PLAN ESTRATÉGICO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN "PESI" – VIGENCIA 2026.

ELABORÓ	REVISÓ	APROBÓ
NOMBRE: Ing. Deiby Leandro Alvarado Rodríguez.	**NOMBRE:** Ing. Ricardo Valenzuela Díaz.	**NOMBRE:** Abog. Martha Eugenia Cortés Baquero.
CARGO: Profesional Defensa – Seguridad de la Información.	**CARGO:** Líder Proceso Gestión de Tecnologías de la Información y las Comunicaciones.	**CARGO:** Jefe de la Oficina Asesora Jurídica, encargada de la Funciones del Despacho de la Dirección General de la Agencia Logística de las Fuerzas Militares.
FIRMA: 	**FIRMA:** 	**FIRMA Y FECHA DE APROBACIÓN:**  26 01 2026

TABLA DE CONTENIDO

1. GENERALIDADES

La Agencia Logística de las Fuerzas Militares (ALFM) reconoce que la información y los activos digitales que administra son elementos esenciales para el cumplimiento de su misión institucional y la prestación de servicios estratégicos al sector defensa y al Estado colombiano. En un entorno donde las amenazas digitales evolucionan con velocidad, proteger la confidencialidad, integridad y disponibilidad de la información se convierte en un componente crítico para garantizar la continuidad operativa, la seguridad nacional y la confianza de las partes interesadas.

El Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), consciente del crecimiento de los incidentes de seguridad digital y su impacto en la prestación de servicios públicos, ha establecido lineamientos claros para fortalecer la seguridad y privacidad de la información en las entidades del Estado. A través de la Resolución 02277 de 2025, el Ministerio redefine el Modelo de Seguridad y Privacidad de la Información (MSPI), consolidándolo como el marco de referencia para la gestión integral de la seguridad digital bajo un enfoque preventivo, resiliente y basado en riesgos.

En este contexto, la ALFM adopta el MSPI como estructura central de su Sistema de Gestión de Seguridad y Privacidad de la Información – SGSPI. Este modelo se fundamenta en el ciclo PHVA (Planear, Hacer, Verificar y Actuar), e integra requisitos legales, técnicos y normativos que permiten gestionar de manera coherente los riesgos que afectan los sistemas de información, los servicios críticos, la infraestructura tecnológica, la seguridad física, el talento humano, los proveedores, los datos personales y los activos misionales.

El MSPI está compuesto por cinco fases (Diagnóstico, Planificación, Operación, Evaluación del Desempeño y Mejoramiento Continuo), las cuales garantizan que la entidad cuente con un sistema dinámico y adaptable a los cambios tecnológicos, regulatorios y del entorno digital. El análisis de brechas realizado en 2025 constituye el insumo principal para este PESI 2026, al evidenciar el estado actual del SGSPI y orientar la priorización de los controles, acciones y proyectos que permitirán elevar el nivel de madurez institucional.

El Plan Estratégico de Seguridad y Privacidad de la Información – PESI 2026 se convierte así en el instrumento rector que articula los lineamientos del MSPI con los objetivos institucionales de la ALFM. Este plan establece las acciones necesarias para fortalecer las capacidades de prevención, detección, respuesta y recuperación ante incidentes; gestionar adecuadamente los riesgos; mejorar la infraestructura tecnológica; consolidar una cultura organizacional de seguridad; y asegurar que la prestación de servicios continúe sin interrupciones ante eventos que puedan comprometer su disponibilidad.

Este documento está alineado con la Política de Gobierno Digital, el Decreto 612 de 2018, la normativa vigente en materia de seguridad digital y los controles definidos en la norma ISO/IEC 27001:2022, integrando tanto los componentes organizacionales, físicos, tecnológicos y humanos que conforman la seguridad de la información en la entidad.

Finalmente, el PESI 2026 es presentado al Comité Institucional de Gestión y Desempeño para su análisis, aprobación y publicación, garantizando su articulación con los instrumentos de planeación institucional y permitiendo a la ALFM avanzar hacia un modelo de seguridad más maduro, resiliente y alineado a las mejores prácticas nacionales e internacionales.

2. REFERENCIA NORMATIVA

Conforme con lo establecido en la normatividad vigente el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), hace referencia a las siguientes normas, que se deben tener en cuenta para el desarrollo de la apropiación del MSPI en la entidad.

Constitución Política de la República de Colombia.	Aplicación de los artículos 15, 209 y 269.
Ley 594 de 2000 (julio 14).	Por la cual se dicta la Ley General de Archivos y se dictan otras disposiciones.
Ley 599 de 2000 (julio 24).	Código Penal Colombiano.
Ley 1221 de 2008 (julio 16).	Por la cual se establecen normas para promover y regular el Teletrabajo y se dictan otras disposiciones.
Ley 1266 de 2008 (diciembre 31).	Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.
Ley 1273 de 2009 (enero 05).	Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.
CONPES 3701 de 2011 (julio 14).	Lineamientos de política para ciberseguridad y ciberdefensa.
Ley 1581 de 2012 (octubre 17).	Por la cual se dictan disposiciones generales para la protección de datos personales.
Decreto 2364 de 2012 (noviembre 22).	Por medio del cual se reglamenta el artículo 7° de la Ley 527 de 1999, sobre la firma electrónica y se dictan otras disposiciones.
Decreto 2609 de 2012 (diciembre 14).	Por el cual se reglamenta el Título V de la Ley 594 de 2000, parcialmente los artículos 58 y 59 de la Ley 1437 de 2011 y se dictan otras disposiciones en materia de Gestión Documental para todas las entidades del Estado.
Directiva Permanente Ministerio Defensa No. 913 de 2013 (abril 19).	Guías y procedimientos en tecnología de información y comunicaciones para el Sector Defensa.
Decreto 1377 de 2013 (junio 27).	Por el cual se reglamenta parcialmente la Ley 1581 de 2012.

Decreto 886 de 2014 (mayo 13).	Por el cual se reglamenta el Registro Nacional de Bases de Datos.
Ley 1712 de 2014 (marzo 06).	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.
Directiva Permanente Ministerio de Defensa No. 018 de 2014 (junio 19).	Políticas de seguridad de la información para el Sector Defensa.
Decreto 2573 de 2014 (diciembre 12).	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 (enero 20).	Por medio del cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones.
Decreto 1074 de 2015 (mayo 26).	Por medio del cual se expide el Decreto Único Reglamentario del Sector Comercio, Industria y Turismo.
Decreto 1078 de 2015 (mayo 26).	Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.
Decreto 1083 de 2015 (mayo 26).	Por medio del cual se expide el Decreto Único Reglamentario del Sector de Función Pública.
CONPES 3854 de 2016 (abril 11).	Política Nacional de Seguridad digital.
Decreto 728 de 2017 (mayo 05).	Por el cual se adiciona el capítulo 2 al título 9 de la parte 2 del libro 2 del Decreto Único Reglamentario del sector TIC, Decreto 1078 de 2015, para fortalecer el modelo de Gobierno Digital en las entidades del orden nacional del Estado colombiano, a través de la implementación de zonas de acceso público a Internet inalámbrico.
Decreto 1413 de 2017 (agosto 25).	Por el cual se adiciona el título 17 a la parte 2 del libro 2 del Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones, Decreto 1078 de 2015, para reglamentarse parcialmente el capítulo IV del título 111 de la Ley 1437 de 2011 y el artículo 45 de la Ley 1753 de 2015, estableciendo lineamientos generales en el uso y operación de los servicios ciudadanos digitales.
Decreto 1499 de 2017 (septiembre 11).	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.
CONPES 3920 de 2018 (abril 17).	Política nacional de explotación de datos (BIG DATA).
Decreto 1008 del 2018 (junio 14).	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.

Ley 1915 de 2018 (julio 12).	Por la cual se modifica la Ley 23 de 1982 y se establecen otras disposiciones en materia de derecho de autor y derechos conexos.
Decreto 612 de 2018 (abril 04).	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.
Ley 1952 de 2019 (enero 28).	Por medio de la cual se expide el código general disciplinario.
Directiva Presidencial No. 02 de 2019 (abril 02).	Simplificación de la interacción digital entre los ciudadanos y el estado.
CONPES 3975 de 2019 (noviembre 8).	Política Nacional para la Transformación Digital e Inteligencia Artificial.
Decreto 2106 de 2019 (noviembre 22).	Establece que las autoridades que realicen trámites, procesos y procedimientos por medios digitales, deberán disponer de una estrategia de seguridad digital siguiendo los lineamientos que emita el Ministerio de Tecnologías de la Información y las Comunicaciones.
Decreto 620 de 2020 (mayo 2).	Por el cual se subroga el título 17 de la parte 2 del libro 2 del decreto 1078 de 2015, para reglamentarse parcialmente los artículos 53, 54, 60, 61 y 64 de la ley 1437 de 2011, los literales e, j y literal a del parágrafo 2 del artículo 45 de la ley 1753 de 2015, el numeral 3 del artículo 147 de la ley 1955 de 2019, y el artículo 9 del decreto 2106 de 2019, estableciendo los lineamientos generales en el uso y operación de los servicios ciudadanos digitales.
CONPES 3995 de 2020 (julio 01).	Nacional de confianza y seguridad Digital.
Resolución 1519 de 2020 (agosto 24).	Por la cual se definen los estándares y directrices para publicar la información señalada en la ley 1712 del 2014 y se definen los requisitos materia de acceso a la información pública, accesibilidad web, seguridad digital, y datos abiertos.
Ley 2052 de 2020 (agosto 25).	Por medio de la cual se establecen disposiciones transversales a la rama ejecutiva del nivel nacional y territorial y a los particulares que cumplan funciones públicas y/o administrativas, en relación con la racionalización de trámites y se dictan otras disposiciones.
Resolución 500 de 2021 (marzo 10).	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.
Directiva Presidencial No. 03 de 2021 (marzo 15).	Lineamientos para el uso de servicios en la nube, inteligencia artificial, seguridad digital y gestión de datos.
Decreto 377 de 2021 (abril 9).	Por el cual se subroga el título 1 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, para reglamentar el Registro Único de TIC y se dictan otras disposiciones
Decreto 88 de 2022 (enero 24).	Por el cual se adiciona el Titulo 20 a la Parte 2 del Libro 2 del Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, Decreto 1078 de 2015, para reglamentar los artículos 3, 5 y 6 de la Ley 2052 de 2020, estableciendo los conceptos, lineamientos, plazos y condiciones para la digitalización y automatización de trámites y su realización en línea.
Resolución 0463 de 2022 (febrero 09).	Por el cual se define el uso de Tecnologías en la Nube para el Sector Defensa y se dictan otras disposiciones.
Resolución 000460 de 2022 (febrero 15).	Por la cual se expide el plan nacional de infraestructura de datos y su hoja de ruta en el desarrollo de la política de gobierno digital, y se dictan los lineamientos generales para su implementación.
Directiva Presidencial No. 02 de 2022 (febrero 24).	Por medio del cual se efectúa reiteración de la política pública en materia de seguridad digital.
Decreto 338 de 2022 (marzo 8).	Por el cual se adiciona el Titulo 21 a la Parte 2 del Libro 2 del Decreto Único 1078 de 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 000746 de 2022 (marzo 11).	Por el cual se fortalece el modelo de seguridad y privacidad de la información y se definen lineamientos adicionales a los establecidos en la resolución no. 500 de 2021.
Decreto 767 de 2022 (mayo 16).	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.
Decreto 1263 de 2022 (julio 2022).	Por el cual se adiciona el Título 22 a la Parte 2 del Libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, con el fin de definir lineamientos y estándares aplicables a la Transformación Digital Pública.
Resolución 7870 de 2022 (diciembre 26).	Por la cual se emite y 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, y se dictan otras disposiciones.
Norma ISO/IEC	Seguridad de la información, ciberseguridad y protección de la

27001:2022.	privacidad. Sistemas de gestión de la seguridad de la información.
Ley 2294 de 2023 (mayo 19).	Por el cual se expide el plan nacional de desarrollo 2022 – 2026 "Colombia potencia mundial de vida".
Manual integrado de gestión de 2024 (octubre 3).	Manual integrado de gestión, código: GI-MA-02, versión No. 22.
CONPES 4144 de 2025 (febrero 14).	Política Nacional de Inteligencia Artificial.
Resolución 02277 de 2025 (junio 3).	Por la cual se actualiza el Anexo 1 de la Resolución número 500 de 2021 y se derogan otras disposiciones relacionadas con la materia.

3. OBJETIVO DEL PLAN

Fortalecer la seguridad y privacidad de la información en la ALFM mediante la implementación, actualización y maduración del Modelo de Seguridad y Privacidad de la Información (MSPI), asegurando la protección de los activos institucionales, la gestión efectiva de riesgos, la continuidad del negocio y el cumplimiento del marco normativo vigente, para garantizar la confianza en la prestación de los servicios y la resiliencia organizacional frente a amenazas digitales.

3.1. OBJETIVOS ESPECIFICOS

Alinear el Sistema de Gestión de Seguridad y Privacidad de la Información (SGSPI) con los lineamientos de la Resolución 02277 de 2025, la Política de Gobierno Digital y la norma ISO/IEC 27001:2022, garantizando el cumplimiento del marco normativo vigente.

Cerrar las brechas identificadas en el Análisis GAP MSPI 2025 mediante la actualización, implementación y maduración de los controles organizacionales, físicos, tecnológicos y de personas establecidos en los dominios A.5 a A.8.

Fortalecer la gobernanza del SGSPI mediante la definición clara de roles, responsabilidades, competencias y mecanismos de coordinación institucional.

Actualizar y formalizar políticas, lineamientos, procedimientos y documentación del SGSPI, garantizando su adopción y divulgación en toda la entidad.

Robustecer la gestión de riesgos de seguridad y privacidad de la información mediante la actualización de la metodología institucional, el análisis de riesgos 2026, la Declaración de Aplicabilidad (SoA) y el Plan de Tratamiento de Riesgos (PTR).

Incrementar la capacidad institucional de prevención, monitoreo, detección y respuesta a incidentes de seguridad digital, asegurando el registro, análisis y tratamiento oportuno de eventos.

Garantizar la continuidad de los servicios críticos de la ALFM mediante el fortalecimiento del análisis de impacto al negocio (BIA), la actualización del Plan de Continuidad y Recuperación, y la implementación de medidas técnicas y operativas de resiliencia.

Fortalecer la seguridad en la infraestructura tecnológica, los servicios en la nube y la gestión de proveedores, asegurando el cumplimiento de requisitos de seguridad en todo el ciclo de vida de los servicios y contratos.

Promover una cultura institucional de seguridad y privacidad de la información mediante programas de sensibilización, capacitación y concientización dirigidos al personal, terceros y partes interesadas.

Establecer mecanismos de seguimiento, medición y mejora continua del SGSPI mediante indicadores, auditorías, revisión por la dirección y planes de acción que permitan elevar el nivel de madurez institucional.

4. ALCANCE

El Plan Estratégico de Seguridad y Privacidad de la Información (PESI) de la vigencia 2026 aplica a la totalidad de la Agencia Logística de las Fuerzas Militares (ALFM), e incluye todos los procesos estratégicos, misionales y de apoyo desarrollados tanto en la Oficina Principal como en las regionales. Su alcance comprende toda la infraestructura tecnológica institucional, incluyendo servidores, redes, centros de datos, plataformas en la nube (SaaS, PaaS e IaaS), sistemas de información internos y servicios críticos, así como todos los activos de información en formato físico y digital, clasificados como información pública, pública clasificada y pública reservada, en cumplimiento de la misión institucional.

