PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN "PTR" – VIGENCIA 2025.

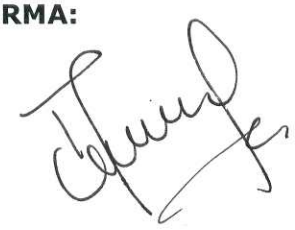
ELABORÓ	REVISÓ	APROBÓ
NOMBRE: Ing. Deiby Leandro Alvarado Rodríguez.	**NOMBRE:** Ing. Ricardo Valenzuela Díaz.	**NOMBRE:** Abog. Martha Eugenia Cortés Baquero.
CARGO: Profesional Defensa – Seguridad de la Información.	**CARGO:** Líder Proceso Gestión de Tecnologías de la Información y las Comunicaciones.	**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:**  23 01 2025

TABLA DE CONTENIDO

1. GENERALIDADES

El contexto de los riesgos en la seguridad de la información ha evolucionado significativamente. Inicialmente, los factores de riesgo se asociaban con contingencias naturales y tecnológicas. Sin embargo, con el paso del tiempo, han surgido nuevas amenazas relacionadas con el terrorismo, la inestabilidad política, las pandemias y los códigos maliciosos. Este panorama ha llevado a la entidad a adoptar una visión más integral, abarcando tanto los riesgos del mundo físico como los del entorno digital, con el fin de proteger los activos de información críticos para la operación.

El análisis de riesgos de los activos de información constituye una fase esencial para identificar posibles afectaciones a la confidencialidad, integridad y disponibilidad de la información. Este análisis permite evaluar el impacto potencial de los riesgos en los activos definidos dentro del alcance y priorizar las acciones de tratamiento necesarias. De esta forma, se garantiza una gestión más efectiva de los riesgos, promoviendo la toma de decisiones fundamentadas en la criticidad de los activos y la probabilidad de ocurrencia de las amenazas.

El Plan de Tratamiento de Riesgos de Seguridad de la Información para la vigencia 2025 se enfoca en la gestión integral de los riesgos que afectan los sistemas de información, los activos digitales y los procesos críticos de la entidad. Para ello, se aplican medidas de control y acciones que buscan reducir los riesgos identificados a niveles aceptables. Estas acciones están alineadas con la normativa aplicable, los resultados de la evaluación de riesgos de vigencias anteriores y las directrices establecidas en el Modelo de Seguridad y Privacidad de la Información (MSPI) del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC).

Este plan no solo se orienta a la mitigación de los riesgos detectados, sino que también aborda los hallazgos de auditoría interna y externa, garantizando la adopción de medidas preventivas y correctivas que contribuyan a la mejora continua de la seguridad de la información. De esta manera, se fortalece la madurez del MSPI y se mejora la eficacia de los controles establecidos. Asimismo, el plan se encuentra alineado con los lineamientos del Modelo Integrado de Planeación y Gestión (MIPG), contribuyendo al cumplimiento de la Política de Gobierno Digital y al fortalecimiento de la transformación digital segura de la entidad.

El presente plan es presentado al Comité Institucional de Gestión y Desempeño, para someterlo a su respectiva aprobación y publicación en la página web institucional; conforme al Decreto 612 de 2018.

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 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.
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.
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.
Directiva Presidencial No. 02 de 2019 (abril 02).	Simplificación de la interacción digital entre los ciudadanos y el estado.
Decreto 2106 de 2019.	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.
Ley 1952 de 2019.	Por medio de la cual se expide el código general disciplinario.
Decreto 620 de 2020	Por el cual se subroga el título 17 de la parte 2 del libro 2 del

(mayo 2).	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.
Decreto 045 de 2021 (enero 15).	Por el cual se derogan el Decreto 704 de 2018 y el artículo 1.1.2.3. del Decreto 1078 de 2015, Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.
Resolución 413 de 2021 (marzo 01).	Por la cual define el uso de las tecnologías en la nube para el sector defensa 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	Por la cual se expide el plan nacional de infraestructura de datos

2022 (febrero 15).	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 27001:2022.	Seguridad de la información, ciberseguridad y protección de la 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.

3. OBJETIVO DEL PLAN

Diseñar e implementar estrategias eficaces para el tratamiento de los riesgos de seguridad y privacidad de la información durante la vigencia 2025, enfocadas en identificar, evaluar y

mitigar los riesgos que puedan comprometer la confidencialidad, integridad y disponibilidad de los activos de información definidos en la ALFM; garantizando la implementación de controles adecuados y proporcionales a la criticidad de los activos, promoviendo el fortalecimiento de la seguridad de la información en la entidad y asegurando la continuidad de sus procesos.

3.1. OBJETIVOS ESPECIFICOS

Establecer y aplicar lineamientos integrales para la gestión de riesgos de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación en los activos de información definidos en la ALFM, garantizando la protección de la confidencialidad, integridad y disponibilidad.

Asegurar el cumplimiento de los requisitos legales y normativos aplicables, conforme a la legislación colombiana y los estándares internacionales de seguridad de la información, promoviendo la adopción de buenas prácticas de gobernanza de la información.

Gestionar los riesgos de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación, considerando los contextos internos y externos de la entidad, con un enfoque preventivo, detectivo y correctivo que permita la reducción de la exposición a riesgos críticos.

Fomentar la cultura de la gestión de riesgos mediante la sensibilización, capacitación y apropiación del conocimiento en materia de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación, asegurando la participación activa de los servidores públicos.

4. ALCANCE

El Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información (PTR) aplica de forma integral a la Agencia Logística de las Fuerzas Militares (ALFM), abarcando todas sus sedes, regionales, dependencias operativas, administrativas y de apoyo a nivel nacional, que participan en la creación, manejo, almacenamiento y transmisión de información. Este plan incluye la gestión de riesgos asociados a los activos de información identificados en la entidad, con el fin de mitigar, reducir o controlar las amenazas que puedan comprometer la confidencialidad, integridad y disponibilidad de la información.

Este plan se desarrollará de forma continua y sistemática durante la vigencia 2025, garantizando la alineación con los requisitos legales y normativos vigentes, así como con los lineamientos del Modelo de Seguridad y Privacidad de la Información (MSPI). Su implementación busca fortalecer la resiliencia de la entidad frente a amenazas potenciales, asegurando la capacidad de respuesta ante incidentes y la mejora continua de la seguridad y privacidad de los activos de información.

5. CUERPO DEL PLAN

5.1. MAPA DE RIESGOS.

5.1.1. Riesgo No. 01. Acceso no autorizado a datos sensibles.

Tabla 1.
Definición del Riesgo No. 01.

