PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN "PTR" – VIGENCIA 2024.

ELABORÓ	REVISÓ	APROBÓ
NOMBRE: Ing. Deiby Leandro Alvarado Rodríguez.	**NOMBRE:** Ing. Roberto Velásquez Arango	**NOMBRE:** CR. Carlos Augusto Mórales Hernández
CARGO: Profesional Defensa – Seguridad de la información.	**CARGO:** Coordinador Grupo Informática	**CARGO:** Director General de la Agencia Logística de las Fuerzas Militares
FIRMA:	**FIRMA:**	**FIRMA:**

TABLA DE CONTENIDO

1. GENERALIDADES 3

2. REFERENCIA NORMATIVA 3

3. OBJETIVO DEL PLAN 6

3.1. OBJETIVOS ESPECÍFICOS 6

4. ALCANCE 7

5. CUERPO DEL MANUAL 7

5.1. MAPA DE RIESGOS. 7

5.2. GESTIÓN DE RIESGOS. 10

6. MATRIZ DE ACTIVIDADES 11

7. SEGUIMIENTO 14

8. ANÁLISIS Y MEDICIÓN 14

1. GENERALIDADES

Desde sus inicios, los factores de riesgo estaban principalmente asociados con contingencias de carácter natural y tecnológico. Sin embargo, eventos significativos como el terrorismo, la inestabilidad política, pandemias y códigos maliciosos han destacado la necesidad de incorporar nuevas amenazas, tanto en el mundo físico como en el entorno digital. Este cambio de perspectiva es esencial para comprender los riesgos más relevantes para los activos de información.

El análisis de riesgos de los activos de información es fundamental para comprender de manera efectiva y eficiente las posibles pérdidas de confidencialidad, integridad y disponibilidad en cada uno de los activos definidos en el alcance del análisis.

La gestión eficaz de la seguridad de la información y los riesgos de seguridad digital en los sistemas de información de la entidad, así como en los activos involucrados en sus procesos, garantiza la confidencialidad, integridad y disponibilidad de la información. Esto se logra mediante la aplicación de opciones adecuadas de tratamiento de riesgos de seguridad de la información y seguridad digital, en concordancia con la evaluación de los resultados de la valoración de riesgos del Sistema de Gestión de Seguridad de la Información y la normativa aplicable.

Este plan respalda la implementación de controles y acciones para mitigar los riesgos en la gestión tecnológica, así como para abordar los hallazgos de auditorías internas. Además, contribuye al cumplimiento del Modelo Integrado de Planeación y Gestión (MIPG) y respalda la implementación del Modelo de Seguridad y Privacidad de la Información (MSPI) del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), en línea con la política de Gobierno Digital de la entidad.

2. REFERENCIA NORMATIVA

Ley 527 (agosto 18) de 1999 “Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones”.

Ley 594 (julio 14) de 2000 “Por la cual se dicta la Ley General de Archivos y se dictan otras disposiciones”.

Ley 599 (julio 14) de 2001 “Código Penal Colombiano”.

Ley 1221 (julio 16) de 2008 “Por la cual se establecen normas para promover y regular el Teletrabajo y se dictan otras disposiciones”.

Ley 1266 (diciembre 31) de 2008 “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 (enero 05) de 2009 “Por medio del 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”.

Ley 1581 (octubre 17) de 2012 “Disposiciones Generales para tratamiento de datos personales”.

Ley 1712 (marzo 06) de 2014 “Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública”.

Ley 1978 (julio 25) de 2019 “Por la cual se moderniza el sector de las tecnologías de la información y las comunicaciones – TIC, se distribuyen competencias, se crea un regulador único y se dictan otras disposiciones”.

Ley 2052 (agosto 25) de 2020 “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”.

Ley 2294 (mayo 19) de 2023 “Por el cual se expide el plan nacional de desarrollo 2022 – 2026 “Colombia potencia mundial de vida””.

NTC-ISO/IEC 27001 de 2022 “Seguridad de la información, ciberseguridad y protección de la privacidad – Sistemas de gestión de la seguridad de la información - Requisitos”.