El PESI abarca igualmente a todos los funcionarios, contratistas, proveedores, terceros y usuarios autorizados que gestionan, procesan o acceden a la información institucional y que resultan esenciales para la operación de la ALFM. Asimismo, el plan integra los componentes de seguridad física, lógica, administrativa, de personal, de continuidad del negocio, ciberseguridad y privacidad de datos personales que conforman el Sistema de Gestión de Seguridad y Privacidad de la Información (SGSPI), e incorpora la gestión de riesgos, incidentes, vulnerabilidades, el cumplimiento normativo, el monitoreo, la auditoría y la mejora continua, conforme al Modelo de Seguridad y Privacidad de la Información (MSPI), la Resolución 02277 de 2025, la Política de Gobierno Digital y la norma ISO/IEC 27001:2022.

5. CUERPO DEL PLAN

5.1. ESTADO ACTUAL DE LA ENTIDAD RESPECTO AL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.

La Agencia Logística de las Fuerzas Militares (ALFM), en su condición de entidad pública, reconoce que el entorno digital actual implica un incremento constante de los riesgos e

incidentes de seguridad digital, los cuales pueden afectar la continuidad de sus operaciones, la integridad de la información y la prestación de servicios a sus partes interesadas. En este contexto, la entidad ha venido adoptando y fortaleciendo los lineamientos definidos por el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), orientados a promover el uso y la apropiación segura de las Tecnologías de la Información y las Comunicaciones (TIC), así como a generar confianza en el entorno digital institucional.

En concordancia con la Política de Gobierno Digital, la ALFM reconoce la seguridad y privacidad de la información como un habilitador transversal para el cumplimiento de sus objetivos misionales y estratégicos. Este enfoque implica la implementación progresiva de controles físicos, lógicos y administrativos que permitan proteger los trámites, servicios, sistemas de información, plataformas tecnológicas e infraestructura física y del entorno, gestionando de manera adecuada los activos de información, la infraestructura crítica cibernética, los riesgos y los incidentes de seguridad y privacidad de la información, con el fin de evitar o minimizar la interrupción de la operación institucional.

Teniendo en cuenta lo anterior, y conforme a lo establecido por el MinTIC, la ALFM ha adoptado el Modelo de Seguridad y Privacidad de la Información (MSPI) como marco de referencia para la gestión integral de la seguridad digital. Este modelo tiene como propósito formalizar al interior de la entidad un Sistema de Gestión de Seguridad y Privacidad de la Información (SGSPI), alineado con la norma ISO/IEC 27001:2022 y fundamentado en el ciclo PHVA (Planear, Hacer, Verificar y Actuar), integrando requisitos legales, técnicos, normativos, reglamentarios y operativos aplicables a la entidad.

Como parte del proceso de maduración del SGSPI, durante la vigencia 2025 la ALFM ha venido adelantando el análisis de brechas (GAP) frente a los lineamientos del MSPI, lo cual permitió identificar el estado actual de implementación de los controles, las fortalezas institucionales y las oportunidades de mejora en materia de seguridad y privacidad de la información. Los resultados de este diagnóstico evidencian avances significativos en la adopción del modelo, así como la necesidad de fortalecer y consolidar la gobernanza, la gestión de riesgos, la documentación, la operación de controles y los mecanismos de seguimiento y mejora continua.

En este escenario, el Plan Estratégico de Seguridad y Privacidad de la Información (PESI) 2026 se formula como la hoja de ruta que permitirá a la ALFM cerrar las brechas identificadas, elevar el nivel de madurez del SGSPI y consolidar una estrategia de seguridad y privacidad de la información coherente, sostenible y alineada con los lineamientos del MSPI, la Resolución 02277 de 2025 y las mejores prácticas nacionales e internacionales en seguridad digital.

El Modelo de Seguridad y Privacidad de la Información (MSPI), adoptado por la Agencia Logística de las Fuerzas Militares (ALFM), se estructura en cinco (5) fases que permiten gestionar, implementar y mantener de manera integral la seguridad y privacidad de los activos de información. Estas fases se desarrollan bajo un enfoque de mejora continua, basado en el ciclo PHVA (Planear, Hacer, Verificar y Actuar), y constituyen el marco operativo para la implementación del Sistema de Gestión de Seguridad y Privacidad de la

Información (SGSPI), conforme a los lineamientos establecidos por el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC).

5.1.1. FASE 1. Diagnóstico.

La fase de Diagnóstico corresponde al punto de partida del MSPI y tiene como objetivo identificar el estado actual de la ALFM frente a los requisitos definidos en el modelo, mediante la realización de un análisis de brechas (GAP). Este diagnóstico permite evaluar el nivel de madurez del SGSPI, identificar fortalezas, debilidades y oportunidades de mejora, así como determinar el grado de implementación de los controles organizacionales, físicos, tecnológicos y de personas.

El análisis GAP constituye un insumo fundamental para la fase de planificación, ya que orienta la priorización de acciones, proyectos y recursos. Asimismo, este diagnóstico sirve como línea base para medir los avances alcanzados al finalizar la fase de mejoramiento continuo, permitiendo evidenciar la evolución progresiva del modelo en la entidad.

5.1.2. FASE 2. Planificación.

En la fase de Planificación se establecen las necesidades, objetivos y estrategias de seguridad y privacidad de la información de la ALFM, considerando su mapa de procesos, el tamaño institucional y el análisis del contexto interno y externo. Esta fase incorpora los resultados del diagnóstico, los requerimientos normativos, las expectativas de las partes interesadas y las prioridades estratégicas de la entidad.

Un componente central de esta fase es la identificación, valoración y tratamiento de los riesgos de seguridad y privacidad de la información, lo que permite definir las medidas necesarias para mitigar, transferir, aceptar o evitar los riesgos identificados. Como resultado, se actualizan instrumentos clave como la metodología de gestión de riesgos, la Declaración de Aplicabilidad (SoA), el Plan de Tratamiento de Riesgos (PTR), los objetivos del SGSPI, el cronograma de actividades, los recursos requeridos y los indicadores de desempeño que permitirán realizar el seguimiento al PESI 2026.

5.1.3. FASE 3. Operación.

La fase de Operación corresponde a la implementación efectiva de los controles definidos durante la planificación, con el propósito de reducir la probabilidad y el impacto de los riesgos identificados. En esta etapa se despliegan controles técnicos, administrativos, físicos y de gestión del talento humano, orientados a proteger los activos de información y la infraestructura tecnológica de la ALFM.

Durante esta fase se fortalecen, entre otros aspectos, la gestión de accesos, la protección contra amenazas cibernéticas, la gestión de incidentes de seguridad, la seguridad en la infraestructura tecnológica y en los servicios en la nube, así como la continuidad del negocio. De igual manera, se promueve la cultura de seguridad y privacidad de la información

mediante actividades de sensibilización y capacitación, asegurando que los controles se integren de manera efectiva a los procesos y a la operación institucional.

5.1.4. FASE 4. Evaluación de desempeño.

En la fase de Evaluación del Desempeño se mide la efectividad del MSPI y del SGSPI a través de auditorías internas, revisiones periódicas y el análisis de los indicadores definidos en la planificación. Esta fase permite verificar el nivel de cumplimiento de los objetivos estratégicos, normativos y operativos, así como identificar desviaciones, debilidades o áreas de mejora en la implementación de los controles.

Los resultados obtenidos facilitan la toma de decisiones informadas, el seguimiento al avance del PESI 2026 y la generación de informes de gestión, constituyéndose en un insumo clave para la revisión por la dirección y para la fase de mejoramiento continuo.

5.1.5. FASE 5. Mejoramiento continuo.

La fase de Mejoramiento Continuo tiene como propósito fortalecer de manera progresiva el SGSPI mediante la identificación y corrección de desviaciones, la implementación de acciones correctivas y preventivas, y la actualización permanente de los controles, políticas y procedimientos. En esta etapa se analizan las causas raíz de las no conformidades, incidentes y hallazgos de auditoría, y se adoptan medidas que eviten su recurrencia.

Este enfoque garantiza que el MSPI evolucione de forma dinámica frente a los cambios normativos, tecnológicos y del entorno de riesgos, permitiendo a la ALFM incrementar su nivel de madurez, resiliencia y capacidad de respuesta ante amenazas a la seguridad y privacidad de la información.

A. Estado de avance del modelo.

En la ALFM, las fases del MSPI se han venido implementando de manera continua y progresiva a lo largo de las vigencias, lo que ha permitido fortalecer el SGSPI y avanzar en el cumplimiento de la normatividad vigente. El análisis de brechas realizado durante la vigencia 2025 evidencia avances significativos en la adopción del modelo, así como la identificación de brechas que serán abordadas mediante las acciones definidas en el PESI 2026, con el objetivo de consolidar el modelo y alcanzar mayores niveles de madurez en todas sus fases.

Tabla 1.
Avance ciclo de funcionamiento del modelo de operación (PHVA).

AVANCE PHVA			
COMPONENTE (PHVA)	**CLAUSULAS**	**% de Avance Actual Entidad**	**% Avance Esperado**
Planificación	Contexto de la organización	6%	14%

	Liderazgo	5%	14%
	Planificación	10%	14%
	Soporte	4%	14%
Implementación	Operación	11%	16%
Evaluación de desempeño	Evaluación del desempeño	3%	14%
Mejora continua	Mejora	8%	14%
TOTAL		**47%**	**100%**

Nota. Avance implementación ciclo PHVA – Instrumento de identificación de la línea base de seguridad, autodiagnóstico Modelo de Seguridad y Privacidad de la Información – MSPI, ejecución vigencia (2025).

Tabla 2.
Evaluación de efectividad de controles.

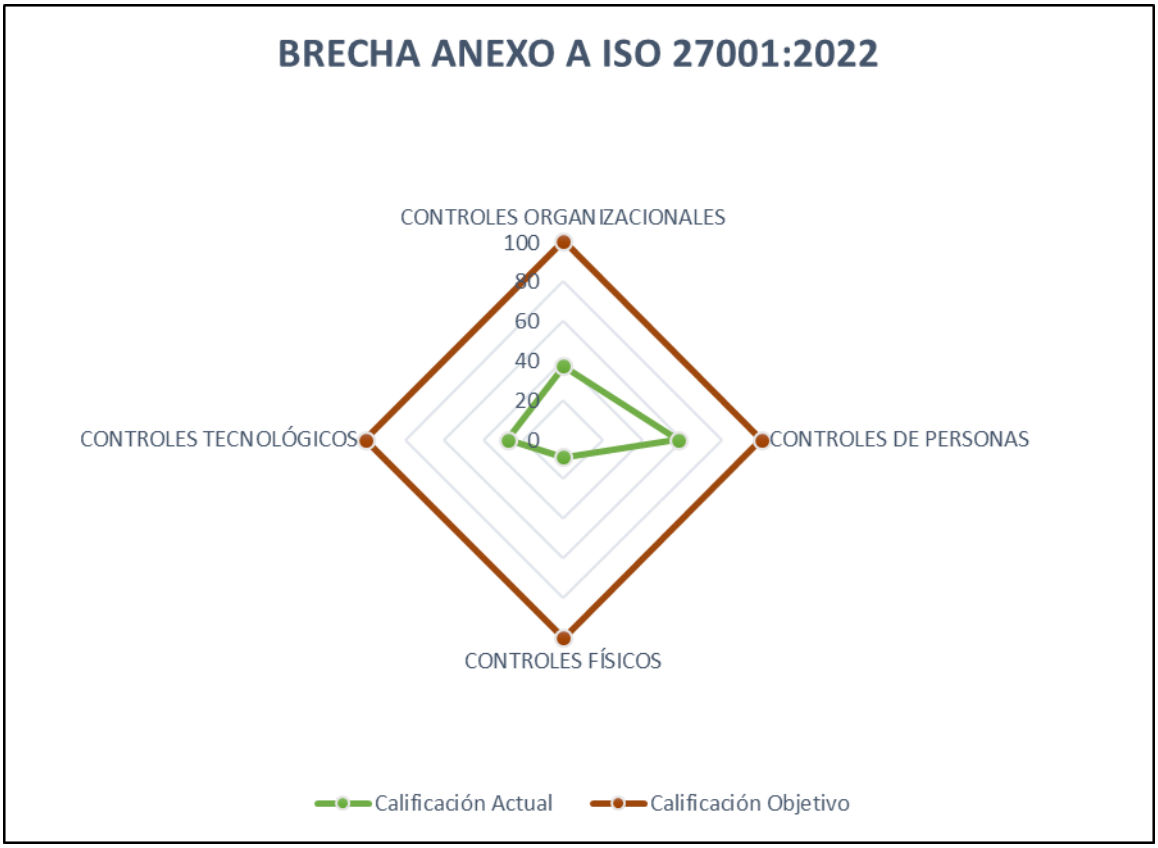
No.	DOMINIO	Calificación Actual	Calificación Objetivo	Efectividad del control
A.5	Controles Organizacionales	37	100	Repetible
A.6	Controles de Personas	58	100	Efectivo
A.7	Controles Físicos	9	100	Inicial
A.8	Controles Tecnológicos	28	100	Repetible
PROMEDIO EVALUACIÓN DE CONTROLES		**33**	**100**	**REPETIBLE**

Nota. Avance evaluación de efectividad de controles – Instrumento de identificación de la línea base de seguridad, autodiagnóstico Modelo de Seguridad y Privacidad de la Información – MSPI, ejecución vigencia (2025).

Con base en los resultados obtenidos, se presenta a continuación el análisis de brechas (GAP), el cual constituye una herramienta metodológica para identificar, analizar y evaluar las diferencias entre el estado actual y el estado objetivo de la implementación del Modelo de Seguridad y Privacidad de la Información (MSPI) en la Agencia Logística de las Fuerzas Militares (ALFM). En este contexto, una "brecha" representa la distancia existente entre la situación actual de la entidad; es decir, dónde se encuentra actualmente y el nivel de madurez esperado o deseado, dónde se espera llegar en materia de seguridad y privacidad de la información.

Este análisis permite identificar de manera estructurada las áreas en las que los controles, procesos y prácticas vigentes no cumplen total o parcialmente con los lineamientos y requisitos establecidos en el MSPI. Asimismo, constituye un insumo fundamental para la priorización de acciones de mejora, la definición de actividades correctivas y la formulación de estrategias orientadas al cierre de brechas, facilitando la alineación del Sistema de Gestión de Seguridad y Privacidad de la Información (SGSPI) con los objetivos estratégicos institucionales, el marco normativo vigente y las mejores prácticas internacionales en seguridad de la información.

Figura 1.
Brecha anexa "A" ISO 27001:2022.



Nota. Identificación brecha anexo "A" ISO 27001:2022 Anexo "A" – Instrumento de identificación de la línea base de seguridad, autodiagnóstico Modelo de Seguridad y Privacidad de la Información – MSPI, ejecución vigencia (2025).

5.2. ALINEACIÓN CON EL PLAN ESTRATÉGICO DE TECNOLOGÍAS DE LA INFORMACIÓN (PETI).

En el marco de la ejecución del Plan Estratégico de Tecnologías de la Información (PETI) y considerando los resultados, avances y lecciones aprendidas en vigencias anteriores, para la vigencia 2026 la Agencia Logística de las Fuerzas Militares (ALFM) dará continuidad y profundizará las acciones orientadas al fortalecimiento, actualización y maduración del Modelo de Seguridad y Privacidad de la Información (MSPI). Estas acciones se desarrollan como parte integral de los proyectos estratégicos de la Política de Gobierno Digital de la entidad, garantizando su alineación con los lineamientos definidos por el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), así como con las buenas prácticas y estándares internacionales en materia de seguridad de la información y ciberseguridad.

