PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION 2026

CONTROL DE GESTION DOCUMENTAL		
Elaboró: SP. Ing. Juan José Tafur Especialista Seguridad Informática	Revisó: EP. Iván Dario Mora Páez Coordinador TICS	Aprobó: Cr. Ernesto Mejía Araque Director Instituto de Casas Fiscales del Ejército

1. INTRODUCCIÓN

En el marco de la transformación digital del Estado y del fortalecimiento de la gestión pública, la información se ha consolidado como uno de los activos más críticos para el Instituto de Casas Fiscales del Ejército (ICFE). Su adecuado manejo, protección y disponibilidad resultan fundamentales para el cumplimiento de la misión institucional, la ejecución eficiente de las políticas públicas y la prestación transparente de los servicios a la ciudadanía.

El crecimiento del uso de tecnologías de la información, la interconexión de sistemas y el incremento de amenazas de origen tecnológico han ampliado el panorama de riesgos que afectan la seguridad y la privacidad de la información institucional. En este contexto, la protección de la información, tanto en medios digitales como en soportes físicos, debe garantizarse a lo largo de todo su ciclo de vida, asegurando los principios de confidencialidad, integridad, disponibilidad y trazabilidad.

El Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información – Vigencia 2026 constituye un instrumento fundamental del Sistema de Gestión de la Seguridad de la Información (SGSI) y del Sistema de Gestión de Continuidad del Negocio (SGCN) del ICFE. Su propósito es definir y aplicar de manera sistemática los controles preventivos, detectivos y correctivos necesarios para mitigar los riesgos que afectan los activos de información, en coherencia con el contexto organizacional, normativo y operativo del Instituto.

Este Plan adopta un enfoque integral y basado en riesgos, alineado con la Norma ISO/IEC 27001:2022, los lineamientos del Modelo de Seguridad y Privacidad de la Información (MSPI) y las buenas prácticas de continuidad del negocio. De manera prioritaria, orienta sus acciones a la protección de los activos de información clasificados con nivel ALTO, conforme a los criterios de Confidencialidad, Integridad y Disponibilidad (CID), asegurando que la información institucional continúe siendo un recurso confiable para la toma de decisiones estratégicas y la operación del Instituto.

Asimismo, el Plan atiende la actualización del Modelo de Seguridad y Privacidad de la Información (MSPI) adoptada por el Ministerio de Tecnologías de la Información y las Comunicaciones mediante la Resolución 2277 de 2025, la cual establece la necesidad de que las entidades públicas adopten una gestión de la seguridad de la información y la continuidad operativa más transversal, articulada y con mayor nivel de madurez. En este marco, la vigencia 2026 consolida los avances alcanzados con el Plan de Implementación del MSPI y del Sistema de Gestión de Continuidad del Negocio (SGCN) desarrollados durante la vigencia 2025, fortaleciendo las capacidades institucionales para prevenir, detectar y responder de manera oportuna y eficaz a los incidentes de seguridad de la información.

De esta manera, el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información 2026 se establece como una herramienta estratégica para reducir la exposición a riesgos, asegurar la continuidad operativa y tecnológica del ICFE, cumplir con los requisitos normativos vigentes y preservar la confianza institucional en la gestión de la información pública.

2. OBJETIVOS

2.1. OBJETIVO GENERAL.

Establecer y aplicar acciones claras y organizadas para identificar, reducir y controlar los riesgos que puedan afectar la seguridad y la privacidad de la información del Instituto de Casas Fiscales del Ejército (ICFE), garantizando que esta se mantenga protegida, disponible y confiable en todo momento, y asegurando la continuidad de los servicios y el cumplimiento de las normas vigentes, incluso ante posibles incidentes o interrupciones.

2.2. OBJETIVOS ESPECIFICOS.

- Identificar los riesgos que afectan la información del ICFE, reconociendo las amenazas y debilidades que puedan poner en peligro los datos, los sistemas y los documentos, tanto en medios digitales como físicos.
- Evaluar el nivel de riesgo de los activos de información, para priorizar aquellos que son más críticos para el cumplimiento de la misión institucional y la prestación de los servicios.
- Definir e implementar medidas de seguridad adecuadas, que permitan prevenir incidentes, detectar fallas o ataques a tiempo y corregir oportunamente las situaciones que puedan afectar la información.
- Proteger la confidencialidad, integridad y disponibilidad de la información, asegurando que solo las personas autorizadas accedan a los datos, que la información no sea alterada de forma indebida y que esté disponible cuando se necesite.
- Fortalecer la capacidad de respuesta ante incidentes de seguridad de la información, garantizando la continuidad de los procesos y servicios del Instituto frente a eventos que puedan generar interrupciones o afectaciones.
- Asegurar el cumplimiento de la normativa vigente, alineando el tratamiento de riesgos con la Norma ISO/IEC 27001:2022, el Modelo de Seguridad y Privacidad de la Información (MSPI) y demás lineamientos aplicables.

- Promover la mejora continua en la gestión de la seguridad de la información, mediante el seguimiento, monitoreo y ajuste periódico de las medidas adoptadas, de acuerdo con los cambios tecnológicos, normativos y organizacionales del Instituto.

3. ALCANCE

El Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información del Instituto de Casas Fiscales del Ejército (ICFE) inicia con la identificación y el análisis de los riesgos que pueden afectar la seguridad, la privacidad y la disponibilidad de la información institucional, y finaliza con la definición, implementación, seguimiento y mejora de las acciones de tratamiento necesarias para reducir dichos riesgos a niveles aceptables, asegurando la continuidad de los servicios y procesos del Instituto.

Este Plan aplica a todos los procesos, dependencias y niveles del ICFE, de acuerdo con su modelo de operación por procesos, e involucra a los activos de información en cualquiera de sus formas, ya sean digitales, físicos o verbales, así como a los sistemas de información, la infraestructura tecnológica, los servicios, el personal y los terceros que tengan relación con la gestión de la información institucional.

El alcance del Plan comprende la gestión integral de los riesgos asociados a la Seguridad y Privacidad de la Información, la Seguridad Digital y la Continuidad de la Operación de los servicios, incluyendo los riesgos derivados de interrupciones tecnológicas, fallas operativas, incidentes de seguridad, amenazas internas o externas y eventos que puedan afectar el cumplimiento de los objetivos institucionales.

El Plan establece los lineamientos necesarios para identificar, analizar, evaluar, tratar, monitorear y revisar los riesgos de seguridad y privacidad de la información, integrando buenas prácticas que apoyen la toma de decisiones y contribuyan a la prevención de incidentes que puedan comprometer la confidencialidad, integridad, disponibilidad y trazabilidad de la información del Instituto.

Para la vigencia 2026, el Plan de Tratamiento de Riesgos prioriza la atención de aquellos riesgos clasificados en niveles Moderado, Alto y Extremo, conforme a los criterios y metodologías definidos por el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC). Los riesgos identificados en niveles inferiores podrán ser aceptados por el Instituto, siempre que se encuentren debidamente documentados y aprobados por las instancias correspondientes.

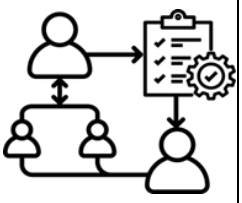
Finalmente, este Plan se encuentra alineado con lo dispuesto en el Decreto 612 de 2018, la Política de Gobierno Digital, el Modelo de Seguridad y Privacidad de la Información (MSPI), la Norma NTC/IEC ISO 27001:2022 y la Estrategia de Seguridad Digital del Estado colombiano, constituyéndose en un instrumento transversal que fortalece la gestión institucional, la continuidad operativa y la confianza en el manejo de la información pública del Instituto.