Decreto 2364 (noviembre 22) de 2012 “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 1377 (junio 27) de 2013 “Por el cual se reglamenta parcialmente la ley 1581 de 2012”.

Decreto 2573 (diciembre 12) de 2014 “Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en línea, se reglamenta parcialmente la Ley 1341 de 2009 y se dictan otras disposiciones.”

Decreto 1078 (mayo 26) de 2015 “Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones”.

Decreto 728 (mayo 05) de 2017 “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 (agosto 25) de 2017 “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 612 (abril 04) 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”.

Decreto 1008 (junio 14) de 2018 “Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones”.

Decreto 620 (mayo 02) de 2020 “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.”

Decreto 45 (enero 15) de 2021 “Por el cual se derogan el decreto 704 de 2018 y el artículo 1.1.2.3. del decreto número 1078 de 2015, único reglamentario del sector de tecnologías de la información y las comunicaciones”.

Decreto 377 (abril 09) de 2021 “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 (enero 24) de 2022 “Por el cual se adiciona el título 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”.

Decreto 338 (marzo 08) de 2022 “Por el cual se adiciona el título 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”.

Decreto 767 (mayo 16) de 2022 “Por la 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 1227 (junio 18) de 2022 “Por el cual se modifican los artículos 2.2.1.5.3, 2.2.1.5.5, 2.2.1.5.8 y 2.2.1.5.9 y se adicionan los artículos 2.2.1.5.15 al 2.2.1.5.25 al Decreto 1072 de 2015, único reglamentario del sector trabajo, relacionados con el teletrabajo.”

Decreto 1263 (julio 22) de 2022 “Por el cual se adiciona el titulo 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.”

CONPES 3701 (julio 14) de 2011 “Lineamientos de política para ciberseguridad y ciberdefensa”.

CONPES 3854 (abril 11) de 2016 “Política Nacional de Seguridad Digital”.

CONPES 3920 (abril 17) de 2018 “Política nacional de explotación de datos (BIG DATA)”.

CONPES 3995 (julio 01) de 2020 “Nacional de confianza y seguridad Digital”.

Resolución 1519 (agosto 24) de 2020 “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”.

Resolución 413 (marzo 01) de 2021 “Por la cual define el uso de las tecnologías en la nube para el sector defensa y se dictan otras disposiciones”.

Resolución 500 (marzo 10) de 2021 “Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de gobierno digital.”

Resolución 0463 (febrero 09) de 2022 “Por el cual se define el uso de Tecnologías en la Nube para el Sector Defensa y se dictan otras disposiciones”.

Resolución 000460 (febrero 15) de 2022 “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”.

Resolución 000746 (marzo 11) de 2022 “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”.

Resolución 7870 (diciembre 26) de 2022 “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”.

Manual integrado de gestión (septiembre 27) de 2019 “Manual integrado de gestión, código: GI-MA-02, versión No. 21”.

Directiva Permanente Ministerio Defensa No. 03 (enero 23) de 2019 “Lineamientos para la definición de la Política de Tratamiento de Datos Personales en el Ministerio de Defensa Nacional”.

Directiva Permanente Ministerio Defensa No. 913 (abril 19) de 2013 “Guías y procedimientos en tecnología de información y comunicaciones para el Sector Defensa”.

Directiva Permanente Ministerio de Defensa No. 018 (junio 19) de 2014 “Políticas de seguridad de la información para el Sector Defensa”.

Directiva Presidencial No. 02 (abril 02) de 2019 “Simplificación de la interacción digital entre los ciudadanos y el estado”.

Directiva Presidencial No. 03 (marzo 15) de 2021 “Lineamientos para el uso de servicios en la nube, inteligencia artificial, seguridad digital y gestión de datos”.

Directiva Presidencial No. 02 (febrero 24) de 2022 “Por medio del cual se efectúa reiteración de la política pública en materia de seguridad digital”.

3. OBJETIVO DEL PLAN

Establecer y ejecutar estrategias efectivas para el tratamiento de riesgos de seguridad y privacidad de la información durante la vigencia 2024; los cuales se centrarán en identificar, evaluar y mitigar los riesgos asociados con la integridad, confidencialidad y disponibilidad de los activos de información identificados en la ALFM.