De igual manera, la implementación de las actividades contempladas en el presente Plan Estratégico de Seguridad y Privacidad de la Información (PESI) contribuirá de manera directa al cumplimiento de las políticas institucionales de Seguridad de la Información, Seguridad Digital y Gobierno Digital, fortaleciendo la gestión de los procesos estratégicos, misionales y de apoyo de la ALFM. Este enfoque permitirá asegurar la confidencialidad,

integridad y disponibilidad de los activos de información, fortalecer la resiliencia institucional frente a riesgos y amenazas del entorno digital y consolidar un ecosistema tecnológico seguro, confiable y alineado con el marco normativo vigente y los objetivos estratégicos de la entidad.

5.3. ESTRATEGIA DE SEGURIDAD DIGITAL.

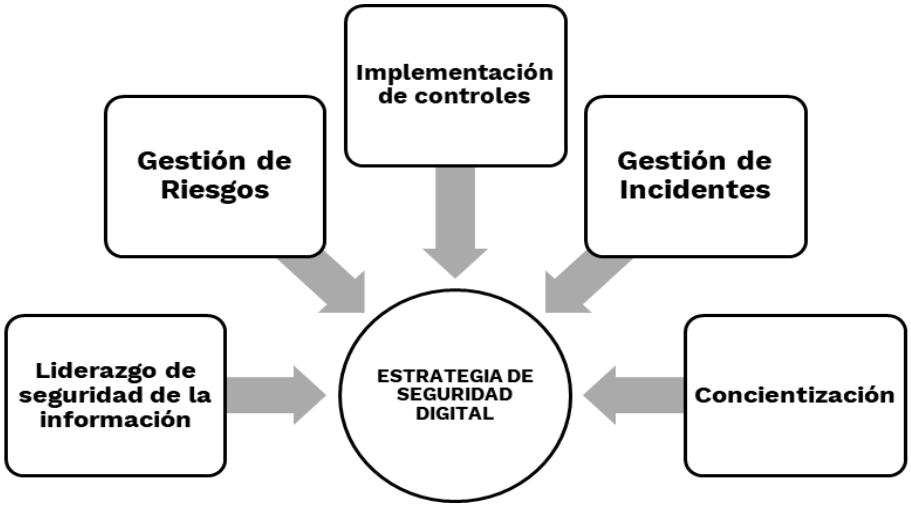
La Agencia Logística de las Fuerzas Militares (ALFM) adoptará e implementará una estrategia integral de seguridad digital orientada a fortalecer la protección de la información y los activos tecnológicos institucionales, mediante la articulación de principios, políticas, procedimientos, guías, manuales, formatos y lineamientos que permitan una gestión eficaz, coherente y sostenible de la seguridad y privacidad de la información.

Esta estrategia tiene como eje estructural la implementación, actualización y maduración del Modelo de Seguridad y Privacidad de la Información (MSPI), en concordancia con la Resolución 02277 de 2025, la Política de Gobierno Digital y la norma ISO/IEC 27001:2022. Asimismo, se apoya en instrumentos institucionales como la Guía de Gestión de Riesgos de Seguridad de la Información, el Plan de Tratamiento de Riesgos, la Declaración de Aplicabilidad (SoA) y el Procedimiento de Gestión de Incidentes de Seguridad de la Información, garantizando una gestión integral basada en el enfoque de riesgos y el ciclo de mejora continua PHVA.

La estrategia de seguridad digital de la ALFM está orientada a garantizar la confidencialidad, integridad y disponibilidad de los activos de información, asegurar la continuidad de los servicios críticos, fortalecer la resiliencia institucional frente a amenazas cibernéticas y dar cumplimiento a los requisitos legales, normativos y regulatorios aplicables, tanto a nivel nacional como internacional, en coherencia con los objetivos estratégicos de la entidad.

En este contexto, la ALFM define cinco (5) estrategias específicas que, de manera articulada, conforman la estrategia general de seguridad digital y orientan la planificación, ejecución, seguimiento y mejora de las acciones previstas en el Plan Estratégico de Seguridad y Privacidad de la Información (PESI) para la vigencia 2026.

Figura 2.
Estrategia de seguridad digital.



Nota. Especificación estrategia de seguridad digital – Manual de Gobierno Digital (2022).

5.3.1. Descripción de las estrategias especificas (Ejes).

A continuación, se describen las estrategias específicas que orientan la implementación del Plan Estratégico de Seguridad y Privacidad de la Información (PESI) para la vigencia 2026. Cada una de estas estrategias se encuentra alineada con los lineamientos establecidos en el Modelo de Seguridad y Privacidad de la Información (MSPI), la Resolución 02277 de 2025, la Política de Gobierno Digital y la norma ISO/IEC 27001:2022.

Estas estrategias tienen como propósito fortalecer la seguridad digital institucional, garantizar el cumplimiento normativo y asegurar la adecuada protección de los activos de información de la Agencia Logística de las Fuerzas Militares (ALFM), mediante un enfoque integral basado en la gestión de riesgos, la mejora continua y la corresponsabilidad institucional.

Tabla 3.
Descripción estrategias específicas.

ESTRATEGIA / EJE	DESCRIPCIÓN / OBJETIVO
Liderazgo de seguridad de la información.	Esta estrategia se orienta a fortalecer el liderazgo activo de la Alta Dirección y de los responsables de los diferentes procesos y dependencias de la entidad, asegurando el cumplimiento de los roles, responsabilidades y autoridades definidos en el Sistema de Gestión de Seguridad y Privacidad de la Información (SGSPI). El enfoque central consiste en consolidar una estructura de gobernanza sólida que permita dirigir, supervisar y respaldar de manera efectiva la implementación del MSPI, promoviendo la toma de decisiones informadas, la asignación adecuada de recursos y la integración de la seguridad de la información en la

	gestión institucional. De esta manera, se busca fomentar una cultura organizacional orientada a la seguridad, en la cual todos los niveles de la entidad contribuyan activamente al fortalecimiento y sostenibilidad del modelo.
Gestión de riesgos.	Esta estrategia tiene como objetivo identificar, analizar, evaluar y tratar los riesgos de seguridad y privacidad de la información mediante un proceso estructurado y sistemático, alineado con el contexto institucional y los objetivos estratégicos de la ALFM. La gestión de riesgos se fundamenta en la valoración de los activos de información, la identificación de amenazas y vulnerabilidades, y la definición de controles adecuados para prevenir, mitigar, transferir o aceptar los riesgos identificados. Asimismo, permite priorizar acciones, actualizar el Plan de Tratamiento de Riesgos (PTR) y la Declaración de Aplicabilidad (SoA), y asegurar que los controles implementados estén alineados con los requisitos normativos y las mejores prácticas, garantizando la confidencialidad, integridad y disponibilidad de la información institucional.
Concientización.	Esta estrategia busca fortalecer una cultura organizacional sólida en materia de seguridad y privacidad de la información, promoviendo la apropiación de buenas prácticas y el cumplimiento de las políticas, procedimientos y lineamientos institucionales en todos los niveles de la entidad. Para ello, se impulsarán actividades permanentes de sensibilización, capacitación y transferencia de conocimiento, orientadas a que funcionarios, contratistas y terceros comprendan su rol y responsabilidad frente a la protección de la información. El objetivo es que la seguridad de la información se convierta en un comportamiento cotidiano y transversal, contribuyendo a la reducción de incidentes, al cumplimiento normativo y al fortalecimiento de la continuidad operativa y la confianza de las partes interesadas.
Implementación de controles.	La implementación de controles de seguridad y privacidad de la información constituye un eje fundamental para garantizar la protección de los activos de información y la continuidad de los procesos institucionales de la Agencia Logística de las Fuerzas Militares (ALFM). En el marco del Modelo de Seguridad y Privacidad de la Información (MSPI), esta estrategia se orienta a planificar, implementar, mantener y madurar controles adecuados y proporcionales al nivel de riesgo identificado, en coherencia con los objetivos estratégicos de la entidad, el contexto organizacional y los requisitos normativos aplicables. Los controles de seguridad se estructuran conforme a la

	clasificación establecida en la norma ISO/IEC 27001:2022, abarcando controles organizacionales, de personas, físicos y tecnológicos, los cuales se implementan de manera articulada para asegurar un enfoque integral de protección: **Controles organizacionales:** Están orientados a establecer el marco de gobernanza, gestión y dirección de la seguridad y privacidad de la información. Incluyen la definición, actualización y aplicación de políticas, procedimientos, lineamientos y estándares institucionales; la asignación de roles y responsabilidades; la gestión de riesgos; la gestión de proveedores y terceros; la gestión de cambios; la continuidad del negocio; el cumplimiento normativo; la auditoría interna y los mecanismos de seguimiento y mejora continua del Sistema de Gestión de Seguridad y Privacidad de la Información (SGSPI). **Controles de personas:** Se enfocan en la gestión del talento humano y en la reducción de riesgos asociados al factor humano. Comprenden procesos de selección, vinculación y desvinculación, definición de responsabilidades en seguridad de la información, acuerdos de confidencialidad, capacitación y concientización permanente, así como la promoción de una cultura organizacional orientada a la seguridad y privacidad de la información, asegurando que funcionarios, contratistas y terceros comprendan y cumplan sus obligaciones en esta materia. **Controles físicos:** Están destinados a proteger las instalaciones, los equipos y la infraestructura física que soporta los activos de información. Incluyen medidas de control de acceso físico, protección de áreas críticas como centros de datos y cuartos técnicos, vigilancia, monitoreo, gestión de visitantes, protección ambiental y salvaguardas contra amenazas físicas o ambientales que puedan afectar la disponibilidad, integridad o confidencialidad de la información. **Controles tecnológicos:** Corresponden a las medidas técnicas implementadas para proteger los sistemas de información y la infraestructura tecnológica. Comprenden, entre otros, la gestión de accesos y autenticación, el uso de cifrado, la protección de redes, la segmentación y monitoreo del tráfico, la detección y respuesta ante amenazas, la gestión de vulnerabilidades, el respaldo y recuperación de la información, la seguridad en servicios en la nube y la protección de los sistemas críticos de la entidad.

	La correcta implementación e integración de estos controles permite reducir la probabilidad y el impacto de incidentes de seguridad, fortalecer la resiliencia institucional y asegurar el cumplimiento de los principios de confidencialidad, integridad y disponibilidad de la información. Asimismo, estos controles son evaluados y ajustados de manera periódica como parte del ciclo de mejora continua del MSPI, garantizando su eficacia frente a la evolución de los riesgos, las amenazas y el entorno normativo y tecnológico.
Gestión de incidentes.	Esta estrategia tiene como finalidad garantizar una gestión integral, oportuna y efectiva de los incidentes de seguridad de la información, abarcando su detección, análisis, contención, respuesta, recuperación y comunicación. La gestión de incidentes se orienta a minimizar el impacto de los eventos de seguridad sobre los procesos, servicios y activos de información de la entidad, así como a fortalecer la capacidad institucional de prevención y respuesta. Adicionalmente, los incidentes y debilidades identificadas se convierten en insumos clave para la mejora continua del SGSPI, permitiendo ajustar controles, actualizar procedimientos y fortalecer las defensas a largo plazo, consolidando un entorno digital seguro y resiliente.

Nota. Descripción estrategias especificas a implementar de acuerdo a los lineamientos de la resolución 500 de 2021. Producto tipo PESI MinTIC (2022).

5.4. RESPONSABILIDADES.

Tabla 4.
Descripción responsabilidades frente a la implementación del MSPI.

ROL Y/O CARGO FRENTE AL SGSI	RESPONSABILIDADES
Alta Dirección. ***(Nivel estratégico y de decisión).***	Aprobar, respaldar y liderar el diseño, implementación, actualización y maduración del SGSPI, conforme al MSPI, la Resolución 02277 de 2025 y la ISO/IEC 27001:2022. Definir, aprobar y promover la Política de Seguridad y Privacidad de la Información, garantizando su divulgación y apropiación institucional. Alinear los objetivos de seguridad y privacidad de la información con los objetivos estratégicos de la entidad y el PETI.

ROL Y/O CARGO FRENTE AL SGSI	RESPONSABILIDADES
	Garantizar el establecimiento y mantenimiento de procesos y controles que protejan la confidencialidad, integridad y disponibilidad de los activos de información. Asignar y aprobar los recursos financieros, técnicos, tecnológicos y humanos necesarios para el SGSPI. Realizar la revisión por la dirección, evaluando la conveniencia, adecuación y eficacia del SGSPI frente al contexto y los riesgos. Garantizar el cumplimiento de los requisitos legales, normativos y contractuales aplicables. Conocer y hacer seguimiento a riesgos, incidentes relevantes y acciones correctivas. Evaluar anualmente el desempeño del SGSPI mediante indicadores, auditorías e informes de gestión. Promover una cultura organizacional de seguridad y privacidad de la información.
Comité Institucional de Gestión y Desempeño. ***(Nivel de gobernanza y seguimiento).***	Analizar los resultados del diagnóstico y del análisis de brechas (GAP) del MSPI. Conocer y apoyar la implementación de la Política de Seguridad y Privacidad de la Información. Realizar seguimiento a la implementación, operación y mejora continua del SGSPI. Conocer y analizar incidentes relevantes de seguridad y las acciones derivadas. Proponer a la Alta Dirección planes, acciones y medidas de fortalecimiento del SGSPI. Hacer seguimiento y análisis a los indicadores de desempeño del SGSPI. Conocer los avances, resultados y efectividad de las acciones de seguridad y privacidad.

ROL Y/O CARGO FRENTE AL SGSI	RESPONSABILIDADES
Líder Proceso Gestión de TIC. ***(Nivel de articulación estratégica - operativa).***	Orientar y coordinar el diseño, implementación, operación y sostenibilidad del SGSPI. Articular el SGSPI con los procesos de TI, el PETI y los proyectos tecnológicos. Proponer acciones de mejora ante desviaciones, riesgos o incidentes. Representar a la entidad ante organismos externos en temas del SGSPI. Informar periódicamente a la Alta Dirección sobre el estado y desempeño del SGSPI. Coordinar con líderes de proceso las acciones necesarias para la implementación del SGSPI.
Profesional Seguridad de la Información. ***(Responsable operativo del SGSPI).***	Diseñar, implementar, operar y mantener el SGSPI. Elaborar, actualizar y socializar políticas, procedimientos, planes y lineamientos del SGSPI. Identificar, analizar, evaluar y tratar los riesgos de seguridad y privacidad de la información. Coordinar programas de sensibilización y capacitación. Liderar la gestión de incidentes de seguridad de la información. Verificar el cumplimiento normativo y apoyar auditorías internas y externas. Informar a la Alta Dirección y al Comité sobre el desempeño y resultados del SGSPI. Solicitar y justificar los recursos necesarios para la operación del SGSPI.
Líderes de Proceso. ***(Responsables de la seguridad en los procesos).***	Garantizar la aplicación de políticas y lineamientos del SGSPI en los procesos a su cargo. Identificar, evaluar y hacer seguimiento a los riesgos de seguridad de la información del proceso.