IDENTIFICACIÓN DEL RIESGO			
Riesgo		**Descripción de la materialización.**	
Posibilidad de afectación de la confidencialidad y seguridad de la información por acceso no autorizado a datos sensibles, debido a vulnerabilidades en los sistemas de seguridad y gestión inadecuada de permisos de acceso.		Este riesgo se materializa cuando hay violaciones de seguridad que permiten el acceso no autorizado a datos sensibles dentro de la entidad. Puede ocurrir mediante la explotación de vulnerabilidades en los sistemas de seguridad, la gestión inapropiada de permisos de acceso, ataques dirigidos como phishing o ingeniería social, y brechas de seguridad internas causadas por acciones de empleados malintencionados o descuidados.	
Causas (Factores)		**Efectos**	
Internos	**Externos**	**Consecuencias Potenciales**	**Beneficios Potenciales (al abordar el hallazgo)**
- Falta de actualización de roles y perfiles de acceso en sistemas de información, generando accesos no necesarios. - Configuración incorrecta de los permisos de acceso en la plataforma de gestión de usuarios (Active Directory). - Falta de revisión periódica de los accesos asignados a los usuarios, especialmente en casos de rotación de personal o cambios de roles. - Desactualización en la aplicación de parches de seguridad en sistemas críticos. - Falta de capacitación continua y adecuada para los funcionarios sobre el uso correcto de accesos y permisos, lo que puede resultar en un uso indebido o inadecuado de los privilegios de acceso a los sistemas de información.	- Exposición a ciberataques externos, como intentos de acceso no autorizado por parte de actores malintencionados. - Fallas en la integración de terceros o proveedores externos, donde se otorgan accesos temporales o permanentes sin control adecuado.	- Filtración de datos sensibles o información crítica hacia personas no autorizadas, con impacto legal y reputacional. - Pérdida de la confianza de los usuarios o clientes ante una posible violación de la privacidad de la información. - Multas o sanciones regulatorias por incumplimiento de normativas de privacidad y seguridad, como la Ley 1581 de Protección de Datos Personales. - Interrupción de la operación por la necesidad de mitigar el incidente de seguridad, afectando la continuidad de los procesos. - Aumento de costos operativos debido a la necesidad de implementar medidas correctivas o de recuperación.	- Reducción del riesgo de acceso no autorizado y exposición de información confidencial. - Cumplimiento normativo con la Ley de Protección de Datos Personales y otras normativas de seguridad. - Fortalecimiento de la confianza de usuarios y clientes en la seguridad de la información de la entidad. - Mayor eficiencia operativa al evitar incidentes de seguridad que puedan interrumpir los procesos.

ANTES DE LOS CONTROLES		
Probabilidad	**Impacto**	**Zona Inherente**
Muy Alta	**Catastrófico**	**Zona de Riesgo Extrema**
Controles		
Tipo	**Descripción**	
Preventivo	Gestión del control de acceso basada en roles y perfiles, conforme a las funciones y responsabilidades asignadas a los usuarios en cada sistema de información o plataforma tecnológica.	
Detectivo	Monitoreo y revisión periódica de los accesos a los sistemas de información para identificar patrones anómalos, inusuales o no autorizados, con el fin de detectar posibles incidentes de seguridad y garantizar el cumplimiento de las políticas de control de acceso.	
Preventivo	Aplicación periódica de parches de seguridad para corregir vulnerabilidades identificadas, asegurando que los sistemas estén protegidos contra amenazas y riesgos emergentes.	
Preventivo	Implementación de programas de sensibilización en seguridad informática y de la información, con el objetivo de fomentar la conciencia sobre las mejores prácticas de seguridad y mitigar los riesgos asociados a los activos de información.	
DESPUÉS DE LOS CONTROLES		
Probabilidad	**Impacto**	**Zona Residual**
Media	**Catastrófico**	**Zona de Riesgo Extrema**
Opción de manejo	**Riesgo Institucional**	**Riesgo de Corrupción**
Evitar el Riesgo	**SI**	**NO**

Nota. Identificación asociada al riesgo No. 01 (Acceso no autorizado a datos sensibles). Elaborado por el Proceso Gestión de TIC ALFM – 2024.

5.1.2. Riesgo No. 02. Riesgo de afectación a sistemas críticos por malware y ataques cibernéticos.

Tabla 2.
Definición del Riesgo No. 02.

IDENTIFICACIÓN DEL RIESGO			
Riesgo		**Descripción de la materialización.**	
Posible afectación integral de los sistemas críticos debido a la infiltración de malware, ataques de DDoS y explotación de vulnerabilidades en el software. Esta situación podría generar deterioro operativo, pérdida de datos, interrupción del acceso y compromiso de la seguridad informática. El riesgo se deriva de la insuficiencia de medidas de protección cibernética, la deficiente gestión de parches de seguridad y la infraestructura de red no fortalecida, en un contexto de crecimiento constante de ataques cibernéticos.		Este riesgo se materializa cuando el malware se infiltra en los sistemas críticos, ya sea por descargas inadvertidas, vulnerabilidades conocidas o ataques de DDoS. También ocurre cuando se aprovechan fallas en el software por falta de actualizaciones o medidas de protección adecuadas.	
Causas (Factores)		**Efectos**	
Internos	**Externos**	**Consecuencias Potenciales**	**Beneficios Potenciales (al abordar el hallazgo)**
- Falta de actualización oportuna de parches de seguridad en servidores, aplicaciones y dispositivos de red. - Deficiente segmentación de la red interna,	- Incremento en la sofisticación de los ataques cibernéticos (malware avanzado, ransomware, DDoS y ataques de día cero). - Presencia de actores de	- Interrupción de los sistemas críticos que afectan la operación de la entidad, con impacto en la continuidad del negocio. - Pérdida de información	- Reducción de interrupciones operativas al contar con medidas preventivas que fortalezcan la continuidad del negocio. - Mitigación de riesgos

permitiendo la propagación de amenazas internas. - Ausencia de monitoreo continuo de la red y los sistemas críticos para detectar comportamientos anómalos. - Capacidad limitada de respuesta a incidentes de ciberseguridad, lo que retrasa la contención y erradicación de ataques. - Inadecuada gestión de control de acceso y permisos excesivos a usuarios internos, facilitando la infiltración de malware.	amenazas externas (hackers, grupos APT, cibercriminales) con técnicas avanzadas de explotación de vulnerabilidades. - Dependencia de terceros y proveedores externos que pueden introducir riesgos a la infraestructura tecnológica. - Descontrol en la exposición de servicios o aplicaciones web en internet, facilitando el acceso de atacantes externos.	crítica y sensible, ya sea por corrupción de archivos, cifrado de ransomware o eliminación de datos. - Impacto financiero por costos de recuperación, pago de rescates, inversión en consultoría externa y pérdida de productividad. - Sanciones regulatorias por incumplimiento de normativas como la Ley de Protección de Datos Personales (Ley 1581) y otros requisitos legales. - Pérdida de reputación e imagen pública en caso de que el incidente sea divulgado externamente o detectado por entidades de control.	legales y regulatorios, al asegurar el cumplimiento de normativas de seguridad y protección de datos. - Disminución de costos de recuperación y tiempo de respuesta a incidentes de seguridad. - Fortalecimiento de la confianza de las partes interesadas (clientes, usuarios y organismos de control) en la seguridad de la entidad.