3.1. OBJETIVOS ESPECÍFICOS

Desarrollar y aplicar lineamientos integrales para abordar los riesgos de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la operación en la ALFM.

Garantizar el cumplimiento de los requisitos legales y reglamentarios de la legislación colombiana.

Gestionar los riesgos de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación, considerando los contextos establecidos en la Entidad.

Promover y fortalecer la apropiación de conocimiento sobre la gestión de riesgos en Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación.

4. ALCANCE

El alcance incluirá la definición de políticas, la implementación de controles de seguridad, la capacitación del personal, y la respuesta y recuperación ante incidentes de seguridad de la información, fortaleciendo la resiliencia de la organización ante posibles amenazas, garantizando la protección y privacidad de la información a lo largo de la vigencia 2024.

5. CUERPO DEL MANUAL

5.1. MAPA DE RIESGOS.

Tabla 1.

Mapa de identificación de los riesgos.

Riesgo	Descripción del Riesgo	Causas	Efectos	Antes de los Controles			Controles	Actividades	Después de los Controles			Opción de Manejo	Institucional	De Corrupción
				Probabilidad	Impacto	Zona Inherente			Probabilidad	Impacto	Zona Residual			
Posibilidad de acceso no autorizado a datos sensibles.	Riesgo de que personas no autorizadas accedan a información crítica, comprometiendo su confidencialidad y generando posibles consecuencias negativas, como divulgación indebida y pérdida de confianza.	Falta de control de acceso adecuado.	Pérdida de confidencialidad.	Media	Mayor	Extrema	Controles de acceso basados en roles.	Guía control de acceso basado en roles (Aprobada y publicada).	Baja	Moderado	Media	Reducir el riesgo	Sí	Sí
								Documento de seguimiento a la implementación de la guía de control de acceso basado en roles						
		Debilidades en la gestión de contraseñas.	Daño a la reputación.				Políticas de contraseñas robustas.	Documento Manual de políticas de seguridad de la información actualizado.						
		Insuficiente conciencia del personal en seguridad.	Divulgación indebida de información.				Programas regulares de concientización en seguridad.	Plan de sensibilización y capacitación a los funcionarios de la ALFM – Informes de Seguimiento.						

Riesgo	Descripción del Riesgo	Causas	Efectos	Antes de los Controles			Controles	Actividades	Después de los Controles			Opción de Manejo	Institucional	De Corrupción
				Probabilidad	Impacto	Zona Inherente			Probabilidad	Impacto	Zona Residual			
								Gestión de boletines, fichas graficas e información relacionada con seguridad de la información.						
Posibilidad de afectación de los sistemas críticos debido a amenazas cibernéticas y vulnerabilidades tecnológicas.	Riesgo significativo de compromiso de la integridad, disponibilidad y confidencialidad de los sistemas críticos debido a amenazas cibernéticas y vulnerabilidades tecnológicas.	Descarga de archivos no seguros.	Pérdida de integridad de datos.	Alta	Mayor	Extrema	Gestión de software de antivirus.	Documento de seguimiento a la funcionalidad de software del antivirus.	Baja	Moderado	Media	Reducir el riesgo	Sí	No
								Documento soportando las acciones ejecutadas frente a las recomendaciones de la funcionalidad del software de antivirus.						
		Falta de protección contra DDoS.	Pérdida de disponibilidad.				Monitoreo continuo de la red.	Revisión y seguimiento al uso de red (Perfiles de navegación medio y alto).						
								Gestión de indicadores Disponibilidad de servicios TIC.						
		Desconocimiento de vulnerabilidades.	Riesgo de infección por malware				Monitoreo de vulnerabilidades.	Documento de identificación de vulnerabilidades tecnológicas (Antivirus, herramientas de seguridad perimetral).						
		Falta de configuraciones y actualizaciones parches de seguridad.	Interrupción de servicios críticos.				Actualización regular de sistemas y aplicaciones.	Seguimiento a la aplicabilidad de acciones frente a las vulnerabilidad						