ROL Y/O CARGO FRENTE AL SGSI	RESPONSABILIDADES
	Proteger los activos de información del proceso, actuando como dueños cuando aplique. Facilitar la participación del personal en actividades de capacitación y sensibilización. Reportar incidentes, incumplimientos y condiciones inseguras. Implementar acciones correctivas, preventivas y de mejora relacionadas con el SGSPI.
Dueños de Activos de Información. ***(Responsables de la información).***	Identificar, clasificar y mantener actualizado el inventario de activos de información. Definir criterios de acceso, uso, conservación y eliminación de la información. Aprobar los controles de seguridad aplicables a los activos bajo su responsabilidad. Participar en la gestión de riesgos asociados a los activos. Verificar el cumplimiento de políticas por parte de custodios y usuarios. Reportar incidentes que afecten los activos de información.
Custodios de Activos de Información. ***(Responsables técnicos/operativos de los activos).***	Administrar y proteger los activos asignados, garantizando su confidencialidad, integridad y disponibilidad. Implementar y operar los controles definidos por el SGSPI y los dueños de activos. Gestionar adecuadamente accesos y uso de los sistemas de información. Reportar incidentes, vulnerabilidades o condiciones inseguras. Apoyar procesos de respaldo, recuperación y continuidad del negocio.

ROL Y/O CARGO FRENTE AL SGSI	RESPONSABILIDADES
Funcionarios – Contratistas. ***(Usuarios de la Información).***	Cumplir las políticas, normas y procedimientos del SGSPI. Utilizar adecuadamente los activos de información y recursos tecnológicos. Participar en capacitaciones y actividades de sensibilización. Proteger la información bajo su responsabilidad. Reportar oportunamente incidentes, riesgos o condiciones inseguras. Cumplir los requisitos legales, normativos y contractuales aplicables.
Responsable de Seguridad Física y del Entorno.	Implementar y mantener los controles de seguridad física y ambiental que protegen instalaciones, centros de datos, cuartos técnicos y áreas críticas. Gestionar los controles de acceso físico, monitoreo, vigilancia y protección ambiental. Coordinar acciones de seguridad física con las áreas de TI y seguridad de la información. Reportar eventos e incidentes físicos que puedan afectar los activos de información. Participar en la identificación y tratamiento de riesgos físicos y ambientales.
Responsable de Talento Humano (Seguridad de Personas).	Incorporar criterios de seguridad y privacidad de la información en los procesos de vinculación, permanencia y desvinculación del personal. Garantizar la firma de acuerdos de confidencialidad y aceptación de políticas de seguridad. Coordinar programas de sensibilización y capacitación en seguridad de la información. Apoyar la aplicación de medidas disciplinarias relacionadas con incumplimientos de políticas de seguridad.

ROL Y/O CARGO FRENTE AL SGSI	RESPONSABILIDADES
	Notificar oportunamente al Proceso Gestión de TIC los cambios de rol, retiros o novedades del personal.
Responsable de Gestión de Proveedores y Terceros.	Asegurar que los proveedores, contratistas y terceros cumplan los requisitos de seguridad y privacidad de la información definidos por la ALFM. Incluir cláusulas de seguridad de la información y protección de datos en contratos y acuerdos. Evaluar riesgos asociados a terceros y servicios externalizados, incluyendo servicios en la nube. Realizar seguimiento al cumplimiento de los compromisos de seguridad por parte de proveedores. Reportar incidentes de seguridad asociados a terceros.
Responsable de Continuidad del Negocio y Recuperación ante Desastres.	Diseñar, mantener y actualizar los planes de continuidad del negocio y recuperación ante desastres. Coordinar pruebas periódicas de continuidad y recuperación. Asegurar la alineación entre los planes de continuidad y los riesgos de seguridad de la información. Reportar resultados de pruebas y eventos reales a la Alta Dirección y al Comité Institucional. Coordinar acciones de respuesta ante incidentes mayores que afecten la operación institucional.
Auditores Internos.	Planificar y ejecutar auditorías internas al SGSPI conforme a la ISO/IEC 27001:2022. Verificar el cumplimiento de políticas, procedimientos y controles del MSPI. Identificar hallazgos, no conformidades y oportunidades de mejora.

ROL Y/O CARGO FRENTE AL SGSI	RESPONSABILIDADES
	Hacer seguimiento a las acciones correctivas y preventivas. Reportar resultados de auditoría a la Alta Dirección y al Comité Institucional de Gestión y Desempeño.
Responsabilidades de los Visitantes	Cumplir las normas, políticas y lineamientos de seguridad y privacidad de la información definidos por la ALFM durante su permanencia en las instalaciones. Acatar los controles de acceso físico y las instrucciones del personal autorizado. Proteger la información a la que eventualmente tenga acceso y reportar cualquier incidente de seguridad identificado.

Nota. Descripción matriz de roles y responsabilidades sistema de gestión de seguridad y privacidad de la información – SGSPI – Proceso Gestión de TIC (Seguridad de la Información) (2025).

6. MATRIZ DE ACTIVIDADES

Tabla 5.
Definición de actividades, establecidas por estrategia.

ESTRATEGIA/EJE	METAS	RESULTADOS	INSTRUMENTO	SEGUIMIENTOS Y MONITOREO	CONTROLES
Liderazgo de seguridad de la información.	Implementación MSPI.	Análisis GAP para identificar el estado actual de la entidad en relación con la adopción del MSPI.	Documento maestro de los lineamientos del Modelo de Seguridad y Privacidad de la Información - Versión 5 (21/04/2025). Autodiagnóstico MSPI.	Plazo: Primer Bimestre. Evidencia: Informe del análisis GAP realizado - Soporte de divulgación a la Alta Dirección y partes interesadas.	A.5.1, A.5.5, A.5.6, A.5.7, A.5.31, A.5.36
		Plan de Gestión del Cambio del MSPI elaborado, documentado y socializado, orientado a facilitar la adopción progresiva del Modelo de Seguridad y Privacidad de la		Plazo: Primer Bimestre. Evidencia: Documento del Plan de Gestión del Cambio del MSPI - Soporte de divulgación a la Alta Dirección y partes interesadas.	

ESTRATEGIA/EJE	METAS	RESULTADOS	INSTRUMENTO	SEGUIMIENTOS Y MONITOREO	CONTROLES
		Información en la entidad.			
		Seguimiento periódico y documentado al avance en la implementación del MSPI en la entidad, permitiendo verificar el nivel de cumplimiento, identificar brechas y definir acciones de mejora.		Plazo: Trimestral. Evidencia: Informe de seguimiento implementación MSPI, anexando el instrumento de evaluación actualizado.	
		Proceso de seguimiento, análisis y verificación de la ejecución de las actividades definidas en el Plan Estratégico de Seguridad de la Información (PESI) realizado, orientado a identificar ajustes, mejoras y/o cambios necesarios que permitan asegurar el cumplimiento de la normativa aplicable y la alineación con los objetivos estratégicos y misionales de la entidad.		Plazo: Anual. Evidencia: Informe de Análisis y Verificación del Plan Estratégico de Seguridad de la Información (PESI).	
	Análisis para determinar la necesidad de actualizar las políticas de seguridad de la información.	Políticas, manuales y lineamientos institucionales de Seguridad y Privacidad de la Información elaborados, actualizados y gestionados, asegurando el cumplimiento	Documento maestro de los lineamientos del Modelo de Seguridad y Privacidad de la Información - Versión 5 (21/04/2025). Lineamientos relación con	Plazo: Semestral. Evidencia: Políticas, manuales y lineamientos institucionales de Seguridad y Privacidad de la Información actualizados y aprobados ante el	

ESTRATEGIA/EJE	METAS	RESULTADOS	INSTRUMENTO	SEGUIMIENTOS Y MONITOREO	CONTROLES
		normativo y la correcta adopción del MSPI en la entidad.	proveedores de Tecnologías de la Información y las Comunicaciones - Versión 5 (21/04/2025). Lineamientos de seguridad de la información para el uso de servicios en la nube - Versión 5 (21/04/2025).	SIG.	
	Fortalecer el control institucional y la mejora continua del Sistema de Seguridad de la Información, en articulación con la Oficina de Control Interno.	Mesa de trabajo con la Oficina de Control Interno realizada y documentada, orientada a definir y acordar lineamientos claros para la revisión, evaluación y fortalecimiento continuo del MSPI.	Documento maestro de los lineamientos del Modelo de Seguridad y Privacidad de la Información - Versión 5 (21/04/2025).	Plazo: Primer Bimestre. Evidencia: Acta y/o registro de la mesa de trabajo realizada con la Oficina de Control Interno.	
		Auditorías internas y/o evaluaciones de control realizadas, con planes de mejora definidos, ejecutados y alineados con los objetivos del PESI y el MSPI.		Plazo: Semestral. Evidencia: Informes de auditoría y/o evaluaciones de control interno con sus debidos soportes en caso de aplicar (Planes de acción y/o mejora derivados de los hallazgos).	
	Gestión Plan Maestro de Continuidad y Gestión de Crisis ALFM.	Documento de justificación elaborado sobre la vigencia o actualización de los formatos asociados al Plan de Continuidad y a las Pruebas de Recuperación.	Documento maestro de los lineamientos del Modelo de Seguridad y Privacidad de la Información - Versión 5 (21/04/2025).	Plazo: Primer trimestre. Evidencia: Documento que justifica la decisión de no actualizar los formatos Evaluación Evento Activación Plan de Continuidad, Diseño y Ejecución de Pruebas de	

ESTRATEGIA/EJE	METAS	RESULTADOS	INSTRUMENTO	SEGUIMIENTOS Y MONITOREO	CONTROLES
				Recuperación y Evaluación Pruebas de Recuperación o las versiones actualizadas del mismo.	
		Revisar, actualizar y ajustar el Plan Maestro de Continuidad y Gestión de Crisis, garantizando su coherencia con el MSPI, la normativa vigente y las necesidades institucionales.		Plazo: Primer trimestre. Evidencia: Plan Maestro de Continuidad y Gestión de Crisis actualizado y ajustado.	
		Seguimiento a la gestión del Plan Maestro de Continuidad y Gestión de Crisis de la ALFM.		Plazo: Semestral. Evidencia: Informes de seguimiento al cumplimiento de las actividades definidas en el Plan Maestro de Continuidad y Gestión de Crisis, con sus respectivos soportes.	
Gestión de riesgos.	Gestión Plan de Tratamiento de Riesgos de seguridad y privacidad de la información.	Seguimiento al estado avance del Plan de tratamiento de riesgos de seguridad y privacidad de la información.	Documento maestro de los lineamientos del Modelo de Seguridad y Privacidad de la Información - Versión 5 (21/04/2025). Lineamientos del Modelo Nacional de Gestión de Riesgo de Seguridad de la Información en Entidades Públicas - Versión 5 (21/04/2025).	Plazo: Trimestral. Evidencia: Informe de seguimiento al cumplimiento de actividades establecidas, mediante el Plan de Tratamiento de Riesgos de seguridad y Privacidad de la Información.	A.5.8, A.5.9, A.5.12, A.5.19, A.5.21, A.5.22, A.5.23
Concientización.	Plan de	Plan de	Documento	Plazo: Primer	A.6.1–A.6.8,

ESTRATEGIA/EJE	METAS	RESULTADOS	INSTRUMENTO	SEGUIMIENTOS Y MONITOREO	CONTROLES
	sensibilización anual funcionarios de la ALFM.	actividades de sensibilización y concientización en temas relacionados a seguridad y privacidad de la información dirigido a todos los funcionarios de la entidad.	maestro de los lineamientos del Modelo de Seguridad y Privacidad de la Información - Versión 5 (21/04/2025).	Bimestre. Evidencia: Plan de sensibilización y capacitación a los funcionarios de la ALFM. Plazo: Semestral. Evidencia: Informes de seguimiento a la ejecución del plan de actividades de sensibilización y concientización.	A.5.10, A.5.11, A.5.34
Implementación de controles.	Verificar la implementación de los controles organizacionales del Sistema de Gestión de Seguridad de la Información (SGSI), conforme al Anexo A de la ISO/IEC 27001:2022, mediante mesas de trabajo articuladas con los procesos, con el fin de identificar el nivel de cumplimiento, brechas y oportunidades de mejora.	Verificación del estado de implementación de los controles organizacionales aplicables al Proceso Gestión de TIC.	Documento maestro de los lineamientos del Modelo de Seguridad y Privacidad de la Información - Versión 5 (21/04/2025). Autodiagnóstico MSPI.	Plazo: Primer Trimestre. Evidencia: Acta de reunión de la mesa de trabajo con el proceso, que soporta la verificación de la implementación de los controles organizacionales del Anexo A de la ISO/IEC 27001:2022 y los compromisos definidos. Plazo: Cuatrimestral. Evidencia: Informe de seguimiento al cumplimiento de los compromisos establecidos en las mesas de trabajo.	A.5.1, A.5.3, A.5.5, A.5.6, A.5.7, A.5.9, A.5.15, A.5.17, A.5.23, A.5.24, A.5.25, A.5.26, A.5.27, A.5.28, A.5.31, A.5.32 y A.5.37.
		Verificación del estado de implementación de los controles organizacionales aplicables a los Procesos Gestión de TIC y Desarrollo Organizacional y Gestión Integral.		Plazo: Primer Trimestre. Evidencia: Acta de reunión de la mesa de trabajo con el proceso, que soporta la verificación de la implementación de los controles organizacionales	A.5.29 y A.5.30

ESTRATEGIA/EJE	METAS	RESULTADOS	INSTRUMENTO	SEGUIMIENTOS Y MONITOREO	CONTROLES
				del Anexo A de la ISO/IEC 27001:2022 y los compromisos definidos.	
				Plazo: Cuatrimestral. Evidencia: Informe de seguimiento al cumplimiento de los compromisos establecidos en las mesas de trabajo.	
		Verificación del estado de implementación de los controles organizacionales aplicables a los Procesos Gestión de TIC y Gestión de la Contratación.		Plazo: Primer Trimestre. Evidencia: Acta de reunión de la mesa de trabajo con el proceso, que soporta la verificación de la implementación de los controles organizacionales del Anexo A de la ISO/IEC 27001:2022 y los compromisos definidos.	A.5.19, A.5.20, A.5.21 y A.5.22
				Plazo: Cuatrimestral. Evidencia: Informe de seguimiento al cumplimiento de los compromisos establecidos en las mesas de trabajo.	
		Verificación del estado de implementación de los controles organizacionales aplicables a los Procesos Gestión de TIC y Gestión Administrativa (Grupo Gestión Documental).		Plazo: Primer Trimestre. Evidencia: Acta de reunión de la mesa de trabajo con el proceso, que soporta la verificación de la implementación de los controles organizacionales	A.5.10, A.5.12, A.5.13, A.5.14 y A.5.33

ESTRATEGIA/EJE	METAS	RESULTADOS	INSTRUMENTO	SEGUIMIENTOS Y MONITOREO	CONTROLES
				del Anexo A de la ISO/IEC 27001:2022 y los compromisos definidos. Plazo: Cuatrimestral. Evidencia: Informe de seguimiento al cumplimiento de los compromisos establecidos en las mesas de trabajo.	
		Verificación del estado de implementación de los controles organizacionales aplicables a los Procesos Gestión de TIC y Gestión de Seguimiento y Evaluación.		Plazo: Primer Trimestre. Evidencia: Acta de reunión de la mesa de trabajo con el proceso, que soporta la verificación de la implementación de los controles organizacionales del Anexo A de la ISO/IEC 27001:2022 y los compromisos definidos. Plazo: Cuatrimestral. Evidencia: Informe de seguimiento al cumplimiento de los compromisos establecidos en las mesas de trabajo.	A.5.36
		Verificación del estado de implementación de los controles organizacionales aplicables a los Procesos Gestión de TIC, Desarrollo Organizacional y Gestión Integral y Gestión de la		Plazo: Primer Trimestre. Evidencia: Acta de reunión de la mesa de trabajo con el proceso, que soporta la verificación de la implementación de los controles organizacionales	A.5.8