ANTES DE LOS CONTROLES		
Probabilidad	**Impacto**	**Zona Inherente**
Muy Alta	**Catastrófico**	**Zona de Riesgo Extrema**

Controles	
Tipo	**Descripción**
Preventivo	Aplicación periódica de parches de seguridad para corregir vulnerabilidades identificadas, asegurando que los sistemas estén protegidos contra amenazas y riesgos emergentes.
Preventivo	Segmentación de red y control de acceso, mediante la configuración de VLANs y la segmentación de la red, para aislar los sistemas críticos y protegerlos de otros entornos de la red.
Preventivo	Seguimiento de medidas de protección contra ataques DDoS mediante firewalls y sistemas de prevención de intrusiones (IPS) para mitigar posibles amenazas.
Preventivo	Análisis de vulnerabilidades: Evaluación periódica de las vulnerabilidades en el software y la infraestructura tecnológica.
Correctivo	Activación y ejecución del plan de respuesta a incidentes de ciberseguridad ante la detección de afectaciones en los sistemas críticos, con procedimientos establecidos para la contención, análisis y mitigación del impacto.
Preventivo	Implementación de programas de sensibilización en seguridad informática y de la información, con el objetivo de fomentar la conciencia sobre las mejores prácticas de seguridad y mitigar los riesgos asociados a los activos de información.
Correctivo	Aislamiento y contención de malware en sistemas infectados y cuentas comprometidas, garantizando que no se propague a otros sistemas y se minimice el impacto en la infraestructura de TI.

DESPUÉS DE LOS CONTROLES		
Probabilidad	**Impacto**	**Zona Residual**
Media	**Mayor**	**Zona de Riesgo Alta**
Opción de manejo	**Riesgo Institucional**	**Riesgo de Corrupción**
Reducir el Riesgo	**SI**	**NO**

Nota. Identificación asociada al riesgo No. 02 (Riesgo de afectación a sistemas críticos por malware y ataques cibernéticos). Elaborado por el Proceso Gestión de TIC ALFM – 2024.

5.1.3. Riesgo No. 03. Riesgo de divulgación no autorizada de información sensible por engaños.

Tabla 3.
Definición del Riesgo No. 03.

IDENTIFICACIÓN DEL RIESGO			
Riesgo		**Descripción de la materialización.**	
Posibilidad de divulgación no autorizada de información sensible como resultado de engaños a funcionarios, debido a deficiencias en la concienciación y capacitación en seguridad de la información, así como a fallos en los procedimientos de verificación de identidad y autorización de acceso.		Este riesgo se materializa cuando funcionarios divulgan información sensible debido a engaños o manipulaciones. Esto puede suceder mediante ingeniería social, phishing, manipulación psicológica o falsificación de identidad, permitiendo a los atacantes obtener acceso a contraseñas, datos confidenciales o información privilegiada al engañar a funcionarios.	
Causas (Factores)		**Efectos**	
Internos	**Externos**	**Consecuencias Potenciales**	**Beneficios Potenciales (al abordar el hallazgo)**
- Falta de capacitación continua y actualizada sobre técnicas de ingeniería social y su impacto en la divulgación de información. - Inexistencia de simulacros de ataque de ingeniería social (phishing, pretexting, baiting) para evaluar la reacción de los funcionarios. - Deficiencias en los procedimientos de verificación de identidad antes de otorgar acceso a información sensible. - Accesos excesivos o inadecuadamente asignados a usuarios internos que no requieren dicha información para sus funciones diarias. - Ausencia de una cultura de seguridad orientada a la protección de la información sensible y la identificación de señales de manipulación social.	- Incremento de ataques de ingeniería social por parte de actores externos (phishing, vishing, smishing, etc.). - Explotación de información pública de la entidad que los atacantes utilizan para personalizar sus tácticas de engaño. - Acceso no autorizado a través de terceros o contratistas con niveles de acceso innecesarios a la información. - Uso de técnicas de pretexting por parte de atacantes, quienes se hacen pasar por figuras de autoridad o soporte técnico para solicitar acceso. -	- Divulgación no autorizada de información sensible que puede afectar la confidencialidad de la información crítica. - Pérdida de confianza de los usuarios, clientes y partes interesadas, especialmente si la divulgación se hace pública. - Impacto financiero debido a posibles sanciones regulatorias (por ejemplo, la Ley 1581 de Protección de Datos Personales) y costos de contención. - Sanciones legales por incumplimiento de las normativas de seguridad y privacidad de la información. - Afectación de la reputación e imagen institucional, especialmente si la divulgación de la información compromete la relación con entidades de control. - Impacto en la continuidad operativa si la información divulgada está relacionada con procesos críticos de la	- Reducción de la exposición a ataques de ingeniería social al fortalecer la capacitación y la concienciación de los funcionarios. - Mejora de la cultura de seguridad de la información en la entidad, con mayor capacidad de los funcionarios para identificar intentos de manipulación. - Cumplimiento de la normativa de protección de datos personales (Ley 1581) y las disposiciones relacionadas con la privacidad de la información. - Fortalecimiento de los procedimientos de verificación de identidad y acceso, disminuyendo la probabilidad de errores humanos. -

		entidad.	
ANTES DE LOS CONTROLES			
Probabilidad	**Impacto**	**Zona Inherente**	
Muy Alta	**Mayor**	**Zona de Riesgo Alta**	
Controles			
Tipo	**Descripción**		
Preventivo	Implementación de programas de sensibilización en seguridad informática y de la información, con el objetivo de fomentar la conciencia sobre las mejores prácticas de seguridad y mitigar los riesgos asociados a los activos de información.		
Preventivo	Implementación de campañas de simulación de phishing para evaluar la respuesta de los usuarios, identificar conductas inseguras y fortalecer la conciencia en seguridad de la información.		
Detectivo	Monitoreo continuo de eventos de seguridad para identificar y alertar sobre accesos inusuales a la información, permitiendo una respuesta oportuna ante posibles incidentes.		
Correctivo	Aislamiento y contención de malware en sistemas infectados y cuentas comprometidas, garantizando que no se propague a otros sistemas y se minimice el impacto en la infraestructura de TI.		
Detectivo	Revisión periódica de la aplicabilidad de excepciones de seguridad informática, incluidas aquellas relacionadas con dispositivos de almacenamiento (SAN, NAS) y puertos USB, para garantizar su pertinencia y minimizar riesgos de acceso no autorizado.		
DESPUÉS DE LOS CONTROLES			
Probabilidad	**Impacto**	**Zona Residual**	
Media	**Mayor**	**Zona de Riesgo Alta**	
Opción de manejo	**Riesgo Institucional**	**Riesgo de Corrupción**	
Reducir el Riesgo	**SI**	**NO**	

Nota. Identificación asociada al riesgo No. 03 (Riesgo No. 03. Riesgo de divulgación no autorizada de información sensible por engaños). Elaborado por el Proceso Gestión de TIC ALFM – 2024.