4. RESPONSABLES

Tabla 1. Roles y Responsabilidades para la Implementación del Plan de Tratamiento Riesgos Seguridad y Privacidad de la Información

Responsable	Rol	Funciones
 **Dirección General**	Actúa como la la máxima autoridad responsable de liderar, respaldar y garantizar la implementación efectiva del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información – Vigencia 2026. Su rol es estratégico y transversal, ya que asegura que la seguridad y la privacidad de la información sean asumidas como una responsabilidad institucional y no únicamente técnica. La Dirección General proporciona la orientación, el apoyo y la toma de decisiones necesarias para que las acciones definidas en el Plan se ejecuten de manera oportuna, coordinada y alineada con los objetivos misionales del Instituto, garantizando la continuidad de los servicios y el cumplimiento de la normativa vigente..	• Aprobar formalmente el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información para la vigencia 2026, asegurando su adopción institucional y su cumplimiento por parte de todos los procesos y dependencias del ICFE. • Promover una cultura organizacional orientada a la protección de la información, impulsando el compromiso de los líderes de proceso y del personal del Instituto en la gestión de los riesgos de seguridad y privacidad de la información. • Garantizar la disponibilidad de los recursos humanos, técnicos y financieros requeridos para la implementación de los controles y acciones definidos en el Plan, de acuerdo con las prioridades institucionales y los niveles de riesgo identificados. • Designar y ratificar las responsabilidades de los líderes de proceso como dueños de los riesgos, exigiendo el cumplimiento de los planes de tratamiento, la implementación de los controles y el reporte oportuno de avances y resultados. • Revisar periódicamente los informes de seguimiento y los indicadores de cumplimiento del Plan, con el fin de evaluar su avance, identificar desviaciones y ordenar las acciones correctivas o de mejora que sean necesarias. • Respaldar las decisiones estratégicas requeridas para la atención de incidentes de seguridad de la información, asegurando una respuesta oportuna que minimice impactos operativos, legales y reputacionales para el ICFE. • Asegurar que las acciones del Plan estén articuladas con el Sistema de Gestión de Continuidad del Negocio (SGCN), de manera

Responsable	Rol	Funciones
		que el Instituto pueda mantener la prestación de sus servicios ante posibles incidentes o interrupciones. • Garantizar que la implementación del Plan se realice en concordancia con la normativa vigente, incluyendo la Norma ISO/IEC 27001:2022, el Modelo de Seguridad y Privacidad de la Información (MSPI), la Política de Gobierno Digital y demás disposiciones aplicables. • Impulsar la revisión y actualización permanente del Plan de Tratamiento de Riesgos, teniendo en cuenta los cambios tecnológicos, organizacionales y normativos, así como los resultados del seguimiento y la materialización de riesgos.
 **Comité Institucional de Gestión y Desempeño**	Actúa como la instancia estratégica de orientación, articulación y seguimiento para la implementación del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información – Vigencia 2026. Su rol principal es garantizar que las acciones definidas en el Plan se integren de manera transversal en los procesos del Instituto y contribuyan al cumplimiento de los objetivos institucionales. El Comité asegura que la gestión de los riesgos de seguridad y privacidad de la información sea coherente con el Modelo Integrado de Planeación y Gestión (MIPG), el Modelo de Seguridad y Privacidad de la Información (MSPI), el Sistema de Gestión de la Seguridad de la Información (SGSI) y el Sistema de Gestión de Continuidad del Negocio (SGCN), promoviendo una gestión ordenada, responsable y sostenible.	• Conocer, revisar y respaldar las directrices, lineamientos y acciones estratégicas del Plan de Tratamiento de Riesgos, asegurando su alineación con la planeación institucional y los modelos de gestión adoptados por el ICFE. • Garantizar que los líderes de proceso integren el Plan de Tratamiento de Riesgos dentro de sus actividades operativas, facilitando la coordinación entre dependencias y evitando duplicidades o vacíos en la gestión del riesgo. • Revisar periódicamente los informes de seguimiento, indicadores de cumplimiento y reportes de avance presentados por Gestión Integral y el Oficial de Seguridad de la Información, con el fin de evaluar el estado de implementación del Plan. • Analizar los riesgos de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación de los Servicios clasificados en niveles Moderado, Alto o Extremo, y recomendar decisiones estratégicas para su tratamiento o mitigación. • Recomendar a la Alta Dirección la asignación de recursos humanos, técnicos y financieros necesarios para la implementación efectiva

Responsable	Rol	Funciones
		de los controles y planes de tratamiento, de acuerdo con las prioridades institucionales. • Impulsar acciones de sensibilización y apropiación institucional que fomenten buenas prácticas en el manejo de la información, la seguridad digital y la prevención de incidentes, involucrando a todos los servidores y colaboradores del ICFE. • Conocer y analizar los incidentes de seguridad de la información de mayor impacto, verificando que se hayan aplicado las acciones correctivas y preventivas necesarias para evitar su repetición. • Asegurar la implementación del Plan se realice conforme a la normativa vigente, incluyendo la Norma ISO/IEC 27001:2022, el MSPI, la Política de Gobierno Digital y las disposiciones aplicables al sector defensa. • Promover la revisión y actualización periódica del Plan de Tratamiento de Riesgos, teniendo en cuenta los resultados del seguimiento, los cambios en el contexto institucional, los avances tecnológicos y las nuevas exigencias normativas.
Asesoría en Gestión Integral 	Cumple un rol articulador, orientador y de seguimiento en la implementación del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información – Vigencia 2026. Su función principal es asegurar que las acciones definidas para reducir los riesgos relacionados con la información se ejecuten de manera ordenada, coherente y alineada con los sistemas de gestión institucionales del ICFE. También actúa como el enlace entre la planeación estratégica, los procesos institucionales y el control del riesgo, facilitando que las decisiones y acciones relacionadas con la seguridad y privacidad de la información se	• Acompañar a los líderes de proceso en la ejecución de las actividades definidas en el Plan de Tratamiento de Riesgos, asegurando que cada acción tenga responsables claros, plazos definidos y resultados verificables. • Asesorar a los procesos del ICFE en la aplicación de la metodología institucional para la gestión de riesgos de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación de los Servicios, facilitando su correcta comprensión y aplicación. • Verificar periódicamente el avance en la implementación de los controles y acciones de tratamiento, de acuerdo con la periodicidad establecida, validando el cumplimiento de actividades y la existencia de evidencias que demuestren su ejecución.

Responsable	Rol	Funciones
	integren efectivamente al quehacer diario del Instituto.	• Recopilar los reportes de avance presentados por los líderes de proceso, revisar su consistencia y analizar los resultados obtenidos, con el fin de identificar retrasos, desviaciones o dificultades en la ejecución del Plan. • Calcular y reportar los indicadores definidos para evaluar el nivel de implementación de los controles y planes de tratamiento de los riesgos de Seguridad y Privacidad de la Información, proporcionando información clara para la toma de decisiones. • Presentar al Comité Institucional de Gestión y Desempeño y a la Alta Dirección informes periódicos sobre el estado de implementación del Plan, destacando avances, riesgos críticos, alertas y recomendaciones de mejora. • Coordinar, junto con los procesos responsables, la definición y seguimiento de acciones correctivas cuando se identifiquen incumplimientos o debilidades en los controles implementados. • Asegurar que el Plan de Tratamiento de Riesgos se encuentre alineado con el Modelo Integrado de Planeación y Gestión (MIPG), el Modelo de Seguridad y Privacidad de la Información (MSPI) y demás sistemas de gestión adoptados por el ICFE. • Impulsar la revisión y actualización del Plan de Tratamiento de Riesgos con base en los resultados del seguimiento, los cambios en el contexto institucional, la materialización de riesgos o incidentes y las lecciones aprendidas. • Fomentar una cultura institucional orientada al uso responsable de la información, la prevención de incidentes y el cumplimiento de las políticas de seguridad y privacidad.
	Cumple un rol técnico, operativo y de soporte en la implementación del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información – Vigencia 2026. Su responsabilidad	• Ejecutar las acciones técnicas establecidas en los planes de tratamiento de riesgos, tales como controles de acceso, respaldos de información, protección de redes, actualización de sistemas, gestión de

