TRD_120_72

INSTITUTO FINANCIERO DE CASANARE

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

SUBGERENCIA ADMINISTRATIVA Y FINANCIERA

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

TABLA DE CONTENIDO

1. INTRODUCCIÓN

El Instituto Financiero de Casanare - “IFC”, es una Institución vinculada a la Secretarla de Desarrollo Económico, Agricultura, Ganadería y Medio Ambiente de Casanare; encargada de adelantar programas de fomento de actividades agropecuarias, industriales, de comercialización, servicios e inversion social; con el objeto de impulsar el desarrollo sostenible de la región y el mejoramiento de la calidad de vida de sus habitantes.

Conscientes de la creciente exposición a riesgos operativos, tecnológicos, normativos y cibernéticos, el IFC formula el presente Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información como un instrumento estratégico que orienta la gestión adecuada de los riesgos que puedan afectar la confidencialidad, integridad, disponibilidad y trazabilidad de la información institucional.

Este plan se desarrolla en concordancia con los lineamientos definidos por el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), particularmente la Política de Seguridad y Privacidad de la Información, la Política de Gobierno Digital y sus disposiciones asociadas, así como con los estándares del Departamento Administrativo de la Función Pública (DAFP) en el marco del Modelo Integrado de Planeación y Gestión (MIPG), especialmente en lo relacionado con la gestión del riesgo, el fortalecimiento institucional y el Sistema de Control Interno.

Asimismo, se articula con la normativa vigente en materia de protección de datos personales (Ley 1581 de 2012 y su reglamentación), acceso a la información pública (Ley 1712 de 2014), gestión documental (Ley 594 de 2000), delitos informáticos (Ley 1273 de 2009), habeas data financiero (Ley 1266 de 2008), y con buenas prácticas y referentes internacionales tales como ISO/IEC 27001, ISO/IEC 27005, ISO/IEC 27701, NIST y OWASP, en la medida en que resulten aplicables al contexto institucional.

En este sentido, el presente Plan constituye un instrumento de gestión que contribuye al fortalecimiento progresivo de las capacidades institucionales en materia de seguridad y privacidad de la información, sirviendo como base para la implementación, consolidación y mejora continua de controles, responsabilidades y acciones orientadas al tratamiento de los riesgos identificados, en articulación con la planeación institucional, el Modelo de Gobierno Digital y el Sistema de Control Interno del IFC.

2. OBJETIVO

Establecer las acciones estratégicas, técnicas, operativas, administrativas y normativas requeridas para garantizar el tratamiento adecuado de los riesgos de seguridad y privacidad de la información del Instituto Financiero de Casanare – IFC, en cumplimiento de los lineamientos del MinTIC, el DAFP, la Secretaría de Transparencia de la Presidencia, el Modelo Integrado de Planeación y Gestión (MIPG) y los estándares internacionales aplicables.

2.2. Objetivos específicos

1. Definir y documentar las estrategias de tratamiento aplicables a los riesgos identificados en materia de seguridad y privacidad de la información.

2. Establecer controles y acciones que permitan reducir la probabilidad y el impacto de los riesgos priorizados.

3. Asignar responsabilidades claras para la implementación, seguimiento y verificación de las acciones del plan.

4. Garantizar la alineación del plan con el MIPG, el Modelo de Gobierno Digital, el Sistema de Control Interno y demás instrumentos de planeación institucional.

5. Contribuir al cumplimiento de las obligaciones legales relacionadas con la protección de datos personales, transparencia, seguridad digital y gestión documental.

3. ALCANCE

El presente plan aplica a:

1. Todos los activos de información del IFC, incluyendo activos físicos, digitales, aplicaciones, bases de datos, servicios en la nube y documentación institucional.

2. Todos los procesos misionales, estratégicos, de apoyo y de evaluación del IFC, así como los sistemas de información que los soportan.

3. Todo el personal del IFC: servidores públicos, contratistas, proveedores y terceros que tengan acceso o administren información institucional.

4. Todas las actividades relacionadas con la captura, almacenamiento, uso, transmisión, preservación, consulta y disposición final de información, sin importar su formato o medio.

5. El tratamiento de datos personales en calidad de responsable o encargado, conforme a la Ley 1581 de 2012 y demás normativa vigente.

4. DEFINICIONES

A continuación, se presentan las definiciones necesarias para la correcta interpretación del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información del Instituto Financiero de Casanare – IFC:

Activo de Información: Recurso que tiene valor para la institución y que requiere protección. Puede ser físico, digital, documental, humano, tecnológico o de servicios.