5.1.4. Riesgo No. 04. Riesgo de exposición o sustracción no autorizada de información o dispositivos.

Tabla 4.
Definición del Riesgo No. 04.

IDENTIFICACIÓN DEL RIESGO			
Riesgo		**Descripción de la materialización.**	
Posibilidad de exposición o sustracción no autorizada de información confidencial o dispositivos tecnológicos, derivadas de deficiencias en los controles de acceso físico y digital, debido a la falta de políticas efectivas de seguridad de la información y gestión de activos.		El riesgo se materializa cuando información confidencial o dispositivos tecnológicos son expuestos o robados sin autorización debido a deficiencias en los controles de acceso físico y digital, y a la falta de políticas efectivas de seguridad de la información y gestión de activos. Esto puede ocurrir por acceso físico no autorizado a instalaciones, acceso digital no autorizado mediante explotación de vulnerabilidades, carencia de políticas de seguridad claras y gestión deficiente de activos.	
Causas (Factores)		**Efectos**	
Internos	**Externos**	**Consecuencias Potenciales**	**Beneficios Potenciales (al abordar el hallazgo)**
- Accesos físicos descontrolados a instalaciones críticas debido a la ausencia de	- Acciones malintencionadas de terceros (intrusos, atacantes, personal	- Divulgación no autorizada de información confidencial, lo que puede	- Fortalecimiento de la seguridad física y digital mediante la implementación de

sistemas de control de acceso automatizados (tarjetas de proximidad, biometría, etc.). - Falta de identificación y registro de visitantes o de personal externo que accede a las instalaciones. - Carencia de procedimientos claros para la devolución o control de dispositivos móviles y equipos portátiles (laptops, USB, discos duros externos) que contienen información confidencial. - Gestión deficiente de activos tecnológicos, incluyendo la falta de inventarios actualizados y la asignación de dispositivos sin trazabilidad. - Accesos digitales no controlados debido a una asignación inadecuada de permisos y roles de acceso en sistemas de información. - Falta de políticas de uso de dispositivos extraíbles (USB, discos externos) y de control de transferencia de archivos entre dispositivos.	externo no autorizado) que pueden sustraer dispositivos o información confidencial. - Aprovechamiento de brechas en la seguridad física (falta de vigilancia, sistemas de videovigilancia inoperantes, puertas sin cerraduras electrónicas). - Incremento en el robo de dispositivos móviles y portátiles en el contexto de trabajo híbrido o remoto. - Accesos no autorizados a sistemas de información a través de VPN o dispositivos personales no controlados. -	comprometer la privacidad de datos personales o información sensible de la entidad. - Pérdida de dispositivos tecnológicos (portátiles, USB, discos duros externos) que contengan información clave para la entidad. - Impacto en la continuidad de las operaciones por la pérdida de activos tecnológicos esenciales para la prestación de servicios. - Pérdida de confianza por parte de terceros y entidades de control, especialmente si la información divulgada se considera crítica. - Impacto económico por la necesidad de reponer activos, aplicar medidas de contención y pagar posibles sanciones regulatorias. - Incumplimiento de normativas legales de protección de datos personales (Ley 1581 de 2012) y de seguridad de la información, con el riesgo de recibir sanciones por parte de las entidades de control.	controles efectivos. - Reducción del riesgo de robo de dispositivos con la trazabilidad de los activos y la correcta asignación de responsabilidades. - Cumplimiento normativo respecto a la protección de la información y la privacidad de los datos personales. - Disminución de la probabilidad de incidentes de pérdida de información mediante la aplicación de políticas de control de dispositivos portátiles. - Mayor control sobre el acceso a instalaciones críticas que optimiza la seguridad física y evita la entrada de personas no autorizadas.

ANTES DE LOS CONTROLES		
Probabilidad	**Impacto**	**Zona Inherente**
Muy Alta	**Catastrófico**	**Zona de Riesgo Extrema**

Controles	
Tipo	**Descripción**
Preventivo	Mantener un inventario actualizado y completo de los activos de información y dispositivos, asegurando la asignación de responsables específicos para la gestión y protección de cada activo.
Preventivo	Seguimiento a los sistemas de control de acceso que utilizan autenticación biométrica, tarjetas de proximidad y/o claves únicas para garantizar el ingreso seguro a áreas críticas, como el Data Center Principal y Alterno.
Preventivo	Implementación de programas de sensibilización en seguridad informática y de la información, con el objetivo de fomentar la conciencia sobre las mejores prácticas de seguridad y mitigar los riesgos asociados a los activos de información.
Detectivo	Supervisión de la funcionalidad del Circuito Cerrado de Televisión (CCTV) y revisión de los registros de acceso físico y digital a la Entidad.
Detectivo	Monitoreo y control del acceso y salida de dispositivos externos de uso personal no institucional (portátiles) en las instalaciones de la entidad.

Detectivo	Seguimiento, control y revisión de los dispositivos externos autorizados (equipos de cómputo) que acceden a los sistemas de información a través del uso de la VPN.
Correctivo	Activación y ejecución del plan de respuesta a incidentes de ciberseguridad ante la detección de afectaciones en los sistemas críticos, con procedimientos establecidos para la contención, análisis y mitigación del impacto.
Detectivo	Revisión periódica de la aplicabilidad de excepciones de seguridad informática, incluidas aquellas relacionadas con dispositivos de almacenamiento (SAN, NAS) y puertos USB, para garantizar su pertinencia y minimizar riesgos de acceso no autorizado.

DESPUÉS DE LOS CONTROLES		
Probabilidad	**Impacto**	**Zona Residual**
Media	**Catastrófico**	**Zona de Riesgo Extrema**
Opción de manejo	**Riesgo Institucional**	**Riesgo de Corrupción**
Evitar el Riesgo	**SI**	**NO**

Nota. Identificación asociada al riesgo No. 04 (Riesgo de exposición o sustracción no autorizada de información o dispositivos). Elaborado por el Proceso Gestión de TIC ALFM – 2024.

5.1.5. Riesgo No. 05. Riesgo de pérdida irreversible de datos críticos.

Tabla 5.
Definición del Riesgo No. 05.