Responsable	Rol	Funciones
Grupo Gestión de Información y TIC 	principal es poner en práctica las medidas tecnológicas y operativas necesarias para proteger la información del ICFE y asegurar que los sistemas, aplicaciones y servicios tecnológicos funcionen de manera segura, continua y confiable. También actúa como el custodio de la infraestructura tecnológica y de varios de los activos de información, siendo clave para prevenir incidentes, responder ante fallas o ataques y apoyar la continuidad de los servicios institucionales.	usuarios y demás medidas de seguridad tecnológica. • Garantizar la seguridad de servidores, redes, equipos, bases de datos, aplicaciones y servicios digitales del ICFE, aplicando buenas prácticas que reduzcan la posibilidad de accesos no autorizados, pérdidas de información o interrupciones del servicio. • Implementar y mantener mecanismos que aseguren la disponibilidad de los sistemas de información, como planes de respaldo, recuperación ante desastres y procedimientos de contingencia, minimizando el impacto de posibles interrupciones. • Acompañar a los líderes de proceso en la identificación de riesgos asociados a la tecnología y a la información, aportando conocimiento técnico sobre amenazas, vulnerabilidades, impactos y posibles medidas de control. • Realizar seguimiento continuo al funcionamiento y la seguridad de los sistemas y servicios tecnológicos, detectando eventos anómalos, fallas o incidentes que puedan convertirse en riesgos para la información. • Atender y dar respuesta oportuna a incidentes de seguridad y privacidad de la información, de acuerdo con los procedimientos institucionales, apoyando el análisis de causas y la implementación de acciones correctivas. • Asegurar que los sistemas, aplicaciones y dispositivos cuenten con actualizaciones, parches de seguridad y configuraciones adecuadas, reduciendo vulnerabilidades técnicas que puedan ser explotadas. • Documentar y conservar los soportes que demuestran la ejecución de los controles tecnológicos, tales como registros de respaldos, bitácoras de accesos, reportes de monitoreo y evidencias de mantenimiento, para efectos de seguimiento y auditoría.

Responsable	Rol	Funciones
		• Proporcionar información y evidencias a la Asesoría en Gestión Integral para la medición de indicadores y la evaluación del nivel de implementación de los controles definidos en el Plan. • Orientar a los usuarios del ICFE en el uso seguro de los sistemas de información y herramientas tecnológicas, contribuyendo a la prevención de errores humanos que puedan afectar la seguridad y privacidad de la información.
Responsable de Seguridad de las Operaciones 	Cumple un rol estratégico y operativo en la implementación del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información – Vigencia 2026. Su función principal es asegurar que las operaciones diarias del Instituto se desarrollen de forma segura, protegiendo la información y los servicios críticos frente a riesgos que puedan afectar su continuidad, confiabilidad y correcto funcionamiento. Este rol actúa como un enlace entre la gestión de riesgos, la operación institucional y la continuidad del servicio, garantizando que las medidas de seguridad definidas en el Plan se integren de manera práctica en las actividades cotidianas del ICFE.	• Velar porque las actividades operativas del ICFE se realicen siguiendo los lineamientos de seguridad de la información, privacidad y seguridad digital definidos en el Plan, minimizando riesgos durante la ejecución de los procesos. • Asegurar la aplicación de los controles operativos establecidos en los planes de tratamiento de riesgos, tales como procedimientos seguros, controles físicos, validaciones operativas y medidas de protección durante la prestación de los servicios. • Coordinar y verificar la correcta ejecución de los planes de continuidad y contingencia relacionados con la operación, asegurando que el ICFE pueda mantener o restablecer sus servicios ante interrupciones o incidentes. • Detectar situaciones operativas que puedan generar riesgos para la seguridad y privacidad de la información, informarlas oportunamente y apoyar su análisis y tratamiento junto con los líderes de proceso y el Oficial de Seguridad de la Información. • Colaborar en la atención, análisis y gestión de incidentes de seguridad de la información que impacten la operación, asegurando una respuesta oportuna que reduzca afectaciones a los servicios y usuarios. • Realizar seguimiento al cumplimiento de los procedimientos operativos relacionados con la seguridad de la información, identificando

Responsable	Rol	Funciones
		desviaciones y promoviendo acciones correctivas cuando sea necesario. • Documentar y validar los registros que demuestren la correcta ejecución de los controles operativos, tales como listas de verificación, reportes de actividades, bitácoras y actas, que sirven como soporte para el seguimiento del Plan. • Trabajar de manera articulada con el Grupo de Gestión de la Información y TIC, la Asesoría en Gestión Integral y los líderes de proceso, para asegurar que las medidas de seguridad operativa estén alineadas con los controles técnicos y administrativos. • Suministrar información sobre el estado de los controles operativos y los planes de tratamiento, contribuyendo a la medición de indicadores y a la evaluación del nivel de implementación del Plan de Tratamiento de Riesgos. • Fomentar entre los equipos operativos prácticas seguras en el manejo de la información y en la prestación de los servicios, ayudando a prevenir errores humanos que puedan derivar en incidentes de seguridad.
 **Responsable de Seguridad de la Información**	Su rol principal es dirigir, coordinar y supervisar todas las acciones orientadas a proteger la información del ICFE, asegurando que esta se mantenga segura, confiable y disponible, incluso ante posibles incidentes o interrupciones. Este rol garantiza que la información institucional, tanto digital como física, esté protegida durante todo su ciclo de vida y que el Instituto cumpla con las normas vigentes, como el Modelo de Seguridad y Privacidad de la Información (MSPI) y la Norma ISO/IEC 27001:2022.	• Dirigir la ejecución del Plan de Tratamiento de Riesgos 2026, asegurando que las acciones definidas se implementen de manera organizada, oportuna y alineada con los objetivos institucionales del ICFE. • Orientar y acompañar a los líderes de proceso en la identificación, análisis, valoración y tratamiento de los riesgos que puedan afectar la seguridad y la privacidad de la información institucional. • Establecer, junto con las áreas responsables, los controles preventivos, detectivos y correctivos necesarios para reducir los riesgos, verificando que estos sean adecuados, proporcionales y efectivos. • Velar porque el Plan y su implementación cumplan con la normativa vigente, incluyendo la Resolución 2277 de 2025, el

Responsable	Rol	Funciones
		MSPI, la ISO/IEC 27001:2022 y demás disposiciones aplicables al ICFE. • Garantizar que los activos de información clasificados con niveles de riesgo moderado, alto o extremo cuenten con medidas de protección acordes a su importancia, especialmente aquellos críticos para la operación del Instituto. • Coordinar acciones con los responsables del Sistema de Gestión de Continuidad del Negocio (SGCN) para asegurar que los riesgos de seguridad de la información estén integrados en los planes de continuidad y recuperación. • Liderar la atención de incidentes de seguridad de la información, asegurando su reporte oportuno, análisis de causas, aplicación de acciones correctivas y actualización del mapa de riesgos cuando sea necesario. • Supervisar el avance y cumplimiento de los planes de tratamiento, revisando evidencias, resultados de controles e indicadores, y promoviendo acciones de mejora cuando se identifiquen desviaciones. • Impulsar buenas prácticas en el manejo de la información mediante actividades de sensibilización y orientación, buscando que todos los servidores y contratistas comprendan su responsabilidad en la protección de la información. • Presentar informes claros y periódicos sobre el estado de los riesgos, los incidentes ocurridos y el nivel de implementación del Plan, facilitando la toma de decisiones estratégicas. • Evaluar de forma permanente la eficacia de los controles implementados y proponer ajustes al Plan de Tratamiento de Riesgos, fortaleciendo progresivamente la madurez de la seguridad de la información en el ICFE.
	Actores clave y directamente responsables de la correcta implementación del Plan de	• Reconocer y mantener actualizados los activos de información que se utilizan o generan en su área (documentos, bases de