Amenaza: Evento o situación con potencial de causar daño a un activo de información, afectando su confidencialidad, integridad o disponibilidad.

Vulnerabilidad: Debilidad o falla en procesos, tecnologías, controles o comportamientos humanos que puede ser explotada por una amenaza.

Riesgo de Seguridad de la Información: Posibilidad de que una amenaza aproveche una vulnerabilidad, generando un impacto negativo sobre la información o los servicios institucionales.

Riesgo de Privacidad: Posible afectación a los derechos y libertades de los titulares de datos personales debido al tratamiento inadecuado de su información.

Tratamiento de Riesgos: Proceso de seleccionar e implementar medidas para modificar el riesgo, ya sea mitigándolo, evitándolo, transfiriéndolo o aceptándolo.

Riesgo Residual: Nivel de riesgo que permanece después de considerar la efectividad de los controles existentes, antes de implementar nuevas acciones de tratamiento.

Datos Personales: Cualquier información que pueda asociarse o identificar a una persona natural. Incluye datos sensibles, semiprivados, públicos y privados.

Seguridad de la Información: Conjunto de medidas destinadas a proteger la confidencialidad, integridad, disponibilidad y trazabilidad de los activos de información.

Confidencialidad: Propiedad que garantiza que la información solo sea accesible por personas autorizadas.

Integridad: Propiedad que asegura que la información se mantiene completa, exacta y sin alteraciones no autorizadas.

Disponibilidad: Condición que garantiza que la información esté accesible y utilizable cuando se requiera por quienes tienen autorización.

Trazabilidad: Capacidad para reconstruir el historial, uso o ubicación de un activo de información.

Incidente de Seguridad de la Información: Evento que compromete o puede comprometer la seguridad de la información, la privacidad o la operación institucional.

Control: Medida implementada para gestionar un riesgo, reducirlo o prevenir que se materialice.

Proveedor Crítico: Tercero que proporciona servicios esenciales para la operación del IFC y que tiene acceso a información institucional o infraestructura tecnológica.

SGSI – Sistema de Gestión de Seguridad de la Información: Marco de políticas, procedimientos y controles adoptados para proteger la información institucional, basada en ISO/IEC 27001.

SGPI – Sistema de Gestión de Privacidad de la Información: Conjunto de lineamientos y controles que garantizan el cumplimiento de la normativa de protección de datos personales, alineado con ISO/IEC 27701.

5. NORMATIVIDAD / REQUISITOS

El presente Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información del Instituto Financiero de Casanare – IFC se fundamenta en el marco normativo colombiano y en estándares internacionales aplicables a la gestión del riesgo, la seguridad digital, la protección de datos personales y la transparencia institucional. A continuación, se relacionan las normas, lineamientos y requisitos que orientan su elaboración y aplicación:

5.1. Normatividad Nacional

Protección de Datos Personales

- Ley 1581 de 2012 – Régimen general de protección de datos personales.
- Decreto 1377 de 2013 – Reglamenta la Ley 1581 de 2012.
- Circular Única de la SIC – Lineamientos y obligaciones en materia de protección de datos.
- Ley 1266 de 2008 – Habeas data financiero.

Transparencia y Acceso a la Información

- Ley 1712 de 2014 – Ley de Transparencia y del Derecho de Acceso a la Información Pública.
- Decreto 1081 de 2015 – Reglamentación del Sistema de Transparencia y Acceso a la Información.
- Lineamientos de la Secretaría de Transparencia de la Presidencia de la República**.**

Seguridad Digital y Tecnologías de la Información

- Política de Gobierno Digital – MinTIC**.**
- Política de Seguridad y Privacidad de la Información – MinTIC**.**
- Guía de Gestión de Riesgos de Seguridad de la Información**.**
- Guía de Implementación de Seguridad y Privacidad**.**
- Modelo de Seguridad y Privacidad de la Información del Estado (MSPI)**.**

Gestión Documental

- Ley 594 de 2000 – Ley General de Archivos.
- Acuerdos y directrices del AGN sobre gestión documental y archivos electrónicos.

Delitos Informáticos

- Ley 1273 de 2009 – Delitos contra la información y los datos.

Gestión Pública e Institucional

- Modelo Integrado de Planeación y Gestión (MIPG) – Departamento Administrativo de la Función Pública (DAFP).
- Normas de Control Interno – MECI y lineamientos del DAFP.
- Sistema de Gestión de Seguridad de la Información del Estado (SGSI Gobierno).