IDENTIFICACIÓN DEL RIESGO			
Riesgo		**Descripción de la materialización.**	
Posibilidad de pérdida irreversible de datos críticos, debido a la ausencia de procedimientos efectivos de recuperación ante desastres, derivadas de deficiencias en la implementación y mantenimiento de políticas de respaldo de información.		Este riesgo se materializa cuando la entidad enfrenta la pérdida irreversible de datos críticos debido a la falta de copias de seguridad adecuadas. Esto puede ocurrir por la carencia de políticas claras de respaldo, deficiencias en la implementación de copias de seguridad y la ausencia de procedimientos efectivos de recuperación ante desastres. Estas fallas pueden resultar en copias de seguridad irregulares o incompletas, aumentando el riesgo de pérdida de datos ante situaciones adversas como fallas técnicas, desastres o ciberataques.	
Causas (Factores)		**Efectos**	
Internos	**Externos**	**Consecuencias Potenciales**	**Beneficios Potenciales (al abordar el hallazgo)**
- Falta de una política formal de copias de seguridad (backups) que defina la frecuencia, el alcance y los mecanismos de respaldo. - Ausencia de procedimientos de recuperación ante desastres (DRP) formalizados y probados mediante simulacros o pruebas periódicas. - Carencia de un sistema de monitoreo de la integridad de los respaldos para	- Amenazas de ciberataques (ransomware) que cifran los archivos de producción y las copias de seguridad, si estas no están debidamente protegidas. - Desastres naturales (inundaciones, incendios, terremotos) que pueden destruir los centros de datos donde se almacenan las copias de respaldo si no se cuenta con una ubicación externa. - Interrupciones de la	- Pérdida permanente de información crítica que podría ser necesaria para la operación diaria o la recuperación tras un incidente. - Interrupción de los servicios esenciales de la entidad, afectando la continuidad operativa y el cumplimiento de compromisos institucionales. - Riesgo de incumplimiento normativo respecto a las obligaciones de protección de la	- Reducción del tiempo de recuperación ante incidentes mediante la implementación de un plan de recuperación ante desastres (DRP). - Mayor disponibilidad de la información y continuidad de las operaciones en caso de interrupciones inesperadas. - Cumplimiento de normativas de protección de datos y control de la seguridad de la información, evitando sanciones

garantizar que los archivos no estén corruptos ni incompletos. - Deficiencias en la automatización de los respaldos, lo que genera una alta dependencia de la intervención manual, propensa a errores humanos. - Inadecuada designación de roles y responsabilidades para la gestión de respaldos y restauraciones, lo que genera confusión o retrasos en la respuesta ante incidentes. - No actualización de la matriz de activos críticos, lo que provoca la exclusión de algunos sistemas o aplicaciones clave en los procesos de respaldo. - Falta de redundancia geográfica de los respaldos, almacenando las copias en la misma ubicación física que el sistema de producción.	infraestructura tecnológica (fallas de hardware, cortes eléctricos prolongados) que impiden la ejecución automática de los respaldos programados.	información bajo la Ley 1581 de 2012 y otros requisitos de seguridad de la información (ISO 27001). - Impacto financiero significativo por la necesidad de contratar servicios de recuperación de datos, así como sanciones por incumplimiento normativo. - Pérdida de confianza por parte de terceros (clientes, partes interesadas, reguladores) al no poder garantizar la integridad y la disponibilidad de la información. - Dificultad para reanudar operaciones tras un incidente, debido a la falta de respaldo de configuraciones, bases de datos o archivos esenciales.	legales. - Fortalecimiento de la confianza de los clientes y partes interesadas, al contar con mecanismos de respaldo de información. - Capacidad de respuesta más ágil ante ciberataques (ransomware), recuperando los sistemas con respaldos actualizados y protegidos.

ANTES DE LOS CONTROLES		
Probabilidad	**Impacto**	**Zona Inherente**
Muy Alta	**Catastrófico**	**Zona de Riesgo Extrema**

Controles	
Tipo	**Descripción**
Preventivo	Supervisión continua de la implementación y el cumplimiento de las políticas de respaldo de la información, garantizando la ejecución periódica de los respaldos conforme a las directrices establecidas, con el objetivo de preservar la seguridad e integridad de los datos.
Preventivo	Seguimiento a la ejecución pruebas periódicas de restauración de respaldos, simulando el proceso de recuperación para verificar la integridad y disponibilidad de la información, dentro del marco del Plan de Continuidad TIC.
Correctivo	Aislamiento y contención de malware en sistemas infectados y cuentas comprometidas, garantizando que no se propague a otros sistemas y se minimice el impacto en la infraestructura de TI.
Correctivo	Reuniones de revisión post-incidente, acompañadas de los documentos que evidencian los ajustes y mejoras implementadas en los procedimientos.

DESPUÉS DE LOS CONTROLES		
Probabilidad	**Impacto**	**Zona Residual**
Alta	**Catastrófico**	**Zona de Riesgo Extrema**
Opción de manejo	**Riesgo Institucional**	**Riesgo de Corrupción**
Evitar el Riesgo	**SI**	**NO**

Nota. Identificación asociada al riesgo No. 05 (Riesgo de pérdida irreversible de datos críticos). Elaborado por el Proceso Gestión de TIC ALFM – 2024.

6. MATRIZ DE ACTIVIDADES

Tabla 6.
Definición de actividades establecidas mediante los riesgos.

No.	RIESGOS IMPACTADOS	ACTIVIDAD (CONTROLES)	EVIDENCIA	FRECUENCIA	RESPONSABLE
1	Riesgo No. 01	Gestión del control de acceso basada en roles y perfiles, conforme a las funciones y responsabilidades asignadas a los usuarios en cada sistema de información o plataforma tecnológica.	Registro documentado de la asignación, modificación y revocación de roles y perfiles de acceso en los sistemas de información, incluyendo las autorizaciones correspondientes y la trazabilidad de los cambios realizados.	Cuatrimestral	Profesional Defensa – Grupo Redes e Infraestructura Tecnológica.
2	Riesgo No. 01	Monitoreo y revisión periódica de los accesos a los sistemas de información para identificar patrones anómalos, inusuales o no autorizados, con el fin de detectar posibles incidentes de seguridad y garantizar el cumplimiento de las políticas de control de acceso.	Informes de seguimiento de los accesos a los sistemas de información, que incluya registros de acceso, análisis de eventos, identificación de accesos inusuales y acciones correctivas, en cumplimiento con las políticas de seguridad de acceso.	Semestral	Profesional Defensa – Grupo Informática.
3	Riesgo No. 01	Aplicación	Registro de	Semestral	Técnico de

