridad desde la contratación: los requisitos de seguridad deben estar definidos antes de iniciar la prestación del servicio.

5. Supervisión permanente: el IFC debe monitorear la prestación del servicio y los controles aplicados por el proveedor.

6. Trazabilidad: todo acceso, interacción o intervención del proveedor debe quedar registrado y documentado.

7. No delegación de responsabilidad: aunque un tercero ejecute actividades, la responsabilidad institucional sigue siendo del IFC.

### 16.2. Evaluación y Selección de Proveedores

Antes de contratar un proveedor con acceso a información o sistemas institucionales, el IFC debe:

- ✓ Evaluar su capacidad técnica, operativa y experiencia.
- ✓ Verificar su cumplimiento en seguridad digital, continuidad y protección de datos.
- ✓ Analizar reportes de antecedentes o incidentes previos (si aplica).
- ✓ Evaluar el riesgo asociado a la prestación del servicio.
- ✓ Confirmar el cumplimiento de requisitos mínimos de seguridad establecidos por la entidad.

En contratos que involucren datos personales, se debe verificar el cumplimiento de la Ley 1581 de 2012 y sus decretos reglamentarios.

### 16.3. Requisitos de Seguridad en los Contratos

Los contratos con proveedores o terceros deben incluir, como mínimo:

- ✓ Obligaciones de confidencialidad y reserva.
- ✓ Requisitos de seguridad de la información definidos por el IFC.
- ✓ Controles mínimos aplicables al servicio o tecnología contratada.
- ✓ Responsabilidades sobre protección de datos personales.
- ✓ Esquemas de acceso restringido y roles autorizados.
- ✓ Tiempos de respuesta ante incidentes o fallas del servicio.
- ✓ Condiciones para la entrega, devolución o destrucción de información.
- ✓ Niveles de servicio (SLA) y penalidades por incumplimiento.
- ✓ Obligación de notificar incidentes de seguridad de manera inmediata.
- ✓ Restricciones frente a subcontratación sin autorización del IFC.

### 16.4. Supervisión y Seguimiento a Proveedores

Durante la ejecución del contrato, el IFC debe realizar acciones de monitoreo orientadas a:

- ✓ Verificar el cumplimiento de los controles de seguridad.
- ✓ Revisar reportes técnicos, informes de soporte y bitácoras del proveedor.
- ✓ Evaluar la continuidad del servicio y la disponibilidad acordada.
- ✓ Supervisar la gestión de incidentes presentados por el tercero.
- ✓ Validar los accesos otorgados a personal del proveedor.
- ✓ Comprobar la actualización, mantenimiento o parches aplicados.

El supervisor del contrato debe garantizar que la seguridad y privacidad sean parte integral del seguimiento contractual.

### 16.5. Acceso de Proveedores a Sistemas y Datos Institucionales

Cuando un proveedor necesite acceder a sistemas o información del IFC, se deben aplicar medidas como:

- ✓ Autorización previa por parte del área responsable.
- ✓ Acceso limitado por tiempo y alcance estrictamente necesario.
- ✓ Registro y trazabilidad de todas las actividades realizadas.
- ✓ Supervisión del personal institucional durante las intervenciones.
- ✓ Uso de cuentas temporales o credenciales controladas.
- ✓ Prohibición del uso de dispositivos personales sin autorización.

Estas medidas buscan minimizar el riesgo de manipulación indebida o acceso no autorizado.

### 16.6. Terceros que Procesan Datos Personales

En caso de terceros que traten datos personales, el IFC debe:

- ✓ Asegurar que el proveedor cumpla con la Ley 1581 de 2012 y su régimen sancionatorio.
- ✓ Exigir acuerdos de tratamiento de datos personales (ENCARGADOS).
- ✓ Supervisar las medidas técnicas y organizativas aplicadas por el proveedor.
- ✓ Garantizar que la información solo se use para los fines autorizados.
- ✓ Establecer mecanismos seguros de transferencia y almacenamiento.
- ✓ Verificar la eliminación o devolución segura de datos al finalizar el contrato.

### 16.7. Gestión de Incidentes Reportados por Proveedores

Cuando un proveedor presente un incidente de seguridad que afecte al IFC, este debe:

- ✓ Reportarlo inmediatamente a la entidad.
- ✓ Proporcionar información clara sobre la causa y el alcance.
- ✓ Implementar medidas de contención y corrección.
- ✓ Colaborar con el análisis interno del IFC.
- ✓ Proveer evidencias y documentación de soporte.
- ✓ Garantizar que no se repita la situación.

El incidente se integrará al proceso institucional de gestión de incidentes.

### 16.8. Finalización del Contrato y Disposición de la Información

Al terminar la relación contractual, el proveedor debe:

- ✓ Entregar toda la documentación, información o credenciales en su poder.
- ✓ Eliminar de manera segura cualquier copia o respaldo que tenga del IFC.
- ✓ Entregar certificación de eliminación segura (cuando aplique).

- ✓ Ceder o desactivar accesos y cuentas temporales asignadas.
- ✓ Garantizar la devolución de equipos o elementos institucionales.

Este proceso debe quedar documentado como evidencia institucional.

### 16.9. Evidencias y Registros del Proceso

La gestión de proveedores debe generar:

- ✓ Evaluaciones previas del proveedor.
- ✓ Contratos y actas de inicio, seguimiento y cierre.
- ✓ Registros de acceso otorgado a terceros.
- ✓ Bitácoras de soporte técnico.
- ✓ Informes de incidentes gestionados por el proveedor.
- ✓ Documentos de cierre o eliminación segura de información.
- ✓ Certificaciones de cumplimiento contractual.

### 16.10. Mejora Continua

La gestión de terceros debe actualizarse y fortalecerse considerando:

- ✓ Recomendaciones de auditorías internas o externas.
- ✓ Incidentes asociados a proveedores.
- ✓ Cambios normativos o contractuales.
- ✓ Evaluaciones del desempeño del proveedor.
- ✓ Riesgos emergentes o nuevas dependencias tecnológicas.
- ✓ Actualizaciones del Plan de Seguridad y Privacidad.

## CONTROL DE CAMBIOS

| Versión | Fecha [dd/mm/yy] | Elaborado por | Razón de la actualización |
|---|---|---|---|
| 1.0 | 30/01/2026 | CARLOS ANDRÉS RUBIO BEJARANO Profesional de apoyo CTO. 52 de 2026 - SAF | Elaboración del PSPI, para para la vigencia 2026, teniendo en cuenta las versiones de los planes realizados en 2015, 2019, 2022 y 2023 |