5.2. Estándares y Buenas Prácticas Internacionales

Seguridad de la Información

- ISO/IEC 27001:2022 – Sistema de Gestión de Seguridad de la Información.
- ISO/IEC 27002:2022 – Controles de seguridad de la información.
- ISO/IEC 27005:2022 – Gestión de riesgos en seguridad de la información.
- ISO/IEC 22301 – Sistemas de gestión de continuidad del negocio

Privacidad y Protección de Datos

- ISO/IEC 27701:2019 – Sistema de Gestión de Privacidad.
- ISO/IEC 29100 – Marco de privacidad.

Ciberseguridad y Riesgos Técnicos

- Lineamientos del NIST Cybersecurity Framework**.**
- Buenas prácticas OWASP para seguridad de aplicaciones.

5.3. Requisitos Institucionales del IFC

El IFC, como entidad pública, debe cumplir con:

- Su Política Institucional de Seguridad de la Información.
- Su Política de Protección de Datos Personales.
- Su Matriz de Riesgos Institucional.
- Los lineamientos del Sistema de Control Interno**.**
- Los principios de transparencia, eficiencia y responsabilidad administrativa.

6. Metodología de Evaluación y Tratamiento de Riesgos

La metodología adoptada por el Instituto Financiero de Casanare (IFC) para la evaluación y tratamiento de riesgos se fundamenta en los lineamientos del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), el Departamento Administrativo de la Función Pública (DAFP), la Secretaría de Transparencia, el Sistema de Gestión de Seguridad de la Información (SGSI), el Sistema de Gestión de Privacidad de la Información (SGPI) y las buenas prácticas establecidas en las normas ISO/IEC 27001, ISO/IEC 27005 e ISO/IEC 27701.

El propósito de esta metodología es identificar los riesgos que puedan afectar la información, los procesos y los activos institucionales; analizar su probabilidad e impacto; establecer niveles de priorización; y definir acciones de tratamiento que permitan mantenerlos dentro de niveles aceptables, conforme al marco normativo y a las necesidades operativas del IFC. Su aplicación contribuye a fortalecer la capacidad institucional para prevenir incidentes, asegurar la protección de los datos personales y garantizar la continuidad de la operación.

El proceso de gestión del riesgo se desarrolla de manera estructurada y sistemática, mediante las siguientes actividades:

- ✓ Identificación de los activos de información, sus propietarios y los procesos que soportan.
- ✓ Identificación de amenazas y vulnerabilidades que puedan comprometer dichos activos.
- ✓ Análisis del riesgo considerando la probabilidad de ocurrencia y el impacto potencial sobre la institución.
- ✓ Valoración del riesgo de acuerdo con los criterios institucionales de aceptabilidad definidos por el IFC.
- ✓ Priorización de los riesgos de acuerdo con su criticidad, impacto operativo o normativo.
- ✓ Definición de acciones de tratamiento orientadas a mitigar, transferir, evitar o aceptar el riesgo.
- ✓ Determinación del riesgo residual resultante de los controles existentes.
- ✓ Seguimiento periódico de la efectividad de las acciones implementadas y ajuste de las mismas cuando sea necesario.

El proceso se ejecuta de manera iterativa, como parte del ciclo de mejora continua institucional, y permite que los riesgos identificados sean revisados, actualizados y reevaluados según los cambios tecnológicos, operativos y normativos que afecten al IFC.

Para ejecutar esta metodología, el IFC utiliza como soporte herramientas institucionales tales como la matriz de riesgos, el inventario de activos de información, los catálogos de amenazas del MinTIC, las recomendaciones del NIST y OWASP, así como políticas y procedimientos internos relacionados con la seguridad, la privacidad, la gestión documental y el control interno. Estas herramientas facilitan la toma de decisiones informadas y aseguran que el proceso de gestión del riesgo se realice de manera sistemática y alineada con los estándares nacionales e internacionales.

La validación y análisis de los riesgos se realiza con la participación del líder de seguridad de la información, del área TIC, de los jefes de proceso y, cuando aplica, de proveedores externos que administran activos o servicios tecnológicos. Esta articulación garantiza que el proceso considere el contexto real de operación y las particularidades de cada dependencia.

Finalmente, la Matriz Programática constituye el instrumento técnico mediante el cual se documentan las acciones de tratamiento, responsables, recursos, indicadores y plazos definidos para cada riesgo priorizado, y sirve como guía operativa para la ejecución y seguimiento del plan.