No.	RIESGOS IMPACTADOS	ACTIVIDAD (CONTROLES)	EVIDENCIA	FRECUENCIA	RESPONSABLE
	Riesgo No. 02	periódica de parches de seguridad para corregir vulnerabilidades identificadas, asegurando que los sistemas estén protegidos contra amenazas y riesgos emergentes.	parches aplicados a los sistemas (Windows Server Update Services - WSUS) y/o informes de actualización de sistemas.		Apoyo Seguridad y Defensa – Grupo Informática. Profesional Defensa – Grupo Redes e Infraestructura Tecnológica.
4	Riesgo No. 01 Riesgo No. 02 Riesgo No. 03 Riesgo No. 04	Implementación de programas de sensibilización en seguridad informática y de la información, con el objetivo de fomentar la conciencia sobre las mejores prácticas de seguridad y mitigar los riesgos asociados a los activos de información.	Registros de capacitaciones y/o sesiones de sensibilización, materiales educativos utilizados (presentaciones, manuales, videos), difusiones masivas por correo y listas de asistencia de los participantes.	Semestral	Profesional Defensa – Seguridad de la Información.
5	Riesgo No. 02	Segmentación de red y control de acceso, mediante la configuración de VLANs y la segmentación de la red, para aislar los sistemas críticos y protegerlos de	Mapas de red actualizados y documentación detallada de la configuración de VLANs, almacenada en las herramientas de administración de red.	Primer Cuatrimestre	Profesional Defensa – Grupo de Redes e Infraestructura Tecnológica.

No.	RIESGOS IMPACTADOS	ACTIVIDAD (CONTROLES)	EVIDENCIA	FRECUENCIA	RESPONSABLE
		otros entornos de la red.			
6	Riesgo No. 02	Seguimiento de medidas de protección contra ataques DDoS mediante firewalls y sistemas de prevención de intrusiones (IPS) para mitigar posibles amenazas.	Registros de alertas de DDoS generados y almacenados en herramientas de monitoreo, como FortiAnalyzer, para seguimiento y análisis de incidentes.	Cuatrimestral	Profesional Defensa – Seguridad de la Información.
7	Riesgo No. 02	Análisis de vulnerabilidades: Evaluación periódica de las vulnerabilidades en el software y la infraestructura tecnológica.	Informes de análisis de vulnerabilidades.	Cuatrimestral	Profesional Defensa – Seguridad de la Información.
8	Riesgo No. 02 Riesgo No. 04	Activación y ejecución del plan de respuesta a incidentes de ciberseguridad ante la detección de afectaciones en los sistemas críticos, con procedimientos establecidos para la contención, análisis y mitigación del impacto.	Informes de respuesta a incidentes y/o (tickets de incidentes en la herramienta de mesa de ayuda GLPI).	Trimestral	Profesional Defensa – Seguridad de la Información.
9	Riesgo No. 02 Riesgo No. 03	Aislamiento y contención de	Registros detallados de las	Trimestral	Profesional Defensa –

No.	RIESGOS IMPACTADOS	ACTIVIDAD (CONTROLES)	EVIDENCIA	FRECUENCIA	RESPONSABLE
	Riesgo No. 05	malware en sistemas infectados y cuentas comprometidas, garantizando que no se propague a otros sistemas y se minimice el impacto en la infraestructura de TI.	acciones de contención del malware en los sistemas infectados, incluyendo fechas, sistemas afectados, y procedimientos de aislamiento implementados.		Grupo Redes e Infraestructura Tecnológica.
10	Riesgo No. 03	Implementación de campañas de simulación de phishing para evaluar la respuesta de los usuarios, identificar conductas inseguras y fortalecer la conciencia en seguridad de la información.	Informes de resultados de las campañas de simulación de phishing, incluyendo métricas de usuarios que interactuaron con los correos simulados y acciones correctivas implementadas.	Semestral	Profesional Defensa – Seguridad de la Información.
11	Riesgo No. 03	Monitoreo continuo de eventos de seguridad para identificar y alertar sobre accesos inusuales a la información, permitiendo una respuesta oportuna ante posibles incidentes.	Registros de alertas generadas y/o informes de intentos de acceso bloqueados, soportados mediante las herramientas de monitoreo y control de seguridad.	Cuatrimestral	Profesional Defensa – Seguridad de la Información.
12	Riesgo No. 03 Riesgo No. 04	Revisión periódica de la	Registros de seguimiento y	Cuatrimestral	Profesional Defensa –

No.	RIESGOS IMPACTADOS	ACTIVIDAD (CONTROLES)	EVIDENCIA	FRECUENCIA	RESPONSABLE
		aplicabilidad de excepciones de seguridad informática, incluidas aquellas relacionadas con dispositivos de almacenamiento (SAN, NAS) y puertos USB, para garantizar su pertinencia y minimizar riesgos de acceso no autorizado.	control de la aplicabilidad de excepciones de seguridad informática, incluyendo la justificación, aprobación y periodo de vigencia de cada excepción.		Seguridad de la Información.
13	Riesgo No. 04	Mantener un inventario actualizado y completo de los activos de información y dispositivos, asegurando la asignación de responsables específicos para la gestión y protección de cada activo.	Matriz actualizada de activos de información, que incluye la asignación de responsables y códigos de identificación únicos (etiquetas) para cada activo.	Actividad que se encuentra integrada al Plan Estratégico de Seguridad y Privacidad de la Información – PESI vigencia 2025, con un plazo de cumplimiento Semestral.	
14	Riesgo No. 04	Seguimiento a los sistemas de control de acceso que utilizan autenticación biométrica, tarjetas de proximidad y/o claves únicas para garantizar	Informe de Seguimiento a la verificación de los registros de acceso físico, autenticación biométrica y/o reportes de ingreso a áreas restringidas (Data Center	Semestral	Técnico de Apoyo Seguridad y Defensa – Grupo Redes e Infraestructura Tecnológica.

No.	RIESGOS IMPACTADOS	ACTIVIDAD (CONTROLES)	EVIDENCIA	FRECUENCIA	RESPONSABLE
		el ingreso seguro a áreas críticas, como el Data Center Principal y Alterno.	Principal y Alterno).		
15	Riesgo No. 04	Supervisión de la funcionalidad del Circuito Cerrado de Televisión (CCTV) y revisión de los registros de acceso físico y digital a la Entidad.	Informes de seguimiento sobre la funcionalidad del Circuito Cerrado de Televisión (CCTV) y la gestión del control de acceso a las instalaciones.	Semestral	Profesional Defensa – Grupo Servicios Administrativos.
16	Riesgo No. 04	Monitoreo y control del acceso y salida de dispositivos externos de uso personal no institucional (portátiles) en las instalaciones de la entidad.	Informes de seguimiento sobre el control aplicado al ingreso y salida de dispositivos no institucionales.	Cuatrimestral	Profesional Defensa – Grupo Servicios Administrativos.
17	Riesgo No. 04	Seguimiento, control y revisión de los dispositivos externos autorizados (equipos de cómputo) que acceden a los sistemas de información a través del uso de la VPN.	Informes de seguimiento sobre la verificación de los dispositivos autorizados para el uso de la VPN.	Semestral	Técnico de Apoyo Seguridad y Defensa – Grupo Redes e Infraestructura Tecnológica.
18	Riesgo No. 05	Supervisión continua de la	Informes de seguimiento	Semestral	Técnicos de Apoyo