Responsable	Rol	Funciones
Responsables de áreas o dependencias, y Dueños de procesos. 	Tratamiento de Riesgos de Seguridad y Privacidad de la Información dentro de sus procesos y áreas de trabajo. Su rol principal es identificar, gestionar y controlar los riesgos que puedan afectar la información bajo su responsabilidad, asegurando que las actividades diarias se desarrollen de forma segura, que la información se use correctamente y que los servicios del ICFE continúen operando sin interrupciones. Estos responsables convierten los lineamientos del Plan en acciones prácticas, aplicadas en cada proceso y en el trabajo cotidiano del Instituto.	datos, sistemas, archivos físicos), identificando su importancia y nivel de riesgo. • Detectar las situaciones que pueden afectar la seguridad y privacidad de la información (pérdida, daño, uso indebido, divulgación no autorizada o indisponibilidad), considerando amenazas y debilidades propias del proceso. • Apoyar la evaluación de la probabilidad y el impacto de los riesgos identificados, aportando conocimiento del proceso y de la operación diaria para determinar el nivel real del riesgo. • Diseñar, implementar y cumplir las acciones definidas en los planes de tratamiento de riesgos, aplicando los controles necesarios para reducir los riesgos a niveles aceptables. • Gestionar y justificar los recursos humanos, técnicos y presupuestales necesarios para ejecutar los controles y actividades del plan de tratamiento dentro de su área. • Verificar que los controles definidos (procedimientos, validaciones, restricciones de acceso, respaldos, controles físicos, entre otros) se apliquen correctamente y de forma continua. • Realizar el seguimiento periódico al cumplimiento de los controles y planes de tratamiento, reportando avances, dificultades y resultados a las instancias correspondientes. • Mantener los registros y soportes que demuestren la ejecución de los controles (formatos, informes, actas, listas de verificación, registros de actividades), los cuales son necesarios para el seguimiento y auditoría del Plan. • Informar de manera inmediata cualquier incidente o situación anómala que afecte o pueda afectar la seguridad de la información, siguiendo los procedimientos institucionales establecidos. • Implementar acciones correctivas cuando se presenten incidentes, fallas en los controles o cambios en el proceso, ajustando los

Responsable	Rol	Funciones
		planes de tratamiento y el mapa de riesgos cuando sea necesario. • Sensibilizar y orientar a los funcionarios y contratistas de su área sobre el manejo seguro de la información, fomentando hábitos responsables y preventivos. • Asegurar que los procesos a su cargo cuenten con medidas que permitan continuar o restablecer la operación ante interrupciones, en coordinación con los planes de continuidad del ICFE.
 **Personal del Instituto (Funcionarios, Contratistas y Proveedores)**	El personal del ICFE, incluyendo funcionarios, contratistas y proveedores, cumple un rol fundamental y transversal en la implementación del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información. Su responsabilidad principal es proteger la información del Instituto en el desarrollo de sus actividades diarias, aplicando las normas, procedimientos y buenas prácticas de seguridad establecidas. Cada persona que maneja información del ICFE es corresponsable de su seguridad, ya que una acción inadecuada, un descuido o el incumplimiento de las normas pueden generar incidentes que afecten la operación, la confidencialidad de la información y la confianza institucional.	• Conocer, respetar y aplicar las políticas, lineamientos y procedimientos de seguridad y privacidad de la información establecida por el ICFE en el marco del Plan de Tratamiento de Riesgos. • Manejar la información institucional únicamente para fines laborales autorizados, evitando su uso indebido, divulgación no autorizada o acceso a información que no corresponda a sus funciones. • Cuidar los equipos, sistemas, documentos, archivos físicos y digitales, contraseñas y accesos asignados, evitando su pérdida, daño o uso por personas no autorizadas. • Seguir prácticas básicas de seguridad, como el uso adecuado de contraseñas, el bloqueo de equipos cuando no se usan, la verificación de correos sospechosos y el uso seguro de dispositivos y redes. • Actuar de manera preventiva, identificando situaciones de riesgo y evitando acciones que puedan comprometer la seguridad de la información, como compartir credenciales o descargar software no autorizado. • Informar de forma inmediata cualquier incidente, pérdida de información, acceso no autorizado, correo sospechoso o situación que pueda afectar la seguridad y privacidad de la información, siguiendo los canales definidos por el ICFE. • Asistir y participar en las jornadas de capacitación y sensibilización en seguridad

Responsable	Rol	Funciones
		de la información, con el fin de fortalecer su conocimiento y reducir errores involuntarios. • En el caso de contratistas y proveedores, respetar las cláusulas de confidencialidad y seguridad de la información establecida en los contratos y acuerdos firmados con el ICFE. • Seguir los procedimientos definidos para actuar ante incidentes o interrupciones, contribuyendo a la continuidad de la operación y a la recuperación oportuna de los servicios. • Aplicar las medidas de seguridad cuando se trabaje de forma remota o fuera de las instalaciones del Instituto, garantizando el uso seguro de dispositivos, conexiones y documentos. • Mantener la reserva de la información a la que se tenga acceso, incluso después de finalizar la relación laboral o contractual con el ICFE.

Fuente: Desarrollo propio de Gestión Integral según el "Documento Maestro de Los Lineamientos del Modelo de Seguridad y Privacidad de la Información" del Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC y lo establecido en la Norma ISO 27001:2022.

5. DEFINICIONES

- **AUTORIZACIÓN:** Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales (Ley 1581 de 2012, art 3)
- **BASES DE DATOS PERSONALES:** Conjunto organizado de datos personales que sea objeto de Tratamiento (Ley 1581 de 2012, art 3)
- **CAPACIDAD DE RIESGO:** Es el máximo valor del nivel de riesgo que una Entidad puede soportar y a partir del cual se considera por la Alta Dirección y el Órgano de Gobierno que no sería posible el logro de los objetivos de la Entidad.
- **CIBERSEGURIDAD:** Protección de activos de información, mediante el tratamiento de las amenazas que ponen en riesgo la información que se procesa, almacena y transporta mediante los sistemas de información que se encuentran interconectados en el ciberespacio.
- **CIBERESPACIO:** Es el ambiente tanto físico como virtual compuesto por computadores en la gran red (Internet), sistemas computacionales, programas computacionales (software), redes de telecomunicaciones, datos e información que es

utilizado para la interacción entre usuarios. (Resolución CRC 2258 de 2009).