7. Identificación, Análisis y Valoración del Riesgo

La identificación, análisis y valoración del riesgo constituye una fase esencial dentro del proceso de gestión de riesgos del Instituto Financiero de Casanare (IFC), ya que permite reconocer de manera estructurada los eventos, escenarios y condiciones que pueden afectar la seguridad y privacidad de la información institucional. Este proceso se desarrolla conforme a los lineamientos del MinTIC, el DAFP, la Secretaría de Transparencia, el Modelo Integrado de Planeación y Gestión (MIPG) y los estándares internacionales ISO/IEC 27005 e ISO/IEC 27701.

La identificación de riesgos inicia con el reconocimiento de los activos de información, los procesos institucionales y los actores que intervienen en su manejo. Dichos activos pueden ser físicos, digitales, tecnológicos, documentales o humanos, y cada uno de ellos posee características, niveles de criticidad específicos. Posteriormente, se identifican las amenazas y vulnerabilidades que, al coincidir, pueden generar afectaciones a la confidencialidad, integridad, disponibilidad, trazabilidad de la información.

Entre los insumos utilizados para la identificación y análisis de riesgos se encuentran las matrices institucionales del SGSI y SGPI, el inventario de activos de información, los catálogos de amenazas definidos por el MinTIC, los lineamientos del NIST y OWASP, y los reportes de incidentes presentados por las áreas y proveedores. Estos elementos facilitan la comprensión del contexto real de exposición y permiten obtener una visión objetiva de los riesgos potenciales.
El análisis del riesgo se realiza valorando dos componentes fundamentales:

- ✓ Probabilidad de ocurrencia, entendida como la posibilidad de que una amenaza se materialice aprovechando una vulnerabilidad existente.
- ✓ Impacto, referido a las consecuencias operativas, reputacionales, financieras, normativas o de afectación a los derechos de los titulares de datos personales.

Una vez evaluados estos elementos, se determina el nivel de riesgo mediante la calificación establecida por el IFC, lo que permite ubicar cada riesgo en categorías tales como bajo, medio, alto o extremo. Esta clasificación constituye el insumo principal para la priorización y para la definición de las acciones de tratamiento más adecuadas.

La valoración del riesgo se complementa con la participación del líder de seguridad de la información (o el encargado del área TIC cuando esta función no exista formalmente), el área de sistemas, los líderes de proceso y el Comité Institucional de Gestión y Desempeño (CIGD), quienes validan la pertinencia de la calificación asignada y su coherencia con el entorno institucional.

8. Gestión y Resultados del Tratamiento, Riesgo Residual y Mejora Continua

El tratamiento de riesgos en el Instituto Financiero de Casanare (IFC) comprende la definición e implementación de acciones orientadas a reducir los riesgos priorizados a niveles aceptables, de acuerdo con los criterios institucionales establecidos. A partir del análisis de probabilidad e impacto realizado en la etapa previa, se determinan las medidas técnicas, administrativas, operativas y

organizacionales necesarias para mitigar, evitar, transferir o aceptar los riesgos identificados, considerando la criticidad de los activos, procesos y servicios institucionales relacionados.

Los resultados del análisis y tratamiento permiten establecer las acciones específicas que deben ejecutarse para disminuir el nivel de exposición de la entidad, así como los responsables, recursos y plazos requeridos para su aplicación. Estas decisiones se adoptan de manera articulada entre el área de sistemas, los jefes de proceso, el líder de seguridad de la información (o el encargado del área TIC cuando esta función no exista formalmente) y la Subgerencia Administrativa y Financiera, garantizando que las medidas seleccionadas sean coherentes con la operación institucional, el marco normativo vigente y la naturaleza financiera del IFC.

El riesgo residual corresponde al nivel de riesgo que permanece después de considerar la efectividad de los controles existentes. Su análisis permite determinar si el riesgo se encuentra dentro de los niveles aceptables definidos por la entidad o si es necesario ajustar los controles actuales o implementar nuevas acciones de tratamiento. La valoración del riesgo residual es realizada de manera conjunta por el área de sistemas, los jefes de proceso y el líder de seguridad de la información, mientras que la Subgerencia Administrativa y Financiera consolida este análisis para efectos de seguimiento institucional y toma de decisiones.

La gestión del riesgo requiere un proceso permanente de seguimiento y mejora continua. Por esto, el IFC realiza revisiones periódicas del avance y la efectividad de las acciones de tratamiento definidas, así como del comportamiento del riesgo residual. Este seguimiento permite identificar oportunidades de mejora, actualizar controles, ajustar plazos, fortalecer procedimientos y detectar nuevos riesgos derivados de cambios tecnológicos, normativos u operativos. De igual manera, los incidentes de seguridad que se presenten en la entidad constituyen una fuente importante de retroalimentación, al evidenciar brechas o debilidades que deben considerarse en las actualizaciones del plan.