No.	RIESGOS IMPACTADOS	ACTIVIDAD (CONTROLES)	EVIDENCIA	FRECUENCIA	RESPONSABLE
		implementación y el cumplimiento de las políticas de respaldo de la información, garantizando la ejecución periódica de los respaldos conforme a las directrices establecidas, con el objetivo de preservar la seguridad e integridad de los datos.	sobre la aplicación de las directrices para la generación de respaldos, que incluyen los usuarios involucrados, las herramientas empleadas y los sistemas de información abarcados.		Seguridad y Defensa – Grupo Redes e Infraestructura Tecnológica y Grupo Informática.
19	Riesgo No. 05	Seguimiento a la ejecución pruebas periódicas de restauración de respaldos, simulando el proceso de recuperación para verificar la integridad y disponibilidad de la información, dentro del marco del Plan de Continuidad TIC.	Informes de seguimiento sobre la ejecución de las pruebas de restauración y los resultados obtenidos, conforme al Plan de Continuidad TIC.	Actividad que se encuentra integrada al Plan Estratégico de Seguridad y Privacidad de la Información – PESI vigencia 2025, con un plazo de cumplimiento Semestral.	
20	Riesgo No. 05	Reuniones de revisión post-incidente, acompañadas de los documentos que evidencian los	Actas de las reuniones de revisión post-incidente, acompañadas de los documentos que	Trimestral	Profesional Defensa – Seguridad de la Información.

No.	RIESGOS IMPACTADOS	ACTIVIDAD (CONTROLES)	EVIDENCIA	FRECUENCIA	RESPONSABLE
		ajustes y mejoras implementadas en los procedimientos.	evidencian los ajustes y mejoras implementadas en los procedimientos.		
21	N/A	Realizar un proceso de análisis y verificación de la ejecución de las actividades definidas en el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información. Este análisis estará orientado a identificar ajustes y/o cambios necesarios para garantizar el cumplimiento de la normativa aplicable y los objetivos de la misión institucional.	Informe de Análisis y Verificación del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información	Anual	Profesional Defensa – Seguridad de la Información.

Nota. Definición de actividades a ejecutar establecidas mediante la Matriz de Riesgos para la vigencia 2025. Elaborado por el Proceso Gestión de TIC ALFM – 2024.

7. SEGUIMIENTO

A través de la herramienta Suite visión empresarial y el personal de la oficina principal, 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.

8. ANÁLISIS Y MEDICIÓN

El análisis y medición de la ejecución del Plan de Tratamiento de Riesgos de Seguridad de la Información - PTR 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 de Tratamiento de Riesgos de Seguridad de la Información – PTR a través de informes cuatrimestrales; así mismo se coordinara con la OAPII la alineación de los riesgos aquí identificados en la matriz de riesgos de la entidad.