- **CONFIDENCIALIDAD:** Propiedad de la información de no estar disponible o ser revelada a individuos, entidades o procesos no autorizados.
- **CONTROL:** Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.
- **DATOS ABIERTOS:** Son todos aquellos datos primarios o sin procesar, que se encuentran en formatos estándar e interoperables que facilitan su acceso y reutilización, los cuales están bajo la custodia de las Entidades públicas o privadas que cumplen con funciones públicas y que son puestos a disposición de cualquier ciudadano, de forma libre y sin restricciones, con el fin de que terceros puedan reutilizarlos y crear servicios derivados de los mismos (Ley 1712 de 2014, art 6)
- **DATOS PERSONALES:** Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables. (Ley 1581 de 2012, art 3).
- **DATOS PERSONALES PÚBLICOS:** Es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva. (Decreto 1377 de 2013, art 3).
- **DATOS PERSONALES PRIVADOS:** Es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular. (Ley 1581 de 2012, art 3 literal h)
- **DATOS PERSONALES MIXTOS:** Para efectos de este documento es la información que contiene datos personales públicos junto con datos privados o sensibles.
- **DATOS PERSONALES SENSIBLES:** Se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual, y los datos biométricos. (Decreto 1377 de 2013, art 3).
- **DISPONIBILIDAD:** Propiedad de la información de estar accesible y utilizable cuando lo requiera un individuo, entidad o proceso a través de los canales adecuados siguiendo los procedimientos establecidos.
- **ENCARGADO DEL TRATAMIENTO DE DATOS:** Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el Tratamiento de datos personales por cuenta del responsable del Tratamiento. (Ley 1581 de 2012, art 3).

- **EVENTO:** Ocurrencia o cambio de un conjunto particular de circunstancias: Un evento puede tener más de una ocurrencia y puede tener varias causas y varias consecuencias. Un evento también puede ser algo previsto que no llega a ocurrir, o algo no previsto que ocurre. Un evento puede ser una fuente de riesgo.
- **FUENTE DE RIESGO:** Elemento que, por sí solo o en combinación con otros, tiene el potencial de generar riesgo.
- **FACTORES DE RIESGO:** Son las fuentes generadoras de riesgos.
- **GESTIÓN DEL RIESGO:** Actividades definidas para dirigir y controlar una organización con respecto al riesgo.
- **GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN:** Procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información. (ISO/IEC 27000).
- **INFORMACIÓN PÚBLICA CLASIFICADA:** Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6).
- **INFORMACIÓN PÚBLICA RESERVADA:** Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6)
- **INTEGRIDAD:** Cualidad de la información para ser correcta y no haber sido modificada, manteniendo sus datos exactamente tal cual fueron generados, sin manipulaciones ni alteraciones por parte de terceros.
- **IMPACTO:** Las consecuencias que puede ocasionar a la organización la materialización del riesgo.
- **LEY DE HABEAS DATA:** Se refiere a la Ley Estatutaria 1266 de 2008.
- **MECANISMOS DE PROTECCIÓN DE DATOS PERSONALES:** Lo constituyen las distintas alternativas con que cuentan las Entidades destinatarias para ofrecer protección a los datos personales de los titulares tales como acceso controlado, anonimización o cifrado.
- **NIVEL DE RIESGO:** Es el valor que se determina a partir de combinar la probabilidad de ocurrencia de un evento potencialmente dañino y la magnitud del impacto que este evento traería sobre la capacidad institucional de alcanzar los objetivos. En general la fórmula del Nivel del Riesgo poder ser: Probabilidad * Impacto, sin embargo, pueden relacionarse las variables a través de otras maneras diferentes a la multiplicación, por ejemplo, mediante una matriz de Probabilidad – Impacto.
- **PLAN DE CONTINUIDAD DEL NEGOCIO:** Plan orientado a permitir la continuación de las principales funciones misionales o del negocio en el caso de un evento imprevisto

que las ponga en peligro. (ISO/IEC 27000).

- **PLAN DE TRATAMIENTO DE RIESGOS:** Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma. (ISO/IEC 27000).
- **REGISTRO NACIONAL DE BASES DE DATOS:** Directorio público de las bases de datos sujetas a Tratamiento que operan en el país. (Ley 1581 de 2012, art 25)
- **RESPONSABLE DEL TRATAMIENTO DE DATOS:** Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el Tratamiento de los datos. (Ley 1581 de 2012, art. 3).
- **RIESGO:** Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000).
- **RIESGO DE SEGURIDAD DE LA INFORMACIÓN:** Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000)
- **RIESGO DE CORRUPCIÓN:** Posibilidad de que, por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado
- **SEGURIDAD DE LA INFORMACIÓN:** Preservación de la confidencialidad, integridad, y disponibilidad de la información en cualquier medio: impreso o digital. (ISO/IEC 27000).
- **SEGURIDAD DIGITAL:** Preservación de la confidencialidad, integridad, y disponibilidad de la información que se encuentra en medios digitales.
- **TITULARES DE LA INFORMACIÓN:** Personas naturales cuyos datos personales sean objeto de Tratamiento. (Ley 1581 de 2012, art 3)
- **TOLERANCIA DEL RIESGO:** Es el valor de la máxima desviación admisible del nivel de riesgo con respecto al valor del Apetito de riesgo determinado por la entidad.
- **TRATAMIENTO DE DATOS PERSONALES:** Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión. (Ley 1581 de 2012, art 3).
- **TRAZABILIDAD:** Cualidad que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sean asociadas de modo inequívoco a un individuo o Entidad. (ISO/IEC 27000).
- **VULNERABILIDAD:** Debilidad de un activo o control que puede ser explotada por una o más amenazas. (ISO/IEC 27000).
- **PARTES INTERESADAS (STAKEHOLDER):** Persona u organización que puede afectar a, ser afectada por o percibirse a sí misma como afectada por una decisión o actividad.
- **RIESGO INHERENTE:** Es aquel al que se enfrenta una entidad en ausencia de acciones de la dirección para modificar su probabilidad o impacto.

- **RIESGO RESIDUAL:** Nivel de riesgo que permanece luego de tomar medidas de tratamiento del riesgo. Es aquel que subsiste, después de haber implementado controles.

6. NORMATIVIDAD

- **Ley 1581 de 2012.** "*Por la cual se dictan disposiciones generales para la protección de datos personales*".
- **Ley 1712 de 2014.** "*Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones*".
- **Decreto 886 de 2014**. "*Por el cual se reglamenta el artículo 25 de la Ley 1581 de 2012, relativo al Registro Nacional de Bases de Datos*".
- **Decreto 2573 de 2014**. "*Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en línea, se reglamenta parcialmente la Ley 1341 de 2009 y se dictan otras disposiciones*".
- **Decreto 103 de 2015**. "*Por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones*.".
- **Decreto 1078 de 2015**. "*Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones*".
- **Decreto 1081 de 2015**. "*Por medio del cual se expide el Decreto Reglamentario Único del Sector Presidencia de la República".*
- **CONPES 3854-2016 de 2016**. "Política Nacional de Seguridad digital".
- **Decreto 1083 de 2015 Sector de Función Pública**. "Decreto Único Reglamentario del Sector de Función Pública".
- **Decreto 648 de 2017.** "*Por el cual se modifica y adiciona el Decreto 1083 de 2015, Reglamentario Único del Sector de la Función Pública*".
- **Decreto 1499 de 2017.** "*Por medio del cual se modifica el Decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública, en lo relacionado con el Sistema de Gestión establecido en el artículo 133 de la Ley 1753 de 2015*".
- **Decreto 612 de 2018. "**Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado", donde se encuentra el presente Plan Estratégico de Seguridad de la Información (PESI) como uno de los requisitos a desarrollar para cumplir con esta normativa.
- **Decreto 1008 de 2018.** "*Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones*".
- **CONPES 3701-2011 de 2018.** "Lineamientos de política para ciberseguridad y ciberdefensa".
- **Resolución 500 del 2021.** "*Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad*

como habilitador de la política de Gobierno Digital".