ESTRATEGIA/EJE	METAS	RESULTADOS	INSTRUMENTO	SEGUIMIENTOS Y MONITOREO	CONTROLES
		Contratación.		del Anexo A de la ISO/IEC 27001:2022 y los compromisos definidos. Plazo: Cuatrimestral. Evidencia: Informe de seguimiento al cumplimiento de los compromisos establecidos en las mesas de trabajo.	
		Verificación del estado de implementación de los controles organizacionales aplicables a los Procesos Gestión de TIC, Gestión Administrativa (Grupo Gestión Documental) y Gestión de la Contratación.		Plazo: Primer Trimestre. Evidencia: Acta de reunión de la mesa de trabajo con el proceso, que soporta la verificación de la implementación de los controles organizacionales del Anexo A de la ISO/IEC 27001:2022 y los compromisos definidos. Plazo: Cuatrimestral. Evidencia: Informe de seguimiento al cumplimiento de los compromisos establecidos en las mesas de trabajo.	A.5.16 y A.5.18
		Verificación del estado de implementación de los controles organizacionales aplicables a los Procesos Gestión de TIC, Gestión de Talento Humano y Gestión Administrativa.		Plazo: Primer Trimestre. Evidencia: Acta de reunión de la mesa de trabajo con el proceso, que soporta la verificación de la implementación de los controles organizacionales	A.5.11

ESTRATEGIA/EJE	METAS	RESULTADOS	INSTRUMENTO	SEGUIMIENTOS Y MONITOREO	CONTROLES
				del Anexo A de la ISO/IEC 27001:2022 y los compromisos definidos.	
				Plazo: Cuatrimestral. Evidencia: Informe de seguimiento al cumplimiento de los compromisos establecidos en las mesas de trabajo.	
		Verificación del estado de implementación de los controles organizacionales aplicables a los Procesos Gestión de TIC, Gestión de Innovación y Redes de Valor (Grupo de Atención y Orientación Ciudadana), Talento Humano, Gestión Administrativa y Gestión de la Contratación.		Plazo: Primer Trimestre. Evidencia: Acta de reunión de la mesa de trabajo con el proceso, que soporta la verificación de la implementación de los controles organizacionales del Anexo A de la ISO/IEC 27001:2022 y los compromisos definidos.	A.5.34
				Plazo: Cuatrimestral. Evidencia: Informe de seguimiento al cumplimiento de los compromisos establecidos en las mesas de trabajo.	
	Verificar la implementación de los controles de personas del Sistema de Gestión de Seguridad de la Información (SGSI), conforme al Anexo A de la ISO/IEC	Verificación del estado de implementación de los controles de personas aplicables a los Procesos Gestión de TIC.	Documento maestro de los lineamientos del Modelo de Seguridad y Privacidad de la Información - Versión 5 (21/04/2025). Autodiagnóstico MSPI.	Plazo: Primer Trimestre. Evidencia: Acta de reunión de la mesa de trabajo con el proceso, que soporta la verificación de la implementación de los controles organizacionales	A.6.3

ESTRATEGIA/EJE	METAS	RESULTADOS	INSTRUMENTO	SEGUIMIENTOS Y MONITOREO	CONTROLES
	27001:2022, mediante mesas de trabajo articuladas con los procesos, con el fin de identificar el nivel de cumplimiento, brechas y oportunidades de mejora.			del Anexo A de la ISO/IEC 27001:2022 y los compromisos definidos.	
				Plazo: Cuatrimestral. Evidencia: Informe de seguimiento al cumplimiento de los compromisos establecidos en las mesas de trabajo.	
		Verificación del estado de implementación de los controles de personas aplicables a los Procesos Gestión de TIC y Gestión del Talento Humano.		Plazo: Primer Trimestre. Evidencia: Acta de reunión de la mesa de trabajo con el proceso, que soporta la verificación de la implementación de los controles organizacionales del Anexo A de la ISO/IEC 27001:2022 y los compromisos definidos.	A.6.7
				Plazo: Cuatrimestral. Evidencia: Informe de seguimiento al cumplimiento de los compromisos establecidos en las mesas de trabajo.	
		Verificación del estado de implementación de los controles de personas aplicables a los Procesos Gestión de TIC, Gestión del Talento Humano y Gestión de la Contratación.		Plazo: Primer Trimestre. Evidencia: Acta de reunión de la mesa de trabajo con el proceso, que soporta la verificación de la implementación de los controles organizacionales	A.6.1, A.6.2, A.6.5, A.6.6 y A.6.8

ESTRATEGIA/EJE	METAS	RESULTADOS	INSTRUMENTO	SEGUIMIENTOS Y MONITOREO	CONTROLES
				del Anexo A de la ISO/IEC 27001:2022 y los compromisos definidos. Plazo: Cuatrimestral. Evidencia: Informe de seguimiento al cumplimiento de los compromisos establecidos en las mesas de trabajo.	
		Verificación del estado de implementación de los controles de personas aplicables a los Procesos Gestión de TIC, Gestión del Talento Humano (Oficina Control Interno Disciplinario) y Gestión de la Contratación.		Plazo: Primer Trimestre. Evidencia: Acta de reunión de la mesa de trabajo con el proceso, que soporta la verificación de la implementación de los controles organizacionales del Anexo A de la ISO/IEC 27001:2022 y los compromisos definidos. Plazo: Cuatrimestral. Evidencia: Informe de seguimiento al cumplimiento de los compromisos establecidos en las mesas de trabajo.	A.6.4
	Verificar la implementación de los controles físicos del Sistema de Gestión de Seguridad de la Información (SGSI), conforme al Anexo A de la ISO/IEC	Verificación del estado de implementación de los controles de personas aplicables a los Procesos Gestión de TIC.	Documento maestro de los lineamientos del Modelo de Seguridad y Privacidad de la Información - Versión 5 (21/04/2025). Autodiagnóstico MSPI.	Plazo: Primer Trimestre. Evidencia: Acta de reunión de la mesa de trabajo con el proceso, que soporta la verificación de la implementación de los controles organizacionales	A.7.7 y A.7.13

ESTRATEGIA/EJE	METAS	RESULTADOS	INSTRUMENTO	SEGUIMIENTOS Y MONITOREO	CONTROLES
	27001:2022, mediante mesas de trabajo articuladas con los procesos, con el fin de identificar el nivel de cumplimiento, brechas y oportunidades de mejora.			del Anexo A de la ISO/IEC 27001:2022 y los compromisos definidos.	
				Plazo: Cuatrimestral. Evidencia: Informe de seguimiento al cumplimiento de los compromisos establecidos en las mesas de trabajo.	
		Verificación del estado de implementación de los controles de personas aplicables a los Procesos Gestión de TIC y Gestión Administrativa.		Plazo: Primer Trimestre. Evidencia: Acta de reunión de la mesa de trabajo con el proceso, que soporta la verificación de la implementación de los controles organizacionales del Anexo A de la ISO/IEC 27001:2022 y los compromisos definidos.	A.7.1, A.7.2, A.7.3, A.7.4, A.7.6, A.7.8 y A.7.11
				Plazo: Cuatrimestral. Evidencia: Informe de seguimiento al cumplimiento de los compromisos establecidos en las mesas de trabajo.	
		Verificación del estado de implementación de los controles de personas aplicables a los Procesos Gestión de TIC y Gestión Administrativa (Seguridad y Salud en el		Plazo: Primer Trimestre. Evidencia: Acta de reunión de la mesa de trabajo con el proceso, que soporta la verificación de la implementación de los controles organizacionales	A.7.5

ESTRATEGIA/EJE	METAS	RESULTADOS	INSTRUMENTO	SEGUIMIENTOS Y MONITOREO	CONTROLES
		Trabajo).		del Anexo A de la ISO/IEC 27001:2022 y los compromisos definidos. Plazo: Cuatrimestral. Evidencia: Informe de seguimiento al cumplimiento de los compromisos establecidos en las mesas de trabajo.	
		Verificación del estado de implementación de los controles de personas aplicables a los Procesos Gestión de TIC y Planificación del Abastecimiento (Dirección de Infraestructura).		Plazo: Primer Trimestre. Evidencia: Acta de reunión de la mesa de trabajo con el proceso, que soporta la verificación de la implementación de los controles organizacionales del Anexo A de la ISO/IEC 27001:2022 y los compromisos definidos. Plazo: Cuatrimestral. Evidencia: Informe de seguimiento al cumplimiento de los compromisos establecidos en las mesas de trabajo.	A.7.12
		Verificación del estado de implementación de los controles de personas aplicables a los Procesos Gestión de TIC y Gestión Administrativa y el grupo de Seguridad y		Plazo: Primer Trimestre. Evidencia: Acta de reunión de la mesa de trabajo con el proceso, que soporta la verificación de la implementación de los controles organizacionales	A.7.10 y A.7.14

ESTRATEGIA/EJE	METAS	RESULTADOS	INSTRUMENTO	SEGUIMIENTOS Y MONITOREO	CONTROLES
		Salud en el Trabajo.		del Anexo A de la ISO/IEC 27001:2022 y los compromisos definidos. Plazo: Cuatrimestral. Evidencia: Informe de seguimiento al cumplimiento de los compromisos establecidos en las mesas de trabajo.	
		Verificación del estado de implementación de los controles de personas aplicables a los Procesos Gestión de TIC, Gestión del Talento Humano, Gestión Administrativa y el grupo de Gestión Documental.		Plazo: Primer Trimestre. Evidencia: Acta de reunión de la mesa de trabajo con el proceso, que soporta la verificación de la implementación de los controles organizacionales del Anexo A de la ISO/IEC 27001:2022 y los compromisos definidos. Plazo: Cuatrimestral. Evidencia: Informe de seguimiento al cumplimiento de los compromisos establecidos en las mesas de trabajo.	A.7.9
	Verificar la implementación de los controles tecnológicos del Sistema de Gestión de Seguridad de la Información (SGSI), conforme al Anexo A de la ISO/IEC	Verificación del estado de implementación de los controles tecnológicos aplicables a los Procesos Gestión de TIC.	Documento maestro de los lineamientos del Modelo de Seguridad y Privacidad de la Información - Versión 5 (21/04/2025). Autodiagnóstico MSPI.	Plazo: Primer Trimestre. Evidencia: Acta de reunión de la mesa de trabajo con el proceso, que soporta la verificación de la implementación de los controles organizacionales	A.8.1, A.8.2, A.8.3, A.8.4, A.8.5, A.8.6, A.8.7, A.8.8, A.8.9, A.8.11, A.8.12, A.8.13, A.8.14, A.8.15, A.8.16, A.8.17,

ESTRATEGIA/EJE	METAS	RESULTADOS	INSTRUMENTO	SEGUIMIENTOS Y MONITOREO	CONTROLES
	27001:2022, mediante mesas de trabajo articuladas con los procesos, con el fin de identificar el nivel de cumplimiento, brechas y oportunidades de mejora.			del Anexo A de la ISO/IEC 27001:2022 y los compromisos definidos. Plazo: Cuatrimestral. Evidencia: Informe de seguimiento al cumplimiento de los compromisos establecidos en las mesas de trabajo.	A.8.18, A.8.19, A.8.20, A.8.21, A.8.22, A.8.23, A.8.24, A.8.25, A.8.26, A.8.27, A.8.28, A.8.29, A.8.30, A.8.31, A.8.32, A.8.33 y A.8.34
		Verificación del estado de implementación de los controles tecnológicos aplicables a los Procesos Gestión de TIC y Gestión Administrativa (Gestión Documental).		Plazo: Primer Trimestre. Evidencia: Acta de reunión de la mesa de trabajo con el proceso, que soporta la verificación de la implementación de los controles organizacionales del Anexo A de la ISO/IEC 27001:2022 y los compromisos definidos. Plazo: Cuatrimestral. Evidencia: Informe de seguimiento al cumplimiento de los compromisos establecidos en las mesas de trabajo.	A.8.10
Gestión de incidentes.	Prevención de eventos de seguridad informática.	Procedimientos documentados para la gestión de incidentes.	Documento maestro de los lineamientos del Modelo de Seguridad y Privacidad de la Información - Versión 5 (21/04/2025).	Plazo: Primer Cuatrimestre. Evidencia: Documento que justifica la decisión de no actualizar el Procedimiento de Seguridad de la Información o la	A.5.24, A.5.25, A.5.26, A.5.27, A.5.29, A.5.30, A.8.13

ESTRATEGIA/EJE	METAS	RESULTADOS	INSTRUMENTO	SEGUIMIENTOS Y MONITOREO	CONTROLES
				versión actualizada del mismo.	
				Plazo: Primer Semestre. Evidencia: Documento que soporte la definición de lineamientos para la gestión de incidentes de seguridad de la información.	
		Intercambiar y/o compartir con el CSIRT, COLCERT, CAIVIRUTAL, (DIJIN) y CCOCI para apoyar la gestión de riesgos y la toma de decisiones (priorización, tratamiento y aceptación, respuesta a incidentes), especialmente, para prevenir interna y externamente amenazas cibernéticas.		Plazo: Cuatrimestral. Evidencia: Soporte de los mensajes de correos electrónicos generados.	
		Informes de seguimiento a los eventos de seguridad presentados (Fortisandbox).		Plazo: Cuatrimestral. Evidencia: Informes de seguimiento eventos de seguridad.	

Nota. Definición de actividades a ejecutar establecidas por estrategia para la vigencia 2026. Proceso Gestión de TIC (Seguridad de la Información) (2026).

7. SEGUIMIENTO

A través de la herramienta Suite visión empresarial, se realizará el cargue y seguimiento a las tareas planeadas y estructuradas como se describe en la matriz de actividades anexa y de acuerdo al análisis realizado por el Profesional Defensa – Seguridad de la Información de la Oficina principal. De igual manera, a través del seguimiento mediante el instrumento de

identificación de la línea base de seguridad – Modelo de Seguridad y Privacidad de la Información – MSPI 2026.

8. ANÁLISIS Y MEDICIÓN

El análisis y medición de la ejecución del Plan Estratégico de Seguridad y Privacidad de la Información (PESI) estará cargo de la Jefatura de la Oficina TIC. En atención al 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", en su artículo 1. Adicionar al Capítulo 3 del Título 22 de la Parte 2 del Libro 2 del Decreto 1083 de 2015, Único Reglamentario del Sector de Función Pública, los siguientes artículos "2.2.22.3.14. Integración de los planes institucionales y estratégicos al Plan de Acción; las entidades del Estado, de acuerdo con el ámbito de aplicación del Modelo Integrado de Planeación y Gestión, al Plan de Acción de que trata el artículo 74 de la Ley 1474 de 2011, deberán integrar los planes institucionales y estratégicos…"; por lo consiguiente, de acuerdo con mesas de trabajo adelantadas se realizará la articulación del: Plan Estratégico de Seguridad y Privacidad de la Información (PESI) a través de informes trimestrales de avance a su cumplimiento.