Adicionalmente, como parte del proceso de mejora continua, el IFC integra acciones de sensibilización y fortalecimiento de la cultura organizacional en seguridad y privacidad de la información. Estas actividades, definidas y desarrolladas en articulación con el Plan de Seguridad y Privacidad de la Información, permiten reforzar las medidas de tratamiento implementadas y reducir la probabilidad de ocurrencia de incidentes derivados del error humano o del uso inadecuado de los sistemas institucionales. La retroalimentación proveniente de estas actividades y de los resultados del análisis del riesgo residual contribuye a la actualización permanente del presente plan.

Los resultados del tratamiento, el nivel de riesgo residual y los hallazgos derivados del seguimiento se consolidan en la Matriz Programática, que constituye el instrumento técnico de gestión mediante el cual se registran las actividades, responsables, recursos, indicadores y fechas de cumplimiento. La actualización permanente de esta matriz asegura que el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información se mantenga alineado con la realidad institucional, contribuya a la mejora continua y garantice la protección de la información administrada por el IFC.

9. Gestión de Incidentes de Seguridad de la Información

La gestión de incidentes de seguridad de la información en el Instituto Financiero de Casanare (IFC) tiene como propósito detectar, analizar, contener y resolver aquellos eventos que puedan comprometer la confidencialidad, integridad, disponibilidad o privacidad de la información. Su adecuada ejecución contribuye a minimizar el impacto operativo, tecnológico, reputacional y normativo sobre la entidad.

El IFC adopta un enfoque basado en los lineamientos de la ISO/IEC 27035 y en la Guía de Gestión de Incidentes de Seguridad Digital del MinTIC, el cual contempla las siguientes fases: identificación, notificación, clasificación, análisis, contención, resolución, recuperación, documentación y retroalimentación. Este ciclo permite asegurar una respuesta oportuna ante eventos que puedan afectar los activos de información.

Los incidentes deberán ser reportados de manera inmediata al área de sistemas a través de los canales institucionales definidos por el IFC, garantizando la trazabilidad, el análisis de causa, la priorización y la asignación de acciones correctivas.

El procedimiento detallado para la atención, análisis, clasificación, escalamiento y cierre de incidentes se encuentra definido en el Plan de Seguridad y Privacidad de la Información del IFC, el cual establece los niveles de severidad, tiempos de respuesta, rutas de atención y responsabilidades operativas. Dicho procedimiento constituye el instrumento técnico que guía la gestión diaria de incidentes y será actualizado de manera periódica según los requisitos institucionales y normativos.

La información derivada de los incidentes de seguridad constituye una entrada fundamental para el proceso de seguimiento y mejora continua, permitiendo fortalecer los controles existentes, evidenciar brechas y ajustar las acciones contenidas en el presente Plan de Tratamiento de Riesgos.

10. Continuidad del Negocio

La continuidad del negocio en el Instituto Financiero de Casanare (IFC) tiene como propósito asegurar la disponibilidad de los procesos críticos, servicios tecnológicos y activos de información ante situaciones que puedan interrumpir la operación normal de la entidad. Este componente es fundamental debido a la naturaleza financiera del IFC, que requiere mantener la integridad, disponibilidad y confiabilidad de los servicios que presta a la ciudadanía y a los diferentes grupos de interés.

El IFC adopta los lineamientos de la norma ISO/IEC 22301 y las directrices del MinTIC para la gestión de continuidad, orientadas a garantizar que la entidad pueda preparar, responder y recuperarse adecuadamente ante incidentes o eventos de disrupción. La continuidad del negocio integra actividades como análisis de impacto (BIA), identificación de procesos críticos, establecimiento de tiempos máximos de recuperación y definición de estrategias que permitan restablecer los servicios esenciales en el menor tiempo posible.

El presente Plan de Tratamiento de Riesgos considera la continuidad del negocio como un elemento transversal para reducir la probabilidad y el impacto de las interrupciones. Las medidas y acciones

identificadas en la matriz programática contribuyen a fortalecer la resiliencia institucional, mejorar la disponibilidad de los sistemas de información y disminuir el riesgo asociado a fallas tecnológicas, indisponibilidad de servicios, pérdida de datos o afectaciones a la infraestructura tecnológica.