Riesgo	Descripción del Riesgo	Causas	Efectos	Antes de los Controles			Controles	Actividades	Después de los Controles			Opción de Manejo	Institucional	De Corrupción
				Probabilidad	Impacto	Zona Inherente			Probabilidad	Impacto	Zona Residual			
								es tecnológicas identificadas.						
							Configuraciones de red seguras.	Seguimiento a las restricciones de seguridad mediante las herramientas de seguridad perimetral.						
Posibilidad de engaño a funcionarios para revelar información sensible.	Riesgo de revelar información sensible mediante tácticas de ingeniería social, afectando la confidencialidad de datos críticos.	Insuficiente conciencia del personal en seguridad.	Pérdida de credenciales.	Alta	Moderado	Alta	Programas regulares de concientización en seguridad.	Plan de sensibilización y capacitación a los funcionarios de la ALFM – Informes de Seguimiento.	Baja	Menor	Baja	Reducir el riesgo	Sí	No
								Gestión de boletines, fichas graficas e información relacionada con seguridad de la información.						
			Riesgo de acceso no autorizado.				Filtros de correo electrónico avanzados.	Seguimiento a la aplicabilidad de configuraciones de seguridad en el servidor de correo electrónico.						
			Posible pérdida financiera.				Verificación de eventos e incidentes de seguridad.	Seguimiento de los eventos e incidentes de seguridad presentados.						
			Interrupción de servicios críticos.											
Posibilidad de pérdida o robo de información o equipos tecnológicos.	Riesgo de exponer datos sensibles en caso de pérdida o robo de información y/o dispositivos.	Descuido o falta de medidas de seguridad física.	Acceso no autorizado a información sensible.	Media	Moderado	Alta	Políticas de seguridad física.	Documento Manual de políticas de seguridad de la información actualizado.	Baja	Menor	Baja	Reducir el riesgo	Sí	No
			Robo de dispositivos.											

Riesgo	Descripción del Riesgo	Causas	Efectos	Antes de los Controles			Controles	Actividades	Después de los Controles			Opción de Manejo	Institucional	De Corrupción
				Probabilidad	Impacto	Zona Inherente			Probabilidad	Impacto	Zona Residual			
			Riesgo de divulgación.				Revisiones excepciones de seguridad informática.	Seguimiento aplicabilidad excepciones de seguridad.						
Posibilidad de ausencia de copias de seguridad para datos críticos	Riesgo de pérdida irreversible de datos críticos debido a la falta de copias de seguridad, comprometiendo la disponibilidad e integridad de información vital.	Falta de procesos de respaldo establecidos.	Pérdida irreversible de datos críticos.	Media	Mayor	Extrema	Políticas de respaldo regulares.	Seguimiento aplicabilidad guías de generación de backups, usuarios, herramientas y sistemas de información.	Baja	Moderado	Media	Reducir el riesgo	Sí	No
			Interrupción de operaciones.				Almacenamiento seguro de copias de seguridad.							
		Falta de conciencia sobre la importancia del respaldo.	Pérdida financiera por la incapacidad de recuperación.				Pruebas regulares de recuperación.	Seguimiento a la ejecución del Plan de Continuidad TIC						

Nota: Definición de riesgos de seguridad y privacidad de la información. Lineamientos establecidos Manual de administración del riesgo ALFM Código: GI-MA-01 Versión No. 11 – Suite Vision Empresarial.

5.2. GESTIÓN DE RIESGOS.

Implementación de controles del Proceso Gestión de TIC, los cuales serán integrados con el Plan de Acción de la Entidad.

Objetivo Estratégico No. 03.
Priorizar el bienestar y la moral de la fuerza y de los servidores públicos vinculados al sector defensa.

Estrategia No. 3.2.
Modernizar y actualizar la gestión de la Entidad.

5.2.1. Posibilidad de acceso no autorizado a datos sensibles.

Controles:

Controles de acceso basados en roles.
Políticas de contraseñas robustas.
Programas regulares de concientización en seguridad.

5.2.2. Posibilidad de afectación de los sistemas críticos debido a amenazas cibernéticas y vulnerabilidades tecnológicas.

Controles:

Gestión de software de antivirus.