ANEXO

TAREAS	EVIDENCIA / ENTREGABLE	Fecha Inicio (día-mes-año)	Fecha Fin (día-mes-año)	Dependencia Responsable	Proceso Asociado	Responsable de documentar y registrar la Tarea en la SVE	Responsable de revisar la Tarea (en caso que se requiera)	Responsable de Aprobar la Tarea en la SVE
Implementación MSPI. Análisis GAP para identificar el estado actual de la entidad en relación con la adopción del MSPI.	Informe del análisis GAP realizado - Soporte de divulgación a la Alta Dirección y partes interesadas.	01/02/2026	06/03/2026	Oficina Tecnologías de la Información y las Comunicaciones.	Proceso Gestión de TIC.	Profesional Defensa – Seguridad de la Información.	N/A	Líder Proceso Gestión de TIC.
Plan de Gestión del Cambio del MSPI elaborado, documentado y socializado, orientado a facilitar la adopción progresiva del Modelo de Seguridad y Privacidad de la Información en la entidad.	Documento del Plan de Gestión del Cambio del MSPI - Soporte de divulgación a la Alta Dirección y partes interesadas.	01/02/2026	06/03/2026	Oficina Tecnologías de la Información y las Comunicaciones.	Proceso Gestión de TIC.	Profesional Defensa – Seguridad de la Información.	N/A	Líder Proceso Gestión de TIC.
Seguimiento periódico y documentado al avance en la implementación del MSPI en la entidad, permitiendo	Informe de seguimiento implementación MSPI, anexando el instrumento de evaluación actualizado.	01/02/2026 01/04/2026 01/07/2026 01/10/2026	10/04/2026 07/07/2026 07/10/2026 08/01/2027	Oficina Tecnologías de la Información y las Comunicaciones.	Proceso Gestión de TIC.	Profesional Defensa – Seguridad de la Información.	N/A	Líder Proceso Gestión de TIC.

TAREAS	EVIDENCIA / ENTREGABLE	Fecha Inicio (día-mes-año)	Fecha Fin (día-mes-año)	Dependencia Responsable	Proceso Asociado	Responsable de documentar y registrar la Tarea en la SVE	Responsable de revisar la Tarea (en caso que se requiera)	Responsable de Aprobar la Tarea en la SVE
verificar el nivel de cumplimiento, identificar brechas y definir acciones de mejora.								
Proceso de seguimiento, análisis y verificación de la ejecución de las actividades definidas en el Plan Estratégico de Seguridad de la Información (PESI) realizado, orientado a identificar ajustes, mejoras y/o cambios necesarios que permitan asegurar el cumplimiento de la normativa aplicable y la alineación con los objetivos estratégicos y misionales de la entidad.	Informe de Análisis y Verificación del Plan Estratégico de Seguridad de la Información (PESI).	01/01/2027	15/01/2027	Oficina Tecnologías de la Información y las Comunicaciones.	Proceso Gestión de TIC.	Profesional Defensa – Seguridad de la Información.	N/A	Líder Proceso Gestión de TIC.
Políticas,	Políticas,	01/02/2026	07/07/2026	Oficina	Proceso Gestión	Profesional	N/A	Líder Proceso

TAREAS	EVIDENCIA / ENTREGABLE	Fecha Inicio (día-mes-año)	Fecha Fin (día-mes-año)	Dependencia Responsable	Proceso Asociado	Responsable de documentar y registrar la Tarea en la SVE	Responsable de revisar la Tarea (en caso que se requiera)	Responsable de Aprobar la Tarea en la SVE
manuales y lineamientos institucionales de Seguridad y Privacidad de la Información elaborados, actualizados y gestionados, asegurando el cumplimiento normativo y la correcta adopción del MSPI en la entidad.	manuales y lineamientos institucionales de Seguridad y Privacidad de la Información actualizados y aprobados ante el SIG.	01/07/2026	08/01/2027	Tecnologías de la Información y las Comunicaciones.	de TIC.	Defensa – Seguridad de la Información.		Gestión de TIC.
Mesa de trabajo con la Oficina de Control Interno realizada y documentada, orientada a definir y acordar lineamientos claros para la revisión, evaluación y fortalecimiento continuo del MSPI.	Acta y/o registro de la mesa de trabajo realizada con la Oficina de Control Interno.	01/02/2026	06/03/2026	Oficina Tecnologías de la Información y las Comunicaciones.	Proceso Gestión de TIC. Proceso Gestión de Seguimiento y Evaluación	Profesional Defensa – Seguridad de la Información.	N/A	Líder Proceso Gestión de TIC.
Auditorías internas y/o evaluaciones de control	Informes de auditoría y/o evaluaciones de control interno	01/02/2026 01/07/2026	07/07/2026 08/01/2027	Oficina de Control Interno.	Proceso Gestión de Seguimiento y Evaluación.	Profesional Defensa – Oficina de Control Interno.	Profesional Defensa – Seguridad de la	Líder Proceso Gestión de TIC.

TAREAS	EVIDENCIA / ENTREGABLE	Fecha Inicio (día-mes-año)	Fecha Fin (día-mes-año)	Dependencia Responsable	Proceso Asociado	Responsable de documentar y registrar la Tarea en la SVE	Responsable de revisar la Tarea (en caso que se requiera)	Responsable de Aprobar la Tarea en la SVE
realizadas, con planes de mejora definidos, ejecutados y alineados con los objetivos del PESI y el MSPI.	con sus debidos soportes en caso de aplicar (Planes de acción y/o mejora derivados de los hallazgos).						Información.	
Documento de justificación elaborado sobre la vigencia o actualización de los formatos asociados al Plan de Continuidad y a las Pruebas de Recuperación.	Documento que justifica la decisión de no actualizar los formatos Evaluación Evento Activación Plan de Continuidad, Diseño y Ejecución de Pruebas de Recuperación y Evaluación Pruebas de Recuperación o las versiones actualizadas del mismo.	01/02/2026	10/04/2026	Oficina Tecnologías de la Información y las Comunicaciones.	Proceso Gestión de TIC.	Profesional Defensa – Seguridad de la Información.	N/A	Líder Proceso Gestión de TIC.
Revisar, actualizar y ajustar el Plan Maestro de Continuidad y Gestión de Crisis, garantizando su	Plan Maestro de Continuidad y Gestión de Crisis actualizado y ajustado.	01/02/2026	10/04/2026	Oficina Tecnologías de la Información y las Comunicaciones.	Proceso Gestión de TIC.	Profesional Defensa – Seguridad de la Información.	N/A	Líder Proceso Gestión de TIC.

TAREAS	EVIDENCIA / ENTREGABLE	Fecha Inicio (día-mes-año)	Fecha Fin (día-mes-año)	Dependencia Responsable	Proceso Asociado	Responsable de documentar y registrar la Tarea en la SVE	Responsable de revisar la Tarea (en caso que se requiera)	Responsable de Aprobar la Tarea en la SVE
coherencia con el MSPI, la normativa vigente y las necesidades institucionales.								
Seguimiento a la gestión del Plan Maestro de Continuidad y Gestión de Crisis de la ALFM.	Informes de seguimiento al cumplimiento de las actividades definidas en el Plan Maestro de Continuidad y Gestión de Crisis, con sus respectivos soportes.	01/02/2026 01/07/2026	07/07/2026 08/01/2027	Oficina Tecnologías de la Información y las Comunicaciones.	Proceso Gestión de TIC.	Profesional Defensa – Seguridad de la Información.	N/A	Líder Proceso Gestión de TIC.
Seguimiento al estado avance del Plan de tratamiento de riesgos de seguridad y privacidad de la información.	Informe de seguimiento al cumplimiento de actividades establecidas, mediante el Plan de Tratamiento de Riesgos de seguridad y Privacidad de la Información.	01/02/2026 01/05/2026 01/09/2026	08/05/2026 07/09/2026 08/01/2027	Oficina Tecnologías de la Información y las Comunicaciones.	Proceso Gestión de TIC.	Profesional Defensa – Seguridad de la Información.	N/A	Líder Proceso Gestión de TIC.
Plan de actividades de sensibilización y concientización en temas	Plan de sensibilización y capacitación a los funcionarios de la ALFM.	01/02/2026	06/03/2026	Oficina Tecnologías de la Información y las Comunicaciones.	Proceso Gestión de TIC.	Profesional Defensa – Seguridad de la Información.	N/A	Líder Proceso Gestión de TIC.

TAREAS	EVIDENCIA / ENTREGABLE	Fecha Inicio (día-mes-año)	Fecha Fin (día-mes-año)	Dependencia Responsable	Proceso Asociado	Responsable de documentar y registrar la Tarea en la SVE	Responsable de revisar la Tarea (en caso que se requiera)	Responsable de Aprobar la Tarea en la SVE
relacionados a seguridad y privacidad de la información dirigido a todos los funcionarios de la entidad. (Elaboración del Plan).								
Plan de actividades de sensibilización y concientización en temas relacionados a seguridad y privacidad de la información dirigido a todos los funcionarios de la entidad. (Informes de seguimiento).	Informes de seguimiento a la ejecución del plan de actividades de sensibilización y concientización.	01/02/2026 01/07/2026	07/07/2026 08/01/2027	Oficina Tecnologías de la Información y las Comunicaciones.	Proceso Gestión de TIC.	Profesional Defensa – Seguridad de la Información.	N/A	Líder Proceso Gestión de TIC.
Verificación del estado de implementación de los controles organizacionales aplicables al Proceso Gestión de TIC. (Acta de reunión mesa de trabajo).	Acta de reunión de la mesa de trabajo con el proceso, que soporta la verificación de la implementación de los controles organizacionales del Anexo A de la	01/02/2026	10/04/2026	Oficina Tecnologías de la Información y las Comunicaciones.	Proceso Gestión de TIC.	Profesional Defensa – Seguridad de la Información.	N/A	Líder Proceso Gestión de TIC.

TAREAS	EVIDENCIA / ENTREGABLE	Fecha Inicio (día-mes-año)	Fecha Fin (día-mes-año)	Dependencia Responsable	Proceso Asociado	Responsable de documentar y registrar la Tarea en la SVE	Responsable de revisar la Tarea (en caso que se requiera)	Responsable de Aprobar la Tarea en la SVE
	ISO/IEC 27001:2022 y los compromisos definidos.							
Verificación del estado de implementación de los controles organizacionales aplicables al Proceso Gestión de TIC. (Informes de seguimiento compromisos acta de reunión mesa de trabajo).	Informe de seguimiento al cumplimiento de los compromisos establecidos en las mesas de trabajo.	01/02/2026 01/05/2026 01/09/2026	08/05/2026 07/09/2026 08/01/2027	Oficina Tecnologías de la Información y las Comunicaciones.	Proceso Gestión de TIC.	Profesional Defensa – Seguridad de la Información.	N/A	Líder Proceso Gestión de TIC.
Verificación del estado de implementación de los controles organizacionales aplicables a los Procesos Gestión de TIC y Desarrollo Organizacional y Gestión Integral. (Acta de reunión mesa de trabajo).	Acta de reunión de la mesa de trabajo con el proceso, que soporta la verificación de la implementación de los controles organizacionales del Anexo A de la ISO/IEC 27001:2022 y los compromisos definidos.	01/01/2026	10/04/2026	Oficina Tecnologías de la Información y las Comunicaciones.	Proceso Gestión de TIC. Proceso Desarrollo Organizacional y Gestión Integral.	Profesional Defensa – Seguridad de la Información.	N/A	Líder Proceso Gestión de TIC.
Verificación del estado de implementación	Informe de seguimiento al cumplimiento de	01/02/2026 01/05/2026 01/09/2026	08/05/2026 07/09/2026 08/01/2027	Oficina Tecnologías de la Información y las	Proceso Gestión de TIC.	Profesional Defensa – Seguridad de la	N/A	Líder Proceso Gestión de TIC.

TAREAS	EVIDENCIA / ENTREGABLE	Fecha Inicio (día-mes-año)	Fecha Fin (día-mes-año)	Dependencia Responsable	Proceso Asociado	Responsable de documentar y registrar la Tarea en la SVE	Responsable de revisar la Tarea (en caso que se requiera)	Responsable de Aprobar la Tarea en la SVE
de los controles organizacionales aplicables a los Procesos Gestión de TIC y Desarrollo Organizacional y Gestión Integral. (Informes de seguimiento compromisos acta de reunión mesa de trabajo).	los compromisos establecidos en las mesas de trabajo.			Comunicaciones.	Proceso Desarrollo Organizacional y Gestión Integral.	Información.		
Verificación del estado de implementación de los controles organizacionales aplicables a los Procesos Gestión de TIC y Gestión de la Contratación. (Acta de reunión mesa de trabajo).	Acta de reunión de la mesa de trabajo con el proceso, que soporta la verificación de la implementación de los controles organizacionales del Anexo A de la ISO/IEC 27001:2022 y los compromisos definidos.	01/02/2026	10/04/2026	Oficina Tecnologías de la Información y las Comunicaciones.	Proceso Gestión de TIC. Proceso Gestión de la Contratación.	Profesional Defensa – Seguridad de la Información.	N/A	Líder Proceso Gestión de TIC.
Verificación del estado de implementación de los controles organizacionales aplicables a los	Informe de seguimiento al cumplimiento de los compromisos establecidos en las mesas de	01/02/2026 01/05/2026 01/09/2026	08/05/2026 07/09/2026 08/01/2027	Oficina Tecnologías de la Información y las Comunicaciones.	Proceso Gestión de TIC. Proceso Gestión de la Contratación.	Profesional Defensa – Seguridad de la Información.	N/A	Líder Proceso Gestión de TIC.

TAREAS	EVIDENCIA / ENTREGABLE	Fecha Inicio (día-mes-año)	Fecha Fin (día-mes-año)	Dependencia Responsable	Proceso Asociado	Responsable de documentar y registrar la Tarea en la SVE	Responsable de revisar la Tarea (en caso que se requiera)	Responsable de Aprobar la Tarea en la SVE
Procesos Gestión de TIC y Gestión de la Contratación. (Informes de seguimiento compromisos acta de reunión mesa de trabajo).	trabajo.							
Verificación del estado de implementación de los controles organizacionales aplicables a los Procesos Gestión de TIC y Gestión Administrativa (Grupo Gestión Documental). (Acta de reunión mesa de trabajo).	Acta de reunión de la mesa de trabajo con el proceso, que soporta la verificación de la implementación de los controles organizacionales del Anexo A de la ISO/IEC 27001:2022 y los compromisos definidos.	01/02/2026	10/04/2026	Oficina Tecnologías de la Información y las Comunicaciones.	Proceso Gestión de TIC. Proceso Gestión Administrativa.	Profesional Defensa – Seguridad de la Información.	N/A	Líder Proceso Gestión de TIC.
Verificación del estado de implementación de los controles organizacionales aplicables a los Procesos Gestión de TIC y Gestión Administrativa (Grupo Gestión	Informe de seguimiento al cumplimiento de los compromisos establecidos en las mesas de trabajo.	01/02/2026 01/05/2026 01/09/2026	08/05/2026 07/09/2026 08/01/2027	Oficina Tecnologías de la Información y las Comunicaciones.	Proceso Gestión de TIC. Proceso Gestión Administrativa.	Profesional Defensa – Seguridad de la Información.	N/A	Líder Proceso Gestión de TIC.