- **Decreto 338 del 2022.** "*Por el cual se adiciona el Título 21 a la Parte 2 del Libro 2 del Decreto Único 1078 del 2015, Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, con el fin de establecer los lineamientos generales para fortalecer la gobernanza de la seguridad digital, se crea el Modelo y las instancias de Gobernanza de Seguridad Digital y se dictan otras disposiciones*".
- **Resolución 7870 del 2022 (Ministerio de Defensa Nacional). "***Por el cual se emite y se adopta la Política General de Seguridad y Privacidad de la Información, Seguridad Digital, Ciberseguridad y Continuidad de los Servicios Tecnológicos en las Unidades Ejecutoras o Dependencias del Ministerio de Defensa Nacional, Policía Nacional, y entidades adscritas y vinculadas al Sector Defensa".*
- **Resolución 2277 del 2025.** *"Por la cual se actualiza el Anexo 1 de la Resolución 500 de 2021 y se derogan otras disposiciones relacionadas con la materia"*
- **NORMA ISO 55000**. "Esta Norma Internacional provee los aspectos generales de la gestión de activos, sus principios y terminología y los beneficios esperados al adoptar la gestión de activos. Esta Norma Internacional puede aplicarse a todo tipo de activos y por cualquier tipo y tamaño de organización".
- **NTC-ISO/IEC COLOMBIANA 20000-1:2011**. "Permite la gestión de servicios de TI de forma metódica a través de la implementación del PHVA (Planear – Hacer – Verificar – Actuar) que ha sido la estructura base y más exitosa de las normas ISO".
- **NTC-ISO/IEC COLOMBIANA 27001-1:2013**. "Proporciona un marco de trabajo para los sistemas de gestión de seguridad de la información (SGSI) con el fin de proporcionar confidencialidad, integridad y disponibilidad continuada de la información, así como cumplimiento legal.".

7. METODOLOGIA

La metodología para el tratamiento de riesgos adoptada por el Instituto de Casas Fiscales del Ejército (ICFE) se fundamenta en los lineamientos establecidos por el Departamento Administrativo de la Función Pública (DAFP) y en el Modelo de Seguridad y Privacidad de la Información (MSPI) definido por el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), los cuales proporcionan un marco metodológico común para la gestión de los riesgos de seguridad digital en las entidades del Estado.

De conformidad con lo dispuesto en el Decreto 1078 de 2015, en relación con la implementación de la estrategia de Gobierno Digital, las entidades públicas están obligadas a adoptar el MSPI con el propósito de establecer y mantener un Sistema de Gestión de la Seguridad de la Información (SGSI) al interior del Instituto, que permita proteger de manera adecuada la información y los servicios digitales que soportan su operación.

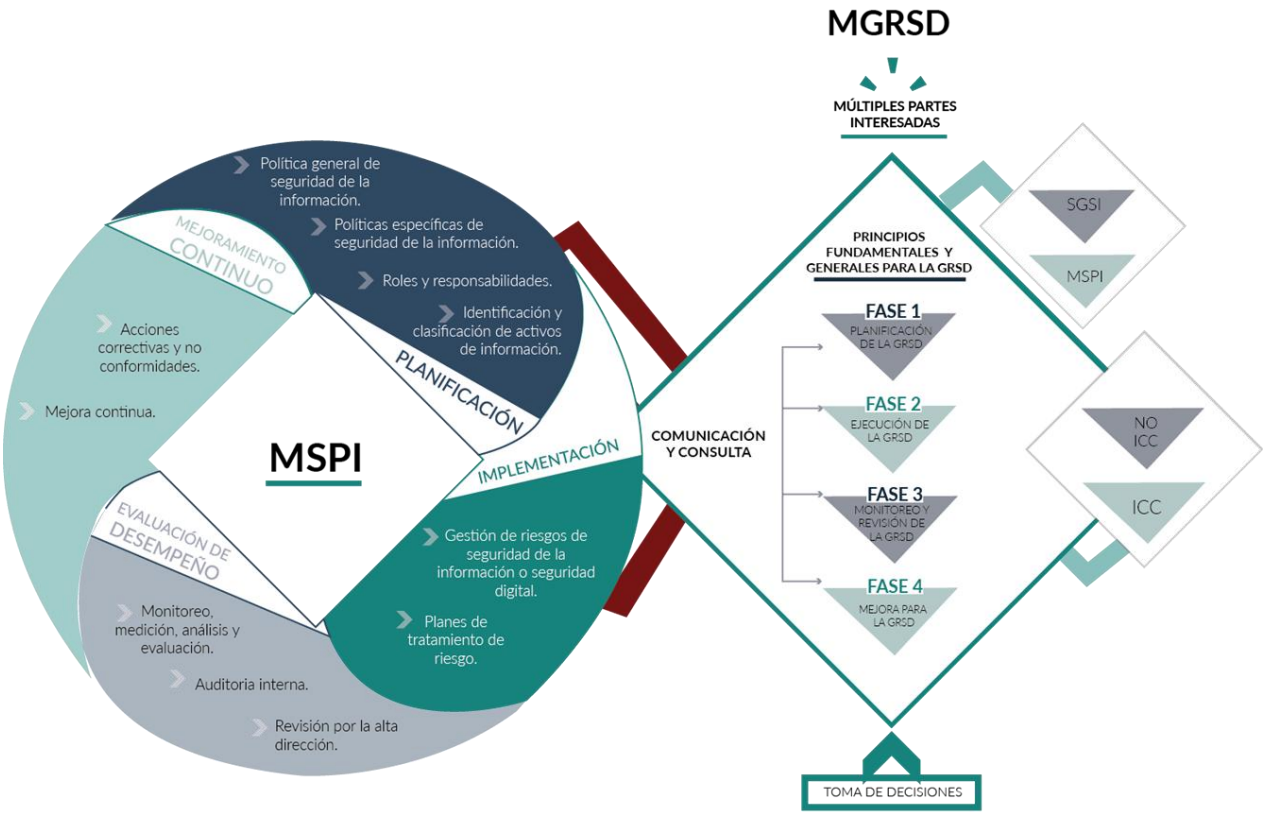
El Modelo de Seguridad y Privacidad de la Información (MSPI) integra de manera transversal un componente de gestión de riesgos, el cual se desarrolla a lo largo de las

etapas de planificación, implementación, evaluación y mejora continua. Este enfoque permite identificar de forma anticipada los riesgos, aplicar controles adecuados y verificar permanentemente la eficacia de las medidas de seguridad implementadas, fortaleciendo así la protección de la información institucional.

Este modelo es aplicable a entidades públicas, privadas y mixtas y, en el caso de las entidades del Estado, constituye un marco de obligatorio cumplimiento para la implementación del Sistema de Gestión de la Seguridad de la Información (SGSI), en concordancia con la normativa vigente y las buenas prácticas internacionales.

En este contexto, la gestión de la seguridad de la información del ICFE se articula con el Modelo Nacional de Gestión de Riesgos de Seguridad Digital (MGRSD), permitiendo una relación e interacción coherente entre la administración de los riesgos institucionales y los riesgos específicos asociados a la seguridad digital. Esta articulación garantiza un enfoque integral, consistente y alineado con las directrices del Gobierno Nacional para la protección de la información y la continuidad de los servicios digitales, tal como se indica a continuación:

Imagen 1. Interacción entre el MSPI y el MGRSD



Fuente: Modelo de gestión del riesgo de seguridad digital de MinTIC.

De acuerdo con el Ciclo de Deming (PHVA), el Instituto de Casas Fiscales del Ejército (ICFE) estructura sus sistemas de gestión a partir de las actividades de Planear (P), Hacer (H), Verificar (V) y Actuar (A), las cuales permiten asegurar una adecuada implementación, control y mejora continua de los procesos institucionales, garantizando resultados eficaces y sostenibles.