Monitoreo continuo de la red.
Monitoreo de vulnerabilidades.
Actualización regular de sistemas y aplicaciones.
Configuraciones de red seguras.

5.2.3. Posibilidad de engaño a funcionarios para revelar información sensible.

Controles:

Programas regulares de concientización en seguridad.
Filtros de correo electrónico avanzados.
Verificación de eventos e incidentes de seguridad.

5.2.4. Posibilidad de pérdida o robo de información o equipos tecnológicos.

Controles:

Políticas de seguridad física.
Revisiones excepciones de seguridad informática.

5.2.5. Posibilidad de ausencia de copias de seguridad para datos críticos.

Controles:

Políticas de respaldo regulares.
Almacenamiento seguro de copias de seguridad.
Pruebas regulares de recuperación.

6. MATRIZ DE ACTIVIDADES

Tabla 2.

Definición de actividades, establecidas por riesgos definidos.

ACTIVIDAD		RESPONSABLE	TAREA	SEGUIMIENTOS Y MONITOREO
1	Definición de controles de acceso basados en roles.	Técnico de Apoyo en Seguridad y Defensa.	Documentar el control de acceso basado en roles, que se encuentra implementado en la ALFM.	Plazo: Primer Cuatrimestre. Evidencia: Guía control de acceso basado en roles (Aprobada y publicada).
		Profesional Defensa	Seguimiento a la implementación de la Guía de control de acceso basado en roles.	Plazo: Semestral. Evidencia: Documento de seguimiento a la implementación de la guía de control de acceso basado en roles.
2	Revisión y	Profesional	Documento Manual	Actividad que se

ACTIVIDAD		RESPONSABLE	TAREA	SEGUIMIENTOS Y MONITOREO
	actualización manual de políticas de seguridad de la información de acuerdo a la actualización de la norma NTC/ISO/IEC 27001:2022.	Defensa.	de políticas de seguridad de la información actualizado.	encuentra integrada al Plan Estratégico de Seguridad de la Información – PESI, con un plazo de cumplimiento para el primer semestre.
3	Sensibilización a usuarios sobre seguridad de la información.	Profesional Defensa.	Plan de sensibilización y capacitación a los funcionarios de la ALFM – Informes de Seguimiento.	Actividad que se encuentra integrada al Plan Estratégico de Seguridad de la Información – PESI, con un plazo de cumplimiento cuatrimestral.
4	Seguimiento funcionalidad software de antivirus.	Técnico de Apoyo en Seguridad y Defensa.	Seguimiento funcionalidad del software de antivirus en la infraestructura tecnológica de la Entidad.	Plazo: Cuatrimestral. Evidencia: Documento de seguimiento a la funcionalidad de software del antivirus.
		Profesional Defensa. Técnicos de Apoyo en Seguridad y Defensa (Regionales).	Corrección de novedades presentadas a la infraestructura tecnológica frente a la ejecución del software de antivirus.	Plazo: Semestral Evidencia: Documento soportando las acciones ejecutadas frente a las recomendaciones de la funcionalidad del software de antivirus.
5	Análisis de vulnerabilidades tecnológicas (Antivirus, herramientas de seguridad perimetral).	Profesional Defensa.	Documento de identificación de vulnerabilidades tecnológicas (Antivirus, herramientas de seguridad perimetral).	Plazo: Cuatrimestral Evidencia: Documento de seguimiento a la identificación de vulnerabilidades tecnológicas (Antivirus, herramientas de seguridad perimetral).
		Profesional Defensa.	Seguimiento a la aplicabilidad de acciones frente a las vulnerabilidades tecnológicas identificadas.	Plazo: Semestral. Evidencia: Documento de aplicabilidad de acciones tomadas a las vulnerabilidades identificadas.
6	Revisión y seguimiento al uso de navegación web, de acuerdo con	Profesional Defensa.	Revisión y seguimiento al uso de red (Perfiles de	Actividad que se encuentra integrada al Plan Estratégico de