TAREAS	EVIDENCIA / ENTREGABLE	Fecha Inicio (día-mes-año)	Fecha Fin (día-mes-año)	Dependencia Responsable	Proceso Asociado	Responsable de documentar y registrar la Tarea en la SVE	Responsable de revisar la Tarea (en caso que se requiera)	Responsable de Aprobar la Tarea en la SVE
Documental). (Informes de seguimiento compromisos acta de reunión mesa de trabajo).								
Verificación del estado de implementación de los controles organizacionales aplicables a los Procesos Gestión de TIC y Gestión de Seguimiento y Evaluación. (Acta de reunión mesa de trabajo).	Acta de reunión de la mesa de trabajo con el proceso, que soporta la verificación de la implementación de los controles organizacionales del Anexo A de la ISO/IEC 27001:2022 y los compromisos definidos.	01/02/2026	10/04/2026	Oficina Tecnologías de la Información y las Comunicaciones.	Proceso Gestión de TIC. Proceso Gestión de Seguimiento y Evaluación.	Profesional Defensa – Seguridad de la Información.	N/A	Líder Proceso Gestión de TIC.
Verificación del estado de implementación de los controles organizacionales aplicables a los Procesos Gestión de TIC y Gestión de Seguimiento y Evaluación. (Informes de seguimiento compromisos	Informe de seguimiento al cumplimiento de los compromisos establecidos en las mesas de trabajo.	01/02/2026 01/05/2026 01/09/2026	08/05/2026 07/09/2026 08/01/2027	Oficina Tecnologías de la Información y las Comunicaciones.	Proceso Gestión de TIC. Proceso Gestión de Seguimiento y Evaluación.	Profesional Defensa – Seguridad de la Información.	N/A	Líder Proceso Gestión de TIC.

TAREAS	EVIDENCIA / ENTREGABLE	Fecha Inicio (día-mes-año)	Fecha Fin (día-mes-año)	Dependencia Responsable	Proceso Asociado	Responsable de documentar y registrar la Tarea en la SVE	Responsable de revisar la Tarea (en caso que se requiera)	Responsable de Aprobar la Tarea en la SVE
acta de reunión mesa de trabajo).								
Verificación del estado de implementación de los controles organizacionales aplicables a los Procesos Gestión de TIC, Desarrollo Organizacional y Gestión Integral y Gestión de la Contratación. (Acta de reunión mesa de trabajo).	Acta de reunión de la mesa de trabajo con el proceso, que soporta la verificación de la implementación de los controles organizacionales del Anexo A de la ISO/IEC 27001:2022 y los compromisos definidos.	01/02/2026	10/04/2026	Oficina Tecnologías de la Información y las Comunicaciones.	Proceso Gestión de TIC. Proceso Desarrollo Organizacional y Gestión Integral. Proceso Gestión de la Contratación.	Profesional Defensa – Seguridad de la Información.	N/A	Líder Proceso Gestión de TIC.
Verificación del estado de implementación de los controles organizacionales aplicables a los Procesos Gestión de TIC, Desarrollo Organizacional y Gestión Integral y Gestión de la Contratación. (Informes de seguimiento compromisos	Informe de seguimiento al cumplimiento de los compromisos establecidos en las mesas de trabajo.	01/02/2026 01/05/2026 01/09/2026	08/05/2026 07/09/2026 08/01/2027	Oficina Tecnologías de la Información y las Comunicaciones.	Proceso Gestión de TIC. Proceso Desarrollo Organizacional y Gestión Integral. Proceso Gestión de la Contratación.	Profesional Defensa – Seguridad de la Información.	N/A	Líder Proceso Gestión de TIC.

TAREAS	EVIDENCIA / ENTREGABLE	Fecha Inicio (día-mes-año)	Fecha Fin (día-mes-año)	Dependencia Responsable	Proceso Asociado	Responsable de documentar y registrar la Tarea en la SVE	Responsable de revisar la Tarea (en caso que se requiera)	Responsable de Aprobar la Tarea en la SVE
acta de reunión mesa de trabajo).								
Verificación del estado de implementación de los controles organizacionales aplicables a los Procesos Gestión de TIC, Gestión Administrativa (Grupo Gestión Documental) y Gestión de la Contratación. (Acta de reunión mesa de trabajo).	Acta de reunión de la mesa de trabajo con el proceso, que soporta la verificación de la implementación de los controles organizacionales del Anexo A de la ISO/IEC 27001:2022 y los compromisos definidos.	01/02/2026	10/04/2026	Oficina Tecnologías de la Información y las Comunicaciones.	Proceso Gestión de TIC. Proceso Gestión Administrativa. Proceso Gestión de la Contratación.	Profesional Defensa – Seguridad de la Información.	N/A	Líder Proceso Gestión de TIC.
Verificación del estado de implementación de los controles organizacionales aplicables a los Procesos Gestión de TIC, Gestión Administrativa (Grupo Gestión Documental) y Gestión de la Contratación. (Informes de seguimiento compromisos	Informe de seguimiento al cumplimiento de los compromisos establecidos en las mesas de trabajo.	01/02/2026 01/05/2026 01/09/2026	08/05/2026 07/09/2026 08/01/2027	Oficina Tecnologías de la Información y las Comunicaciones.	Proceso Gestión de TIC. Proceso Gestión Administrativa. Proceso Gestión de la Contratación.	Profesional Defensa – Seguridad de la Información.	N/A	Líder Proceso Gestión de TIC.

TAREAS	EVIDENCIA / ENTREGABLE	Fecha Inicio (día-mes-año)	Fecha Fin (día-mes-año)	Dependencia Responsable	Proceso Asociado	Responsable de documentar y registrar la Tarea en la SVE	Responsable de revisar la Tarea (en caso que se requiera)	Responsable de Aprobar la Tarea en la SVE
acta de reunión mesa de trabajo).								
Verificación del estado de implementación de los controles organizacionales aplicables a los Procesos Gestión de TIC, Gestión de Talento Humano y Gestión Administrativa. (Acta de reunión mesa de trabajo).	Acta de reunión de la mesa de trabajo con el proceso, que soporta la verificación de la implementación de los controles organizacionales del Anexo A de la ISO/IEC 27001:2022 y los compromisos definidos.	01/02/2026	10/04/2026	Oficina Tecnologías de la Información y las Comunicaciones.	Proceso Gestión de TIC. Proceso Gestión de Talento Humano. Proceso Gestión Administrativa.	Profesional Defensa – Seguridad de la Información.	N/A	Líder Proceso Gestión de TIC.
Verificación del estado de implementación de los controles organizacionales aplicables a los Procesos Gestión de TIC, Gestión de Talento Humano y Gestión Administrativa. (Informes de seguimiento compromisos acta de reunión mesa de trabajo).	Informe de seguimiento al cumplimiento de los compromisos establecidos en las mesas de trabajo.	01/02/2026 01/05/2026 01/09/2026	08/05/2026 07/09/2026 08/01/2027	Oficina Tecnologías de la Información y las Comunicaciones.	Proceso Gestión de TIC. Proceso Gestión de Talento Humano. Proceso Gestión Administrativa.	Profesional Defensa – Seguridad de la Información.	N/A	Líder Proceso Gestión de TIC.

TAREAS	EVIDENCIA / ENTREGABLE	Fecha Inicio (día-mes-año)	Fecha Fin (día-mes-año)	Dependencia Responsable	Proceso Asociado	Responsable de documentar y registrar la Tarea en la SVE	Responsable de revisar la Tarea (en caso que se requiera)	Responsable de Aprobar la Tarea en la SVE
Verificación del estado de implementación de los controles organizacionales aplicables a los Procesos Gestión de TIC, Gestión de Innovación y Redes de Valor (Grupo de Atención y Orientación Ciudadana), Talento Humano, Gestión Administrativa y Gestión de la Contratación. (Acta de reunión mesa de trabajo).	Acta de reunión de la mesa de trabajo con el proceso, que soporta la verificación de la implementación de los controles organizacionales del Anexo A de la ISO/IEC 27001:2022 y los compromisos definidos.	01/01/2026	10/04/2026	Oficina Tecnologías de la Información y las Comunicaciones.	Proceso Gestión de TIC. Proceso Gestión de Innovación y Redes de Valor. Proceso Gestión de Talento Humano. Proceso Gestión Administrativa. Proceso Gestión de la Contratación.	Profesional Defensa – Seguridad de la Información.	N/A	Líder Proceso Gestión de TIC.
Verificación del estado de implementación de los controles organizacionales aplicables a los Procesos Gestión de TIC, Gestión de Innovación y Redes de Valor (Grupo de Atención y	Informe de seguimiento al cumplimiento de los compromisos establecidos en las mesas de trabajo.	01/02/2026 01/05/2026 01/09/2026	08/05/2026 07/09/2026 08/01/2027	Oficina Tecnologías de la Información y las Comunicaciones.	Proceso Gestión de TIC. Proceso Gestión de Innovación y Redes de Valor. Proceso Gestión de Talento Humano. Proceso Gestión	Profesional Defensa – Seguridad de la Información.	N/A	Líder Proceso Gestión de TIC.

TAREAS	EVIDENCIA / ENTREGABLE	Fecha Inicio (día-mes-año)	Fecha Fin (día-mes-año)	Dependencia Responsable	Proceso Asociado	Responsable de documentar y registrar la Tarea en la SVE	Responsable de revisar la Tarea (en caso que se requiera)	Responsable de Aprobar la Tarea en la SVE
Orientación Ciudadana), Talento Humano, Gestión Administrativa y Gestión de la Contratación. (Informes de seguimiento compromisos acta de reunión mesa de trabajo).					Administrativa. Proceso Gestión de la Contratación.			
Verificación del estado de implementación de los controles de personas aplicables a los Procesos Gestión de TIC. (Acta de reunión mesa de trabajo).	Acta de reunión de la mesa de trabajo con el proceso, que soporta la verificación de la implementación de los controles de personas del Anexo A de la ISO/IEC 27001:2022 y los compromisos definidos.	01/02/2026	10/04/2026	Oficina Tecnologías de la Información y las Comunicaciones.	Proceso Gestión de TIC.	Profesional Defensa – Seguridad de la Información.	N/A	Líder Proceso Gestión de TIC.
Verificación del estado de implementación de los controles de personas aplicables a los Procesos Gestión	Informe de seguimiento al cumplimiento de los compromisos establecidos en las mesas de trabajo.	01/02/2026 01/05/2026 01/09/2026	08/05/2026 07/09/2026 08/01/2027	Oficina Tecnologías de la Información y las Comunicaciones.	Proceso Gestión de TIC.	Profesional Defensa – Seguridad de la Información.	N/A	Líder Proceso Gestión de TIC.

TAREAS	EVIDENCIA / ENTREGABLE	Fecha Inicio (día-mes-año)	Fecha Fin (día-mes-año)	Dependencia Responsable	Proceso Asociado	Responsable de documentar y registrar la Tarea en la SVE	Responsable de revisar la Tarea (en caso que se requiera)	Responsable de Aprobar la Tarea en la SVE
de TIC. (Informes de seguimiento compromisos acta de reunión mesa de trabajo).								
Verificación del estado de implementación de los controles de personas aplicables a los Procesos Gestión de TIC y Gestión del Talento Humano. (Acta de reunión mesa de trabajo).	Acta de reunión de la mesa de trabajo con el proceso, que soporta la verificación de la implementación de los controles de personas del Anexo A de la ISO/IEC 27001:2022 y los compromisos definidos.	01/02/2026	10/04/2026	Oficina Tecnologías de la Información y las Comunicaciones.	Proceso Gestión de TIC. Proceso Gestión del Talento Humano.	Profesional Defensa – Seguridad de la Información.	N/A	Líder Proceso Gestión de TIC.
Verificación del estado de implementación de los controles de personas aplicables a los Procesos Gestión de TIC y Gestión del Talento Humano. (Informes de seguimiento compromisos acta de reunión	Informe de seguimiento al cumplimiento de los compromisos establecidos en las mesas de trabajo.	01/02/2026 01/05/2026 01/09/2026	08/05/2026 07/09/2026 08/01/2027	Oficina Tecnologías de la Información y las Comunicaciones.	Proceso Gestión de TIC. Proceso Gestión del Talento Humano.	Profesional Defensa – Seguridad de la Información.	N/A	Líder Proceso Gestión de TIC.

TAREAS	EVIDENCIA / ENTREGABLE	Fecha Inicio (día-mes-año)	Fecha Fin (día-mes-año)	Dependencia Responsable	Proceso Asociado	Responsable de documentar y registrar la Tarea en la SVE	Responsable de revisar la Tarea (en caso que se requiera)	Responsable de Aprobar la Tarea en la SVE
mesa de trabajo).								
Verificación del estado de implementación de los controles de personas aplicables a los Procesos Gestión de TIC, Gestión del Talento Humano y Gestión de la Contratación. (Acta de reunión mesa de trabajo).	Acta de reunión de la mesa de trabajo con el proceso, que soporta la verificación de la implementación de los controles de personas del Anexo A de la ISO/IEC 27001:2022 y los compromisos definidos.	01/02/2026	10/04/2026	Oficina Tecnologías de la Información y las Comunicaciones.	Proceso Gestión de TIC. Proceso Gestión del Talento Humano. Proceso Gestión de la Contratación.	Profesional Defensa – Seguridad de la Información.	N/A	Líder Proceso Gestión de TIC.
Verificación del estado de implementación de los controles de personas aplicables a los Procesos Gestión de TIC, Gestión del Talento Humano y Gestión de la Contratación. (Informes de seguimiento compromisos acta de reunión mesa de trabajo).	Informe de seguimiento al cumplimiento de los compromisos establecidos en las mesas de trabajo.	01/02/2026 01/05/2026 01/09/2026	08/05/2026 07/09/2026 08/01/2027	Oficina Tecnologías de la Información y las Comunicaciones.	Proceso Gestión de TIC. Proceso Gestión del Talento Humano. Proceso Gestión de la Contratación.	Profesional Defensa – Seguridad de la Información.	N/A	Líder Proceso Gestión de TIC.
Verificación del	Acta de reunión	01/02/2026	10/04/2026	Oficina	Proceso Gestión	Profesional	N/A	Líder Proceso

TAREAS	EVIDENCIA / ENTREGABLE	Fecha Inicio (día-mes-año)	Fecha Fin (día-mes-año)	Dependencia Responsable	Proceso Asociado	Responsable de documentar y registrar la Tarea en la SVE	Responsable de revisar la Tarea (en caso que se requiera)	Responsable de Aprobar la Tarea en la SVE
estado de implementación de los controles de personas aplicables a los Procesos Gestión de TIC, Gestión del Talento Humano (Oficina Control Interno Disciplinario) y Gestión de la Contratación. (Acta de reunión mesa de trabajo).	de la mesa de trabajo con el proceso, que soporta la verificación de la implementación de los controles de personas del Anexo A de la ISO/IEC 27001:2022 y los compromisos definidos.			Tecnologías de la Información y las Comunicaciones.	de TIC. Proceso Gestión del Talento Humano. Proceso Gestión de la Contratación.	Defensa – Seguridad de la Información.		Gestión de TIC.
Verificación del estado de implementación de los controles de personas aplicables a los Procesos Gestión de TIC, Gestión del Talento Humano (Oficina Control Interno Disciplinario) y Gestión de la Contratación. (Informes de seguimiento compromisos acta de reunión	Informe de seguimiento al cumplimiento de los compromisos establecidos en las mesas de trabajo.	01/02/2026 01/05/2026 01/09/2026	08/05/2026 07/09/2026 08/01/2027	Oficina Tecnologías de la Información y las Comunicaciones.	Proceso Gestión de TIC. Proceso Gestión del Talento Humano. Proceso Gestión de la Contratación.	Profesional Defensa – Seguridad de la Información.	N/A	Líder Proceso Gestión de TIC.