En el marco del Modelo de Seguridad y Privacidad de la Información (MSPI), el ICFE desarrolla la gestión de la seguridad de la información principalmente en las etapas de planeación e implementación, en las que se definen los controles, responsabilidades y acciones necesarias para proteger los activos de información que soportan la operación y el cumplimiento de la misión institucional. De manera complementaria, el Modelo Nacional de Gestión de Riesgos de Seguridad Digital (MGRSD) es adoptado por el Instituto para fortalecer la gestión de los riesgos de seguridad digital, incorporando de forma explícita las actividades de monitoreo, revisión y mejora continua.

Es importante resaltar que, en el ICFE, la gestión de los riesgos de seguridad digital no se limita únicamente a la identificación, evaluación y tratamiento de los riesgos, sino que también comprende la implementación, seguimiento y control del Plan de Tratamiento de Riesgos, de acuerdo con los niveles de riesgo definidos por la Entidad. Esto permite que las decisiones adoptadas se traduzcan en acciones concretas y efectivas orientadas a reducir la exposición al riesgo y proteger la información institucional.

Por esta razón, el ICFE articula y sincroniza los conceptos, metodologías y actividades definidos en el MSPI, el Sistema de Gestión de la Seguridad de la Información (SGSI) y el MGRSD, especialmente en sus fases iniciales. Adicionalmente, el Instituto aplica de manera transversal y permanente las fases de comunicación y consulta, así como las de monitoreo y revisión establecidas en el MGRSD, las cuales se encuentran directamente relacionadas con las etapas de evaluación del desempeño y mejora continua del MSPI y del SGSI.

Esta integración fortalece la gestión institucional de la seguridad digital en el ICFE, asegura la coherencia entre los modelos adoptados y promueve una cultura de prevención, resiliencia y mejora continua, orientada a la protección efectiva de la información y a la continuidad de los servicios institucionales.

7.1. DESARROLLO METODOLÓGICO

El desarrollo metodológico establece la forma en que el Instituto de Casas Fiscales del Ejército (ICFE) organiza, aplica y mantiene de manera sistemática la gestión de los riesgos de seguridad y privacidad de la información. Su propósito es brindar un marco claro y ordenado que permita identificar, analizar, tratar y hacer seguimiento a los riesgos que puedan afectar la información institucional y la continuidad de los servicios.

El desarrollo metodológico no se limita a la definición teórica de actividades, sino que orienta su aplicación práctica en los procesos del Instituto, facilitando la toma de decisiones, el cumplimiento normativo y la implementación de acciones efectivas para prevenir incidentes, reducir el impacto de los riesgos y fortalecer la protección de la información institucional.

Imagen 2. Desarrollo metodológico

Fuente: Desarrollo propio de Gestión Integral según la guía de Administración de riesgos de seguridad y privacidad de la información, seguridad digital y continuidad de la operación de los servicios de MinTIC.

Establecimiento del contexto. En el Instituto de Casas Fiscales del Ejército (ICFE), el establecimiento del contexto corresponde al análisis y comprensión de los factores internos, externos y propios de los procesos institucionales que influyen en la gestión de los riesgos de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación de los Servicios (riesgos de interrupción).

Este análisis considera, entre otros aspectos, el entorno organizacional del ICFE, su estructura administrativa, el modelo de operación por procesos, la infraestructura física y tecnológica que soporta la misión institucional, el marco normativo aplicable y las partes interesadas internas y externas. A partir de este contexto, el Instituto puede identificar las posibles causas que originan los riesgos, estableciendo una base clara y consistente que facilita su adecuada identificación, análisis y tratamiento, conforme a las metodologías institucionales vigentes.

Identificación del riesgo. La identificación de los riesgos en el ICFE se orienta a reconocer las situaciones que pueden afectar la seguridad y privacidad de la información, la seguridad digital y la continuidad de la operación de los servicios institucionales. Para ello, se analizan aspectos como la infraestructura física y tecnológica, las áreas de trabajo, el entorno operativo, las condiciones ambientales y los servicios que apoyan el cumplimiento de la misión del Instituto.

Es indispensable que cada proceso del ICFE tenga debidamente identificados sus activos de información, así como las situaciones potenciales que puedan generar afectaciones al logro de los objetivos institucionales. La ausencia de controles adecuados o la baja apropiación de las buenas prácticas de seguridad de la información (vulnerabilidades) puede ser aprovechada por amenazas internas o externas, dando lugar a la materialización de riesgos o incidentes de seguridad.

Durante esta etapa, el ICFE identifica como mínimo los siguientes elementos:

- El atributo de la información afectado: Confidencialidad, Integridad o Disponibilidad.
- El proceso responsable o dueño del riesgo.
- El activo de información afectado.
- Las amenazas y vulnerabilidades asociadas.
- Las posibles consecuencias para la operación, la misión y la imagen institucional del Instituto.

Para lograr una visión integral del riesgo, el ICFE puede apoyarse en datos históricos, análisis técnicos, experiencias previas, conceptos de expertos y las necesidades de las partes interesadas.

Valoración del riesgo. La valoración de los riesgos en el ICFE se realiza de conformidad con la Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas, emitida por el Departamento Administrativo de la Función Pública (DAFP), así como con las tablas de impacto, probabilidad y criterios adoptados institucionalmente.

Este ejercicio se desarrolla mediante mesas de trabajo con los responsables de los procesos, en las cuales se analiza el contexto, se identifican los riesgos y se evalúan la probabilidad de ocurrencia y el impacto, con el fin de determinar el nivel de riesgo inherente. En esta etapa también se identifican las vulnerabilidades existentes y los controles actuales o propuestos para su mitigación.

A cada control se le definen variables que permiten evaluar su adecuado diseño e implementación, tales como: responsable, periodicidad, propósito, forma de ejecución, posibles desviaciones y evidencias de su aplicación. Asimismo, se verifica que los

controles se ejecuten de manera consistente y efectiva, de modo que contribuyan realmente a la reducción del riesgo.

En el caso de los riesgos de interrupción, los controles pueden tener un carácter transversal, especialmente cuando el custodio del activo de información pertenece a un proceso diferente o corresponde a un tercero. En estos casos, los controles y planes de tratamiento se definen de manera conjunta, mientras que el proceso que identifica el riesgo aporta los niveles de probabilidad, impacto y riesgo inherente asociados a la posible indisponibilidad del activo.

Definición y aprobación de mapas de riesgos y planes de tratamiento

Una vez culminadas las etapas de administración de riesgos y obtenida la valoración correspondiente, los líderes de los procesos del ICFE deben aprobar formalmente los mapas de riesgos, mediante memorando. En el mismo acto, se aprueban los planes de tratamiento, los cuales contienen las actividades necesarias para mitigar los riesgos cuyo nivel residual se ubique en las zonas Moderada, Alta o Extrema.

Estos planes establecen responsables, plazos y acciones concretas orientadas a reducir la exposición al riesgo y a fortalecer la seguridad y privacidad de la información institucional.

Materialización del riesgo. En caso de que un riesgo se materialice, este debe ser reportado de manera inmediata conforme al procedimiento de gestión de incidentes de seguridad y privacidad de la información del ICFE. Posteriormente, se realiza el análisis correspondiente para determinar el nuevo nivel del riesgo luego de su materialización y se registran los ajustes necesarios en el mapa de riesgos institucional.

Si se materializa un riesgo que no haya sido previamente identificado, este deberá ser reportado para iniciar su identificación, análisis y registro, garantizando así la mejora continua del proceso de gestión de riesgos y el fortalecimiento de la seguridad de la información en el ICFE.