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
Gestión del control de acceso basada en roles y perfiles, conforme a las funciones y responsabilidades asignadas a los usuarios en cada sistema de información o plataforma tecnológica.	Registro documentado de la asignación, modificación y revocación de roles y perfiles de acceso en los sistemas de información, incluyendo las autorizaciones correspondientes y la trazabilidad de los cambios realizados.	01/02/2025 01/05/2025 01/09/2025	08/05/2025 05/09/2025 07/01/2026	Oficina Tecnologías de la Información y las Comunicaciones.	Proceso Gestión de TIC.	Profesional Defensa – Grupo Redes e Infraestructura Tecnológica.	Profesional Defensa – Seguridad de la Información.	Líder Proceso Gestión de TIC.
Monitoreo y revisión periódica de los accesos a los sistemas de información para identificar patrones anómalos, inusuales o no autorizados, con el fin de detectar posibles incidentes de seguridad y garantizar el	Informes de seguimiento de los accesos a los sistemas de información, que incluya registros de acceso, análisis de eventos, identificación de accesos inusuales y acciones correctivas, en cumplimiento con las políticas de	01/02/2025 01/07/2025	07/07/2025 07/01/2026	Oficina Tecnologías de la Información y las Comunicaciones.	Proceso Gestión de TIC.	Profesional Defensa – Grupo Informática.	Profesional Defensa – Seguridad de la Información.	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
cumplimiento de las políticas de control de acceso.	seguridad de acceso.							
Aplicación periódica de parches de seguridad para corregir vulnerabilidades identificadas, asegurando que los sistemas estén protegidos contra amenazas y riesgos emergentes.	Registro de parches aplicados a los sistemas (Windows Server Update Services - WSUS) y/o informes de actualización de sistemas.	01/02/2025 01/07/2025	07/07/2025 07/01/2026	Oficina Tecnologías de la Información y las Comunicaciones.	Proceso Gestión de TIC.	Profesional Defensa – Grupo Redes e Infraestructura Tecnológica. Técnico de Apoyo Seguridad y Defensa – Grupo Informática.	Profesional Defensa – Seguridad de la Información.	Líder Proceso Gestión de TIC.
Implementación de programas de sensibilización en seguridad informática y de la información, con el objetivo de fomentar la conciencia sobre las mejores prácticas de seguridad y mitigar los riesgos asociados a los activos de información.	Registros de capacitaciones y/o sesiones de sensibilización, materiales educativos utilizados (presentaciones, manuales, videos), difusiones masivas por correo y listas de asistencia de los participantes.	01/02/2025 01/07/2025	07/07/2025 07/01/2026	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
Segmentación de red y control de acceso, mediante la configuración de VLANs y la segmentación de la red, para aislar los sistemas críticos y protegerlos de otros entornos de la red.	Mapas de red actualizados y documentación detallada de la configuración de VLANs, almacenada en las herramientas de administración de red.	01/02/2025	08/05/2025	Oficina Tecnologías de la Información y las Comunicaciones.	Proceso Gestión de TIC.	Profesional Defensa – Grupo Redes e Infraestructura Tecnológica.	Profesional Defensa – Seguridad de la Información.	Líder Proceso Gestión de TIC.
Seguimiento de medidas de protección contra ataques DDoS mediante firewalls y sistemas de prevención de intrusiones (IPS) para mitigar posibles amenazas.	Registros de alertas de DDoS generados y almacenados en herramientas de monitoreo, como FortiAnalyzer, para seguimiento y análisis de incidentes.	01/02/2025 01/05/2025 01/09/2025	08/05/2025 05/09/2025 07/01/2026	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.
Análisis de vulnerabilidades: Evaluación periódica de las vulnerabilidades en el software y la infraestructura tecnológica.	Informes de análisis de vulnerabilidades.	01/02/2025 01/05/2025 01/09/2025	08/05/2025 05/09/2025 07/01/2026	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.
Activación y	Informes de	01/02/2025	07/04/2025	Oficina	Proceso	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
ejecución del plan de respuesta a incidentes de ciberseguridad ante la detección de afectaciones en los sistemas críticos, con procedimientos establecidos para la contención, análisis y mitigación del impacto.	respuesta a incidentes y/o (tickets de incidentes en la herramienta de mesa de ayuda GLPI).	01/04/2025 01/07/2025 01/10/2025	07/07/2025 07/10/2025 07/01/2026	Tecnologías de la Información y las Comunicaciones.	Gestión de TIC.	Defensa – Seguridad de la Información.		Gestión de TIC.
Aislamiento y contención de malware en sistemas infectados y cuentas comprometidas, garantizando que no se propague a otros sistemas y se minimice el impacto en la infraestructura de TI.	Registros detallados de las acciones de contención del malware en los sistemas infectados, incluyendo fechas, sistemas afectados, y procedimientos de aislamiento implementados.	01/02/2025 01/04/2025 01/07/2025 01/10/2025	07/04/2025 07/07/2025 07/10/2025 07/01/2026	Oficina Tecnologías de la Información y las Comunicaciones.	Proceso Gestión de TIC.	Profesionales Defensa – Grupo Redes e Infraestructura Tecnológica.	Profesional Defensa – Seguridad de la Información.	Líder Proceso Gestión de TIC.
Implementación de campañas de simulación de phishing para	Informes de resultados de las campañas de simulación de	01/02/2025 01/07/2025	07/07/2025 07/01/2026	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
evaluar la respuesta de los usuarios, identificar conductas inseguras y fortalecer la conciencia en seguridad de la información.	phishing, incluyendo métricas de usuarios que interactuaron con los correos simulados y acciones correctivas implementadas.							
Monitoreo continuo de eventos de seguridad para identificar y alertar sobre accesos inusuales a la información, permitiendo una respuesta oportuna ante posibles incidentes.	Registros de alertas generadas y/o informes de intentos de acceso bloqueados, soportados mediante las herramientas de monitoreo y control de seguridad.	01/02/2025 01/05/2025 01/09/2025	08/05/2025 05/09/2025 07/01/2026	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.
Revisión periódica de la aplicabilidad de excepciones de seguridad informática, incluidas aquellas relacionadas con dispositivos de almacenamiento	Registros de seguimiento y control de la aplicabilidad de excepciones de seguridad informática, incluyendo la justificación,	01/02/2025 01/05/2025 01/09/2025	08/05/2025 05/09/2025 07/01/2026	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
(SAN, NAS) y puertos USB, para garantizar su pertinencia y minimizar riesgos de acceso no autorizado.	aprobación y periodo de vigencia de cada excepción.							
Seguimiento a los sistemas de control de acceso que utilizan autenticación biométrica, tarjetas de proximidad y/o claves únicas para garantizar el ingreso seguro a áreas críticas, como el Data Center Principal y Alterno.	Informe de Seguimiento a la verificación de los registros de acceso físico, autenticación biométrica y/o reportes de ingreso a áreas restringidas (Data Center Principal y Alterno).	01/02/2025 01/07/2025	07/07/2025 07/01/2026	Oficina Tecnologías de la Información y las Comunicaciones.	Proceso Gestión de TIC.	Técnico de Apoyo Seguridad y Defensa – Grupo Redes e Infraestructura Tecnológica.	Profesional Defensa – Seguridad de la Información.	Líder Proceso Gestión de TIC.
Supervisión de la funcionalidad del Circuito Cerrado de Televisión (CCTV) y revisión de los registros de acceso físico y digital a la Entidad.	Informes de seguimiento sobre la funcionalidad del Circuito Cerrado de Televisión (CCTV) y la gestión del control de acceso a las	01/02/2025 01/07/2025	07/07/2025 07/01/2026	Dirección Administrativa y de Talento Humano.	Proceso Gestión Administrativa.	Profesional Defensa – Grupo Servicios Administrativos.	Profesional Defensa – Seguridad de la Información.	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
	instalaciones.							
Monitoreo y control del acceso y salida de dispositivos externos de uso personal no institucional (portátiles) en las instalaciones de la entidad.	Informes de seguimiento sobre el control aplicado al ingreso y salida de dispositivos no institucionales.	01/02/2025 01/05/2025 01/09/2025	08/05/2025 05/09/2025 07/01/2026	Dirección Administrativa y de Talento Humano.	Proceso Gestión Administrativa.	Profesional Defensa – Grupo Servicios Administrativos.	Profesional Defensa – Seguridad de la Información.	Líder Proceso Gestión de TIC.
Seguimiento, control y revisión de los dispositivos externos autorizados (equipos de cómputo) que acceden a los sistemas de información a través del uso de la VPN.	Informes de seguimiento sobre la verificación de los dispositivos autorizados para el uso de la VPN.	01/02/2025 01/07/2025	07/07/2025 07/01/2026	Oficina Tecnologías de la Información y las Comunicaciones.	Proceso Gestión de TIC.	Técnico de Apoyo Seguridad y Defensa – Grupo Redes e Infraestructura Tecnológica.	Profesional Defensa – Seguridad de la Información.	Líder Proceso Gestión de TIC.
Supervisión continua de la implementación y el cumplimiento de las políticas de respaldo de la información, garantizando la ejecución	Informes de seguimiento sobre la aplicación de las directrices para la generación de respaldos, que incluyen los usuarios	01/02/2025 01/07/2025	07/07/2025 07/01/2026	Oficina Tecnologías de la Información y las Comunicaciones.	Proceso Gestión de TIC.	Técnicos de Apoyo Seguridad y Defensa Grupo Redes e Infraestructura Tecnológica y Grupo Informática.	Profesional Defensa – Seguridad de la Información.	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
periódica de los respaldos conforme a las directrices establecidas, con el objetivo de preservar la seguridad e integridad de los datos.	involucrados, las herramientas empleadas y los sistemas de información abarcados.							
Reuniones de revisión post-incidente, acompañadas de los documentos que evidencian los ajustes y mejoras implementadas en los procedimientos.	Actas de las reuniones de revisión post-incidente, acompañadas de los documentos que evidencian los ajustes y mejoras implementadas en los procedimientos.	01/02/2025 01/04/2025 01/07/2025 01/10/2025	07/04/2025 07/07/2025 07/10/2025 07/01/2026	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.
Realizar un proceso de análisis y verificación de la ejecución de las actividades definidas en el Plan de Tratamiento de Riesgos de	Informe de Análisis y Verificación del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información.	01/01/2026	15/01/2026	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
Seguridad y Privacidad de la Información. Este análisis estará orientado a identificar ajustes y/o cambios necesarios para garantizar el cumplimiento de la normativa aplicable y los objetivos de la misión institucional.								