TAREAS	EVIDENCIA / ENTREGABLE	Fecha Inicio (día-mes-año)	Fecha Fin (día-mes-año)	Dependencia Responsable	Proceso Asociado	Responsable de documentar y registrar la Tarea en la SVE	Responsable de revisar la Tarea (en caso que se requiera)	Responsable de Aprobar la Tarea en la SVE
mesa de trabajo).								
Verificación del estado de implementación de los controles físicos aplicables a los Procesos Gestión de TIC. (Acta de reunión mesa de trabajo).	Acta de reunión de la mesa de trabajo con el proceso, que soporta la verificación de la implementación de los controles de personas del Anexo A de la ISO/IEC 27001:2022 y los compromisos definidos.	01/02/2026	10/04/2026	Oficina Tecnologías de la Información y las Comunicaciones.	Proceso Gestión de TIC.	Profesional Defensa – Seguridad de la Información.	N/A	Líder Proceso Gestión de TIC.
Verificación del estado de implementación de los controles físicos aplicables a los Procesos Gestión de TIC. (Informes de seguimiento compromisos acta de reunión mesa de trabajo).	Informe de seguimiento al cumplimiento de los compromisos establecidos en las mesas de trabajo.	01/02/2026 01/05/2026 01/09/2026	08/05/2026 07/09/2026 08/01/2027	Oficina Tecnologías de la Información y las Comunicaciones.	Proceso Gestión de TIC.	Profesional Defensa – Seguridad de la Información.	N/A	Líder Proceso Gestión de TIC.
Verificación del estado de implementación de los controles físicos aplicables a los Procesos	Acta de reunión de la mesa de trabajo con el proceso, que soporta la verificación de la	01/01/2026	10/04/2026	Oficina Tecnologías de la Información y las Comunicaciones.	Proceso Gestión de TIC. Proceso Gestión Administrativa.	Profesional Defensa – Seguridad de la Información.	N/A	Líder Proceso Gestión de TIC.

TAREAS	EVIDENCIA / ENTREGABLE	Fecha Inicio (día-mes-año)	Fecha Fin (día-mes-año)	Dependencia Responsable	Proceso Asociado	Responsable de documentar y registrar la Tarea en la SVE	Responsable de revisar la Tarea (en caso que se requiera)	Responsable de Aprobar la Tarea en la SVE
Gestión de TIC y Gestión Administrativa. (Acta de reunión mesa de trabajo).	implementación de los controles de personas del Anexo A de la ISO/IEC 27001:2022 y los compromisos definidos.							
Verificación del estado de implementación de los controles físicos aplicables a los Procesos Gestión de TIC y Gestión Administrativa. (Informes de seguimiento compromisos acta de reunión mesa de trabajo).	Informe de seguimiento al cumplimiento de los compromisos establecidos en las mesas de trabajo.	01/02/2026 01/05/2026 01/09/2026	08/05/2026 07/09/2026 08/01/2027	Oficina Tecnologías de la Información y las Comunicaciones.	Proceso Gestión de TIC. Proceso Gestión Administrativa.	Profesional Defensa – Seguridad de la Información.	N/A	Líder Proceso Gestión de TIC.
Verificación del estado de implementación de los controles físicos aplicables a los Procesos Gestión de TIC y Gestión Administrativa (Seguridad y Salud en el	Acta de reunión de la mesa de trabajo con el proceso, que soporta la verificación de la implementación de los controles de personas del Anexo A de la ISO/IEC	01/01/2026	10/04/2026	Oficina Tecnologías de la Información y las Comunicaciones.	Proceso Gestión de TIC. Proceso Gestión Administrativa.	Profesional Defensa – Seguridad de la Información.	N/A	Líder Proceso Gestión de TIC.

TAREAS	EVIDENCIA / ENTREGABLE	Fecha Inicio (día-mes-año)	Fecha Fin (día-mes-año)	Dependencia Responsable	Proceso Asociado	Responsable de documentar y registrar la Tarea en la SVE	Responsable de revisar la Tarea (en caso que se requiera)	Responsable de Aprobar la Tarea en la SVE
Trabajo). (Acta de reunión mesa de trabajo).	27001:2022 y los compromisos definidos.							
Verificación del estado de implementación de los controles físicos aplicables a los Procesos Gestión de TIC y Gestión Administrativa (Seguridad y Salud en el Trabajo). (Informes de seguimiento compromisos acta de reunión mesa de trabajo).	Informe de seguimiento al cumplimiento de los compromisos establecidos en las mesas de trabajo.	01/01/2026 01/05/2026 01/09/2026	08/05/2026 07/09/2026 08/01/2027	Oficina Tecnologías de la Información y las Comunicaciones.	Proceso Gestión de TIC. Proceso Gestión Administrativa.	Profesional Defensa – Seguridad de la Información.	N/A	Líder Proceso Gestión de TIC.
Verificación del estado de implementación de los controles físicos aplicables a los Procesos Gestión de TIC y Planificación del Abastecimiento (Dirección de Infraestructura). (Acta de reunión mesa de trabajo).	Acta de reunión de la mesa de trabajo con el proceso, que soporta la verificación de la implementación de los controles de personas del Anexo A de la ISO/IEC 27001:2022 y los compromisos	01/02/2026	10/04/2026	Oficina Tecnologías de la Información y las Comunicaciones.	Proceso Gestión de TIC. Proceso Planificación del Abastecimiento.	Profesional Defensa – Seguridad de la Información.	N/A	Líder Proceso Gestión de TIC.

TAREAS	EVIDENCIA / ENTREGABLE	Fecha Inicio (día-mes-año)	Fecha Fin (día-mes-año)	Dependencia Responsable	Proceso Asociado	Responsable de documentar y registrar la Tarea en la SVE	Responsable de revisar la Tarea (en caso que se requiera)	Responsable de Aprobar la Tarea en la SVE
	definidos.							
Verificación del estado de implementación de los controles físicos aplicables a los Procesos Gestión de TIC y Planificación del Abastecimiento (Dirección de Infraestructura). (Informes de seguimiento compromisos acta de reunión mesa de trabajo).	Informe de seguimiento al cumplimiento de los compromisos establecidos en las mesas de trabajo.	01/02/2026 01/05/2026 01/09/2026	08/05/2026 07/09/2026 08/01/2027	Oficina Tecnologías de la Información y las Comunicaciones.	Proceso Gestión de TIC. Proceso Planificación del Abastecimiento.	Profesional Defensa – Seguridad de la Información.	N/A	Líder Proceso Gestión de TIC.
Verificación del estado de implementación de los controles físicos aplicables a los Procesos Gestión de TIC y Gestión Administrativa y el grupo de Seguridad y Salud en el Trabajo. (Acta de reunión mesa de trabajo).	Acta de reunión de la mesa de trabajo con el proceso, que soporta la verificación de la implementación de los controles de personas del Anexo A de la ISO/IEC 27001:2022 y los compromisos definidos.	01/02/2026	10/04/2026	Oficina Tecnologías de la Información y las Comunicaciones.	Proceso Gestión de TIC. Proceso Gestión Administrativa.	Profesional Defensa – Seguridad de la Información.	N/A	Líder Proceso Gestión de TIC.
Verificación del	Informe de	01/02/2026	08/05/2026	Oficina	Proceso Gestión	Profesional	N/A	Líder Proceso

TAREAS	EVIDENCIA / ENTREGABLE	Fecha Inicio (día-mes-año)	Fecha Fin (día-mes-año)	Dependencia Responsable	Proceso Asociado	Responsable de documentar y registrar la Tarea en la SVE	Responsable de revisar la Tarea (en caso que se requiera)	Responsable de Aprobar la Tarea en la SVE
estado de implementación de los controles físicos aplicables a los Procesos Gestión de TIC y Gestión Administrativa y el grupo de Seguridad y Salud en el Trabajo. (Informes de seguimiento compromisos acta de reunión mesa de trabajo).	seguimiento al cumplimiento de los compromisos establecidos en las mesas de trabajo.	01/05/2026 01/09/2026	07/09/2026 08/01/2027	Tecnologías de la Información y las Comunicaciones.	de TIC. Proceso Gestión Administrativa.	Defensa – Seguridad de la Información.		Gestión de TIC.
Verificación del estado de implementación de los controles físicos aplicables a los Procesos Gestión de TIC, Gestión del Talento Humano, Gestión Administrativa y el grupo de Gestión Documental. (Acta de reunión mesa de trabajo).	Acta de reunión de la mesa de trabajo con el proceso, que soporta la verificación de la implementación de los controles de personas del Anexo A de la ISO/IEC 27001:2022 y los compromisos definidos.	01/02/2026	10/04/2026	Oficina Tecnologías de la Información y las Comunicaciones.	Proceso Gestión de TIC. Proceso Gestión de Talento Humano. Proceso Gestión Administrativa.	Profesional Defensa – Seguridad de la Información.	N/A	Líder Proceso Gestión de TIC.

TAREAS	EVIDENCIA / ENTREGABLE	Fecha Inicio (día-mes-año)	Fecha Fin (día-mes-año)	Dependencia Responsable	Proceso Asociado	Responsable de documentar y registrar la Tarea en la SVE	Responsable de revisar la Tarea (en caso que se requiera)	Responsable de Aprobar la Tarea en la SVE
Verificación del estado de implementación de los controles físicos aplicables a los Procesos Gestión de TIC, Gestión del Talento Humano, Gestión Administrativa y el grupo de Gestión Documental. (Informes de seguimiento compromisos acta de reunión mesa de trabajo).	Informe de seguimiento al cumplimiento de los compromisos establecidos en las mesas de trabajo.	01/02/2026 01/05/2026 01/09/2026	08/05/2026 07/09/2026 08/01/2027	Oficina Tecnologías de la Información y las Comunicaciones.	Proceso Gestión de TIC. Proceso Gestión de Talento Humano. Proceso Gestión Administrativa.	Profesional Defensa – Seguridad de la Información.	N/A	Líder Proceso Gestión de TIC.
Verificación del estado de implementación de los controles tecnológicos aplicables a los Procesos Gestión de TIC. (Acta de reunión mesa de trabajo).	Acta de reunión de la mesa de trabajo con el proceso, que soporta la verificación de la implementación de los controles de personas del Anexo A de la ISO/IEC 27001:2022 y los compromisos definidos.	01/02/2026	10/04/2026	Oficina Tecnologías de la Información y las Comunicaciones.	Proceso Gestión de TIC.	Profesional Defensa – Seguridad de la Información.	N/A	Líder Proceso Gestión de TIC.

TAREAS	EVIDENCIA / ENTREGABLE	Fecha Inicio (día-mes-año)	Fecha Fin (día-mes-año)	Dependencia Responsable	Proceso Asociado	Responsable de documentar y registrar la Tarea en la SVE	Responsable de revisar la Tarea (en caso que se requiera)	Responsable de Aprobar la Tarea en la SVE
Verificación del estado de implementación de los controles tecnológicos aplicables a los Procesos Gestión de TIC. (Informes de seguimiento compromisos acta de reunión mesa de trabajo).	Informe de seguimiento al cumplimiento de los compromisos establecidos en las mesas de trabajo.	01/02/2026 01/05/2026 01/09/2026	08/05/2026 07/09/2026 08/01/2027	Oficina Tecnologías de la Información y las Comunicaciones.	Proceso Gestión de TIC.	Profesional Defensa – Seguridad de la Información.	N/A	Líder Proceso Gestión de TIC.
Verificación del estado de implementación de los controles tecnológicos aplicables a los Procesos Gestión de TIC y Gestión Administrativa (Gestión Documental). (Acta de reunión mesa de trabajo).	Acta de reunión de la mesa de trabajo con el proceso, que soporta la verificación de la implementación de los controles de personas del Anexo A de la ISO/IEC 27001:2022 y los compromisos definidos.	01/02/2026	10/04/2026	Oficina Tecnologías de la Información y las Comunicaciones.	Proceso Gestión de TIC. Proceso Gestión Administrativa.	Profesional Defensa – Seguridad de la Información.	N/A	Líder Proceso Gestión de TIC.
Verificación del estado de implementación de los controles tecnológicos aplicables a los Procesos Gestión	Informe de seguimiento al cumplimiento de los compromisos establecidos en las mesas de trabajo.	01/02/2026 01/05/2026 01/09/2026	08/05/2026 07/09/2026 08/01/2027	Oficina Tecnologías de la Información y las Comunicaciones.	Proceso Gestión de TIC. Proceso Gestión Administrativa.	Profesional Defensa – Seguridad de la Información.	N/A	Líder Proceso Gestión de TIC.

TAREAS	EVIDENCIA / ENTREGABLE	Fecha Inicio (día-mes-año)	Fecha Fin (día-mes-año)	Dependencia Responsable	Proceso Asociado	Responsable de documentar y registrar la Tarea en la SVE	Responsable de revisar la Tarea (en caso que se requiera)	Responsable de Aprobar la Tarea en la SVE
de TIC y Gestión Administrativa (Gestión Documental). (Informes de seguimiento compromisos acta de reunión mesa de trabajo).								
Procedimientos documentados para la gestión de incidentes. (Procedimiento Seguridad de la Información).	Documento que justifica la decisión de no actualizar el Procedimiento de Seguridad de la Información o la versión actualizada del mismo.	01/02/2026	08/05/2026	Oficina Tecnologías de la Información y las Comunicaciones.	Proceso Gestión de TIC.	Profesional Defensa – Seguridad de la Información.	N/A	Líder Proceso Gestión de TIC.
Procedimientos documentados para la gestión de incidentes. (Lineamientos gestión de incidentes de seguridad de la información).	Documento que soporte la definición de lineamientos para la gestión de incidentes de seguridad de la información.	01/02/2026	07/07/2026	Oficina Tecnologías de la Información y las Comunicaciones.	Proceso Gestión de TIC.	Profesional Defensa – Seguridad de la Información.	N/A	Líder Proceso Gestión de TIC.
Intercambiar y/o compartir con el CSIRT, COLCERT, CAIVIRUTAL, (DIJIN) y CCOCI	Soporte de los mensajes de correos electrónicos generados.	01/02/2026 01/05/2026 01/09/2026	08/05/2026 07/09/2026 08/01/2027	Oficina Tecnologías de la Información y las Comunicaciones.	Proceso Gestión de TIC.	Profesional Defensa – Seguridad de la Información.	N/A	Líder Proceso Gestión de TIC.

TAREAS	EVIDENCIA / ENTREGABLE	Fecha Inicio (día-mes-año)	Fecha Fin (día-mes-año)	Dependencia Responsable	Proceso Asociado	Responsable de documentar y registrar la Tarea en la SVE	Responsable de revisar la Tarea (en caso que se requiera)	Responsable de Aprobar la Tarea en la SVE
para apoyar la gestión de riesgos y la toma de decisiones (priorización, tratamiento y aceptación, respuesta a incidentes), especialmente, para prevenir interna y externamente amenazas cibernéticas.								
Informes de seguimiento a los eventos de seguridad presentados (Fortisandbox).	Informes de seguimiento eventos de seguridad.	01/02/2026 01/05/2026 01/09/2026	08/05/2026 07/09/2026 08/01/2027	Oficina Tecnologías de la Información y las Comunicaciones.	Proceso Gestión de TIC.	Profesional Defensa – Seguridad de la Información.	N/A	Líder Proceso Gestión de TIC.