El procedimiento específico para la gestión de la continuidad, incluyendo el análisis de impacto, las estrategias de recuperación, los responsables, las capacidades mínimas operativas y los planes detallados de respuesta y restablecimiento, se encuentra definido en el Plan de Contingencia y Continuidad del Negocio del IFC, documento complementario a este plan. Su ejecución y actualización periódica garantizan que la entidad mantenga una adecuada preparación para enfrentar eventos disruptivos y asegurar la prestación continua de los servicios institucionales.

11. Cultura, Sensibilización y Formación

El fortalecimiento de la cultura institucional en materia de seguridad y privacidad de la información es un componente esencial para la reducción del riesgo y la protección de los activos del Instituto Financiero de Casanare (IFC). La adopción de buenas prácticas por parte de funcionarios, contratistas y terceros contribuye de manera significativa a prevenir incidentes, minimizar vulnerabilidades asociadas al factor humano y promover una apropiación responsable del uso de los sistemas y recursos tecnológicos.

El IFC reconoce la importancia de generar procesos continuos de sensibilización que aborden temas como el uso seguro de la información, protección de datos personales, gestión adecuada de contraseñas, identificación de amenazas digitales comunes, reporte oportuno de incidentes y cumplimiento normativo. Estas acciones permiten fortalecer la cultura institucional y mantener una adecuada preparación frente a las amenazas que afectan el entorno tecnológico actual.

Las actividades específicas de capacitación, campañas, talleres, material educativo y mecanismos de divulgación se encuentran definidas en el Plan de Seguridad y Privacidad de la Información, documento complementario a este plan, y se operacionalizan mediante las acciones consignadas en la Matriz Programática del Plan de Tratamiento de Riesgos. En este instrumento se detallan los responsables, periodicidad, recursos y mecanismos de seguimiento relacionados con la sensibilización institucional.

Los resultados de las actividades de cultura y formación alimentan directamente el proceso de mejora continua, permitiendo identificar brechas de conocimiento, ajustar estrategias pedagógicas, reforzar temas críticos y fortalecer el cumplimiento de las políticas y lineamientos de seguridad digital en toda la entidad.

12. Seguimiento y Mejora Continua

El seguimiento y la mejora continua constituyen elementos esenciales para garantizar la efectividad del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información del Instituto Financiero de Casanare (IFC). Estas actividades permiten verificar el cumplimiento de las acciones definidas, evaluar la eficacia de los controles implementados y asegurar la actualización permanente del plan frente a cambios tecnológicos, normativos y operativos.

El seguimiento se realiza mediante la revisión periódica del avance de las actividades registradas en la Matriz Programática, considerando los plazos establecidos, los responsables asignados y la evidencia de ejecución. El área de sistemas, los líderes de proceso y el líder de seguridad de la información (o el encargado de TIC cuando esta función no exista formalmente) consolidan la información correspondiente a los controles operativos y técnicos, así como las incidencias, dificultades o hallazgos que puedan afectar la gestión del riesgo.

La Subgerencia Administrativa y Financiera consolida los resultados del seguimiento y presenta informes periódicos a la Gerencia y al Comité Institucional de Gestión y Desempeño (CIGD), en el marco de sus funciones de articulación y supervisión institucional. Estos informes permiten evaluar la efectividad del plan, verificar el cumplimiento de los controles y determinar la necesidad de ajustes o la incorporación de nuevas medidas de mitigación.

La mejora continua se fundamenta en la revisión constante del comportamiento del riesgo residual, los resultados de auditorías internas y externas, los incidentes de seguridad registrados, los cambios en la infraestructura tecnológica, las actualizaciones normativas y las necesidades operativas de la entidad. Cuando se identifiquen brechas, debilidades o controles insuficientes, se deberán establecer nuevas acciones de tratamiento, reformular responsabilidades, ajustar plazos o fortalecer los procedimientos existentes.

El IFC reconoce que la gestión del riesgo es un proceso dinámico y evolutivo. Por ello, este plan deberá actualizarse de forma periódica o cuando ocurran eventos relevantes que modifiquen sustancialmente la exposición al riesgo, tales como la adopción de nuevas tecnologías, la implementación de nuevos sistemas, cambios regulatorios, incidentes de seguridad significativos o la identificación de amenazas emergentes.

El seguimiento y la mejora continua aseguran que el Plan de Tratamiento de Riesgos mantenga su vigencia, pertinencia y efectividad, contribuyendo a la protección de la información institucional, a la continuidad del negocio y al cumplimiento de las responsabilidades del IFC como entidad financiera pública.