ACTIVIDAD		RESPONSABLE	TAREA	SEGUIMIENTOS Y MONITOREO
	los perfiles de navegación asignados a los funcionarios.		navegación medio y alto).	Seguridad de la Información – PESI, con un plazo de cumplimiento cuatrimestral.
7	Seguimiento configuración de filtros de seguridad mediante el servidor de correo electrónico.	Profesional Defensa.	Seguimiento a la aplicabilidad de configuraciones de seguridad en el servidor de correo electrónico.	Plazo: Cuatrimestral. Evidencia: Documento de seguimiento a las configuraciones de seguridad en el servidor de correo electrónico.
8	Restricciones de acceso a direccionamientos IP, listas negras y enlaces web reportados como fraudulentos, mediante las herramientas de seguridad perimetral.	Técnico de Apoyo en Seguridad y Defensa.	Seguimiento a las restricciones de seguridad mediante las herramientas de seguridad perimetral.	Plazo: Cuatrimestral. Evidencia: Documento de seguimiento a las restricciones de seguridad en las herramientas de seguridad perimetral.
9	Verificación de eventos e incidentes de seguridad (Fortisandbox).	Profesional Defensa.	Seguimiento de los eventos e incidentes de seguridad presentados.	Actividad que se encuentra integrada al Plan Estratégico de Seguridad de la Información – PESI, con un plazo de cumplimiento cuatrimestral.
10	Revisión asignación de permisos de acceso y uso a Dispositivos extraíbles en funcionarios autorizados.	Profesional Defensa.	Seguimiento aplicabilidad excepciones de seguridad.	Plazo: Cuatrimestral. Evidencia: Documento de seguimiento aplicabilidad excepciones de seguridad.
11	Elaboración de boletines, fichas graficas e información, sensibilizando a los funcionarios de la entidad en temas de seguridad de la información.	Profesional Defensa.	Gestión de boletines, fichas graficas e información relacionada con seguridad de la información.	Plazo: Cuatrimestral. Evidencia: Boletines, fichas graficas e información en temas relacionados a seguridad de la información.
12	Revisión y seguimiento indicadores de disponibilidad en servicios tecnológicos.	Profesional Defensa Técnicos de Apoyo en Seguridad y Defensa	Gestión de indicadores Disponibilidad de servicios TIC.	Actividad que se ejecuta mediante la gestión de indicadores del Proceso Gestión de TIC, con un plazo de cumplimiento trimestral.

ACTIVIDAD		RESPONSABLE	TAREA	SEGUIMIENTOS Y MONITOREO
		(Regionales).		
13	Seguimiento aplicabilidad guías de generación de backups, usuarios, herramientas y sistemas de información.	Técnico de Apoyo en Seguridad y Defensa.	Seguimiento generación de backups usuarios, herramientas y sistemas de información.	Plazo: Semestral. Evidencia: Documento de seguimiento a la generación de backups en usuarios, herramientas y sistemas de información.
14	Seguimiento Plan de Continuidad TIC	Profesional Defensa	Seguimiento a la ejecución del Plan de Continuidad TIC	Actividad que se ejecuta mediante el Plan de Continuidad TIC.

Nota: Definición de actividades a ejecutar establecidas por riesgos definidos para la vigencia 2024. Manual de administración de riesgos y oportunidades ALFM, Código: GI-MA-01 Versión No. 11 – Suite Vision Empresarial.

7. SEGUIMIENTO

Articulación con el Plan de Acción Institucional 2024.

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…”. De acuerdo con mesas de trabajo adelantadas se realizará la articulación del: Plan de Tratamiento de Riesgos de Seguridad de la Información - PTR.

Soporte de las actividades publicadas en la plataforma SUITE VISION EMPRESARIAL.

8. ANÁLISIS Y MEDICIÓN

Seguimiento mediante la plataforma SUITE VISION EMPRESARIAL.