7.2. ACTIVIDADES DE IMPLEMENTACIÓN 2026

Tabla 2. Actividades del Plan de Tratamiento Riesgos Seguridad y Privacidad de la Información - 2026

Estrategia	Actividades	Evidencia
Plan de Implementación del Modelo de Seguridad y Privacidad de la Información (MSPI) y el Sistema de Gestión de Continuidad del	Implementación de la Política de Gestión de Activos.	Documento publicado, aprobado e implementado.
	Implementación de la Política de Identificación, Clasificación y valoración de Activos de Información.	Documento publicado, aprobado e implementado.

Estrategia	Actividades	Evidencia
Negocio (SGCN) del ICFE	Implementación de la Política de Seguridad Para la Gestión del Riesgo Digital.	Documento publicado, aprobado e implementado.
Revisión/actualización de documentación	Implementar el manual de gestión de riesgos de seguridad digital.	Documento publicado, aprobado e implementado.
	Adoptar plantilla para reporte de riesgos de seguridad	Plantilla en Excel para reporte de riesgos de seguridad.
Concientización sobre conceptos y bases para la identificación de riesgos digitales	Elaborar presentación para charlas	Charlas
	Elaborar pieza gráfica relacionada con tips para identificación de riesgos de seguridad.	Piezas gráficas y correo electrónico con envío masivo.
Identificación de riesgos de seguridad de la información	Identificar, analizar y evaluar los riesgos de seguridad para todos los procesos de la cadena de valor	Matriz de riesgos de seguridad publicada.
	Revisar, validar y ajustar los riesgos.	
Plan de tratamiento de riesgos de seguridad de la información	Documentar las actividades relacionadas para implementar los controles establecidos.	Plantilla en Excel para reporte de riesgos de seguridad.
Aceptación del riesgo de seguridad de la información	Consolidar las aprobaciones de las matrices de riesgos de seguridad por el propietario del riesgo (líder del proceso) como declaración formal de la aceptación	Correo electrónico o memorando.
Seguimiento planes de tratamiento de riesgos de seguridad de la información	Revisar la documentación y evidencias de los seguimientos realizados al plan de tratamiento	Correo electrónico, Actas de sesiones
Mejoramiento	Identificar oportunidades de mejora conforme los resultados de la evaluación del riesgo residual	Correo electrónico, Actas de sesiones

Fuente: Desarrollo propio de Gestión Integral según Plan de Implementación del Modelo de Seguridad y Privacidad de la Información (MSPI) y el Sistema de Gestión de Continuidad del Negocio (SGCN) del ICFE y el "Documento Maestro de Los Lineamientos del Modelo de Seguridad y Privacidad de la Información" del Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC y lo establecido en la Norma ISO 27001:2022.

8. PRESUPUESTO PARA LA IMPLEMENTACIÓN DE CONTROLES

La estimación, asignación y gestión del presupuesto requerido para la ejecución del Plan

de Tratamiento de Riesgos de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación de los Servicios (riesgos de interrupción) identificados en el Instituto de Casas Fiscales del Ejército (ICFE) será responsabilidad del dueño del riesgo, entendido como el líder del proceso correspondiente.

El líder del proceso es responsable de gestionar los recursos necesarios para la implementación de los controles definidos y las acciones establecidas en el plan de tratamiento, así como de realizar el seguimiento y control de su ejecución. Lo anterior incluye la verificación del cumplimiento de las actividades programadas, la adecuada utilización de los recursos asignados y la efectividad de las medidas adoptadas para la mitigación de los riesgos.

Asimismo, la asignación presupuestal deberá realizarse de manera articulada con las áreas competentes del ICFE, garantizando que las necesidades de seguridad de la información y continuidad operativa sean consideradas dentro de la planeación institucional, y que las acciones del plan de tratamiento se ejecuten de forma oportuna y sostenible.

9. MEDICIÓN Y SEGUIMIENTO

El monitoreo y seguimiento de los riesgos de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación de los Servicios (riesgos de interrupción) del Instituto de Casas Fiscales del Ejército (ICFE), así como de los controles y planes de tratamiento aprobados por los líderes de los procesos, es realizado por el área de Gestión Integral, de acuerdo con la periodicidad y los plazos de cumplimiento establecidos.

Este seguimiento incluye la verificación de la ejecución de las actividades definidas, la revisión de los resultados obtenidos y la validación del cargue de los soportes y evidencias que demuestran la correcta aplicación de los controles implementados para la mitigación de los riesgos.

Una vez los líderes de los procesos realizan el reporte de cumplimiento de los planes de tratamiento y de los controles a su cargo, Gestión Integral efectúa la revisión y validación de la información reportada, con el fin de consolidar los resultados y medir el nivel de avance en la gestión del riesgo. Esta información sirve de insumo para la toma de decisiones y la adopción de acciones de mejora cuando se identifiquen desviaciones o incumplimientos.

La medición de la gestión del riesgo se realiza a través de un indicador institucional, cuyo propósito es determinar el porcentaje de implementación y ejecución de los controles definidos para mitigar los riesgos de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación de los Servicios del ICFE. Este indicador permite evaluar de manera objetiva el desempeño de los controles, fortalecer la mejora continua y asegurar la efectividad del Plan de Tratamiento de Riesgos.

Tabla 3. Ficha Técnica del Indicador de Medición y Seguimiento

Elemento	Descripción
Nombre del indicador	Nivel de implementación del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información
Objetivo del indicador	Medir el grado de ejecución e implementación de los controles y acciones definidos en el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información, con el fin de evaluar la efectividad de la gestión del riesgo y apoyar la toma de decisiones en el ICFE.
Proceso responsable	Gestión Integral
Alcance	Aplica a todos los procesos del ICFE que cuenten con riesgos de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación de los Servicios.
Tipo de indicador	Gestión / Cumplimiento
Fórmula	(Número de controles implementados y ejecutados / Número total de controles definidos en el Plan de Tratamiento) × 100
Unidad de medida	Porcentaje (%)
Fuente de información	Mapas de riesgos aprobados, planes de tratamiento, reportes de seguimiento de los líderes de proceso, evidencias de ejecución de controles.
Periodicidad de medición	Trimestral
Meta	≥ 90 % de implementación de los controles definidos en el Plan de Tratamiento de Riesgos
Línea base	Resultado de la medición final de la vigencia 2026
Interpretación del resultado	Un valor alto indica un adecuado nivel de implementación y seguimiento de los controles del Plan de Tratamiento. Un valor bajo evidencia retrasos o incumplimientos que requieren acciones correctivas.
Uso del indicador	Seguimiento al cumplimiento del Plan de Tratamiento, toma de decisiones, priorización de acciones de mejora y reporte a la Alta Dirección.
Frecuencia de reporte	Trimestral y consolidado anual
Responsable del reporte	Gestión Integral
Usuarios del indicador	Alta Dirección, líderes de proceso.
Acciones ante desviaciones	Definición de planes de mejora, ajustes al plan de tratamiento, fortalecimiento de controles y reasignación de responsabilidades o recursos, según corresponda.

Fuente: Desarrollo propio de Gestión Integral según el “Documento Maestro de Los Lineamientos del Modelo de Seguridad y Privacidad de la Información” del Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC y lo establecido en la Norma ISO 27001:2022.

10. REGISTROS Y DOCUMENTOS ASOCIADOS

CÓDIGO	NOMBRE DEL DOCUMENTO

11. REGISTRO DE MODIFICACIONES (espacio exclusivo para calidad)

VERSIÓN	FECHA MODIFICACIÓN	NUMERAL MODIFICADO	NATURALEZA DEL CAMBIO
01	10/10/2023		Creación del documento.
02	28/01/2026	Todos	Ajustes conforme a la actualización realizada por el Ministerio de Tecnologías de la Información y las Comunicaciones mediante la Resolución 2277 del 3 de junio de 2025 al MSPI.