13. Gestión Documental y Cumplimiento Normativo

La gestión documental y el cumplimiento normativo constituyen pilares fundamentales para garantizar la trazabilidad, integridad, disponibilidad y protección de la información administrada por el Instituto Financiero de Casanare (IFC). En el marco del presente Plan de Tratamiento de Riesgos, estos componentes aseguran que la documentación asociada a la gestión del riesgo, la operación tecnológica y el tratamiento de datos personales sea administrada conforme a los estándares institucionales y a la normatividad vigente en Colombia.

El IFC adopta las directrices establecidas por el Archivo General de la Nación (AGN), el Modelo Integrado de Planeación y Gestión (MIPG), la Ley 594 de 2000 (Ley General de Archivos), la Ley 1712 de 2014 (Transparencia y Acceso a la Información Pública), la Ley 1581 de 2012 y su Decreto Reglamentario 1377 de 2013 (Protección de Datos Personales), así como las buenas prácticas derivadas de las normas ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27701 e ISO 15489 de gestión documental.

En cumplimiento de estas obligaciones, el IFC garantiza que todos los registros, informes, evidencias, matrices, actas, análisis y documentos generados en el marco del presente Plan sean administrados mediante instrumentos archivísticos institucionales tales como el Programa de Gestión Documental (PGD), el Cuadro de Clasificación Documental (CCD), la Tabla de Retención Documental (TRD) y el Sistema Integrado de Gestión Documental adoptado por la entidad. La correcta aplicación de estos instrumentos asegura la conservación, consulta, custodia y disposición final de la información, conforme a los plazos y series documentales definidos.

Asimismo, el IFC deberá mantener actualizada la documentación derivada del Sistema de Gestión de Seguridad de la Información (SGSI) y del Sistema de Gestión de Privacidad de la Información (SGPI), incluyendo políticas, procedimientos, instructivos, inventarios de activos, reportes de incidentes, registros de auditoría, análisis de riesgos, evaluaciones de impacto y evidencias de cumplimiento. Esta documentación constituye soporte esencial para la toma de decisiones, auditorías, procesos de inspección, vigilancia y control, y para la demostración de conformidad frente a requerimientos internos y externos.

En materia de tratamiento de datos personales, el IFC garantiza el cumplimiento de los principios de legalidad, finalidad, libertad, transparencia, acceso y circulación restringida, seguridad y confidencialidad, lo cual implica la implementación de medidas documentales adecuadas para el manejo de autorizaciones, políticas de privacidad, cláusulas contractuales, acuerdos de confidencialidad, y registros de incidentes de seguridad que afecten información personal.

El cumplimiento normativo también exige que todos los documentos relacionados con el Plan de Tratamiento de Riesgos —incluida la Matriz Programática, el seguimiento de acciones, las evidencias de controles implementados y los registros de validación— sean almacenados, actualizados y custodiados en los repositorios institucionales autorizados, garantizando su integridad y disponibilidad. Ningún documento relacionado con este Plan podrá ser administrado por fuera de los lineamientos archivísticos oficiales del IFC.

Adicionalmente, la documentación y la gestión del presente Plan se articula con el Plan de Seguridad y Privacidad de la Información del IFC, el cual define procedimientos detallados para la gestión de incidentes, controles técnicos y administrativos, continuidad del negocio, protección de datos personales y lineamientos específicos de cumplimiento. Ambas herramientas se complementan y se actualizan de manera coordinada, en función de los cambios normativos, tecnológicos y operativos que afecten a la entidad.

Finalmente, el IFC promoverá la actualización continua de la documentación asociada y realizará auditorías internas y revisiones periódicas que permitan verificar el cumplimiento normativo, garantizar la vigencia de los procedimientos y fortalecer la gestión documental en el marco del ciclo de mejora continua institucional.

14. Roles y responsabilidades

La gestión de los riesgos de seguridad y privacidad de la información en el Instituto Financiero de Casanare (IFC) es una responsabilidad compartida entre las diferentes áreas institucionales. Cada

actor cumple un rol específico dentro del ciclo de identificación, análisis, tratamiento, seguimiento y mejora continua del riesgo. A continuación, se establecen los roles y responsabilidades que garantizan la implementación eficaz del Plan.