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
Documentar el control de acceso basado en roles, que se encuentra implementado en la ALFM.	Guía control de acceso basado en roles (Aprobada y publicada).	01/01/2024	08/05/2024	Oficina TIC.	Gestión de TIC.	Técnico de Apoyo en Seguridad y Defensa.	Profesional Defensa.	Jefe Oficina TIC.
Seguimiento a la implementación de la Guía de control de acceso basado en roles.	Documento de seguimiento a la implementación de la guía de control de acceso basado en roles.	01/01/2024 01/07/2024	08/07/2024 09/01/2025	Oficina TIC.	Gestión de TIC.	Profesional Defensa.	N/A	Jefe Oficina TIC.
Seguimiento funcionalidad del software de antivirus en la infraestructura tecnológica de la Entidad.	Documento de seguimiento a la funcionalidad de software del antivirus.	01/01/2024 01/05/2024 01/09/2024	08/05/2024 06/09/2024 09/01/2025	Oficina TIC.	Gestión de TIC.	Técnico de Apoyo en Seguridad y Defensa.	Profesional Defensa.	Jefe Oficina TIC.
Corrección de novedades presentadas a la infraestructura tecnológica frente a la ejecución del software de antivirus.	Documento soportando las acciones ejecutadas frente a las recomendaciones de la funcionalidad del software de antivirus.	01/01/2024 01/07/2024	08/07/2024 09/01/2025	Oficina TIC.	Gestión de TIC.	Profesional Defensa. Técnicos de Apoyo en Seguridad y Defensa (Regionales).	Profesional Defensa. Profesional Defensa.	Jefe Oficina TIC. Jefe Oficina TIC.

Documento de identificación de vulnerabilidades tecnológicas (Antivirus, herramientas de seguridad perimetral).	Documento de seguimiento a la identificación de vulnerabilidades tecnológicas (Antivirus, herramientas de seguridad perimetral).	01/01/2024 01/05/2024 01/09/2024	08/05/2024 06/09/2024 09/01/2025	Oficina TIC.	Gestión de TIC.	Profesional Defensa.	N/A	Jefe Oficina TIC.
Seguimiento a la aplicabilidad de acciones frente a las vulnerabilidades tecnológicas identificadas.	Documento de aplicabilidad de acciones tomadas a las vulnerabilidades identificadas.	01/01/2024 01/07/2024	08/07/2024 09/01/2025	Oficina TIC.	Gestión de TIC.	Técnico de Apoyo en Seguridad y Defensa.	Profesional Defensa.	Jefe Oficina TIC.
Seguimiento a la aplicabilidad de configuraciones de seguridad en el servidor de correo electrónico.	Documento de seguimiento a las configuraciones de seguridad en el servidor de correo electrónico.	01/01/2024 01/05/2024 01/09/2024	08/05/2024 06/09/2024 09/01/2025	Oficina TIC.	Gestión de TIC.	Profesional Defensa.	Profesional Defensa.	Jefe Oficina TIC.
Seguimiento a las restricciones de seguridad mediante las herramientas de seguridad perimetral.	Documento de seguimiento a las restricciones de seguridad en las herramientas de seguridad perimetral.	01/01/2024 01/05/2024 01/09/2024	08/05/2024 06/09/2024 09/01/2025	Oficina TIC.	Gestión de TIC.	Técnico de Apoyo en Seguridad y Defensa.	Profesional Defensa.	Jefe Oficina TIC.
Seguimiento aplicabilidad excepciones de seguridad.	Documento de seguimiento aplicabilidad excepciones de seguridad.	01/01/2024 01/05/2024 01/09/2024	08/05/2024 06/09/2024 09/01/2025	Oficina TIC.	Gestión de TIC.	Profesional Defensa.	N/A	Jefe Oficina TIC.
Gestión de	Boletines, fichas	01/01/2024	08/05/2024	Oficina TIC.	Gestión de	Profesional	N/A	Jefe Oficina

boletines, fichas graficas e información relacionada con seguridad de la información.	graficas e información en temas relacionados a seguridad de la información.	01/05/2024 01/09/2024	06/09/2024 09/01/2025		TIC.	Defensa.		TIC.
Seguimiento generación de backups usuarios, herramientas y sistemas de información.	Documento de seguimiento a la generación de backups en usuarios, herramientas y sistemas de información.	01/01/2024 01/07/2024	08/07/2024 09/01/2025	Oficina TIC.	Gestión de TIC.	Profesional Defensa	N/A	Jefe Oficina TIC.