Comité Institucional de Gestión y Desempeño (CIGD):

El CIGD actúa como instancia de articulación y seguimiento institucional dentro del marco del Modelo Integrado de Planeación y Gestión (MIPG). En el contexto del presente Plan, sus responsabilidades son:

- ✓ Aprobar el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información.
- ✓ Asignar los recursos necesarios para la ejecución de las acciones definidas.
- ✓ Garantizar la alineación del Plan con los objetivos institucionales, el MIPG y las directrices de la Política de Gobierno Digital.
- ✓ Tomar decisiones institucionales frente a riesgos críticos o incidentes de alto impacto cuando sea requerido.
- ✓ Realizar seguimiento general a los riesgos priorizados desde la perspectiva de gestión y desempeño.
- ✓ Socializar informes semestrales consolidados de la Subgerencia Administrativa y Financiera sobre el avance del Plan.
- ✓ Aprobar ajustes al Plan cuando se presenten cambios normativos, tecnológicos o de contexto.

El CIGD actúa conforme a sus funciones establecidas en el MIPG y no asume responsabilidades técnicas propias del área de sistemas.

Gestión Tecnológica – Líder y responsable del proceso:

- ✓ Coordinar la ejecución de las acciones de tratamiento asignadas a su dependencia.
- ✓ Supervisar el cumplimiento de los controles operativos y administrativos definidos en el presente Plan.
- ✓ Articular con el área de sistemas la implementación, verificación y seguimiento de los controles y actividades.

- ✓ Evaluar periódicamente el avance del tratamiento de riesgos bajo su gestión y reportarlo al CIGD.
- ✓ Ejecutar las actividades técnicas definidas en la Matriz Programática del Plan.
- ✓ Administrar los controles tecnológicos asociados a la disponibilidad, integridad y confidencialidad de la información.
- ✓ Mantener actualizados el inventario de activos, permisos, respaldos, configuraciones y registros de auditoría.
- ✓ Mantener evidencias documentales de la ejecución de los controles definidos.
- ✓ Realizar revisiones periódicas de accesos, respaldos y eventos relevantes, documentando la trazabilidad correspondiente.
- ✓ Reportar a la Subgerencia los hallazgos, brechas, incidentes y recomendaciones técnicas.
- ✓ Apoyar la gestión y documentación de incidentes de seguridad digital.
- ✓ Asesorar la implementación de los lineamientos de seguridad y privacidad conforme a la normatividad vigente.
- ✓ Coordinar el proceso institucional de gestión del riesgo de seguridad y privacidad.
- ✓ Verificar el cumplimiento de políticas, procedimientos y controles relacionados con la seguridad digital.
- ✓ Validar la actualización periódica del Plan y de la Matriz Programática.

Líderes de Proceso:

- ✓ Identificar riesgos asociados a los activos de información y procesos bajo su responsabilidad.
- ✓ Reportar oportunamente amenazas, vulnerabilidades o incidentes al área de sistemas.
- ✓ Implementar los controles operativos y administrativos asignados en la Matriz Programática.
- ✓ Articular con el área de sistemas la identificación de nuevas amenazas o vulnerabilidades.

- ✓ Garantizar la adopción y cumplimiento de políticas internas de seguridad y privacidad.

Servidores Públicos y Contratistas del IFC:

- ✓ Cumplir las políticas, normas y lineamientos de seguridad y privacidad de la información.
- ✓ Proteger la información institucional en concordancia con las políticas vigentes.
- ✓ Hacer uso adecuado de los activos, credenciales, sistemas y servicios tecnológicos institucionales.
- ✓ Reportar inmediatamente cualquier incidente, irregularidad o sospecha de vulneración de la seguridad.
- ✓ Participar en los espacios de sensibilización y capacitación realizados por el IFC.

15. ANEXO TÉCNICO MATRIZ PROGRAMÁTICA

El anexo contiene la Matriz Programática del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información del Instituto Financiero de Casanare (IFC).

Esta matriz consolida, para cada riesgo identificado, los controles existentes, las brechas detectadas, las acciones de tratamiento definidas, las actividades específicas a desarrollar, los responsables, las evidencias requeridas y el mecanismo de seguimiento correspondiente.

Su finalidad es servir como herramienta operativa para la ejecución, monitoreo y mejora continua del tratamiento de riesgos, garantizando coherencia con la metodología descrita en el documento principal y con los lineamientos establecidos por MinTIC, DAFP, la Secretaría de Transparencia y los estándares internacionales aplicables.

La información contenida en este anexo tiene carácter dinámico y deberá actualizarse de acuerdo con la evolución tecnológica, la aparición de nuevos riesgos, los resultados del seguimiento institucional y las decisiones adoptadas por el Comité de Seguridad y Privacidad de la Información.

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 Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la información, para la vigencia 2026, teniendo en cuenta las versiones de los planes realizadas en 2018, 2022 y 2023