AGENCIA LOGÍSTICA
FUERZAS MILITARES
La unión de nuestras Fuerzas

PLAN ESTRATÉGICO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN – PESI.

ELABORÓ	FECHA			REVISÓ	FECHA			REVISÓ	FECHA		
	16	01	2023		19	01	2023		19	01	2023
NOMBRE: Ing. Deiby Leandro Alvarado Rodríguez.				**NOMBRE:** Ing. Daris Yaneth Padilla Díaz.				**NOMBRE** Ing. César Adolfo González Peña.			
CARGO Profesional Defensa Seguridad Informática – Oficina TIC.				**CARGO** Coordinadora Grupo Informática (E) – Oficina TIC.				**CARGO** Coordinador Grupo Redes e Infraestructura Tecnológica – Oficina TIC.			
FIRMA Deiby Leandro Alvarado Rodriguez Firmado digitalmente por Deiby Leandro Alvarado Rodriguez Fecha: 2023.01.30 13:30:29 -05'00'				**FIRMA** Ing. Daris Yaneth Padilla Díaz Firmado digitalmente por Ing. Daris Yaneth Padilla Díaz Fecha: 2023.01.30 14:19:34 -05'00'				**FIRMA** César González Firmado digitalmente por César González Fecha: 2023.01.30 13:52:50 -05'00'			
REVISÓ	**FECHA**			**REVISÓ**	**FECHA**			**APROBÓ**	**FECHA**		
	19	01	2023		19	01	2023		25	01	2023
NOMBRE: Adm. Esp. Ronald Oswaldo Duarte Rodríguez.				**NOMBRE:** Ing. Diana Marlen Caicedo Benavides.				**NOMBRE** Adm. Emp. Jaime Rafael Morón Barros.			
CARGO Coordinador Grupo de Desarrollo Organizacional y Gestión Integral – Oficina Asesora de Planeación e Innovación Institucional.				**CARGO** Jefe Oficina TIC (E).				**CARGO** Jefe Oficina Asesora de Planeación e Innovación Institucional Encargado de las Funciones del Despacho de la Dirección General de la Agencia Logística de las Fuerzas Militares.			
FIRMA Ronald Oswaldo Duarte Rodriguez Firmado digitalmente por Ronald Oswaldo Duarte Rodriguez Fecha: 2023.01.30 15:37:46 -05'00'				**FIRMA** Diana marlen Caicedo Benavides Firmado digitalmente por Diana marlen Caicedo Benavides Fecha: 2023.01.30 14:39:14 -05'00'				**FIRMA** Jaime Morón Barros Firmado digitalmente por Jaime Morón Barros Fecha: 2023.01.31 09:16:41 -05'00'			
PROCESO y/o DEPENDENCIA:				**Oficina Tecnologías de la Información y las Comunicaciones**							

TABLA DE CONTENIDO

1. GENERALIDADES.

En la actualidad, la Agencia Logística de las Fuerzas Militares – ALFM, identifica la información como uno de los activos indispensables en la conducción y consecución de los objetivos definidos en su Plan Estratégico, razón por la cual es necesario establecer un marco en el cual se asegure que la información es protegida de manera adecuada independientemente del medio en la que ésta sea manejada, procesada, transportada o almacenada. Adicional a los expuesto, en la medida en que los sistemas de información se constituyen en un apoyo a los procesos de la entidad, se requiere contar con estrategias de al nivel que permitan el control y administración efectiva de la información.

La ALFM adopta una metodología para la identificación y valoración de los activos de información, y una metodología para la evaluación y tratamiento de los riesgos; siendo este el medio más eficaz de tratar, gestionar y minimizar los riesgos, considerando el impacto para la entidad y las partes interesadas. Así mismo, el Modelo de Seguridad y Privacidad de la Información – MSPI, define políticas y procedimientos eficaces y coherentes con la estrategia de la entidad, como desarrollo de los controles adoptados para el tratamiento de los riesgos, los cuales están en continuo seguimiento y medición, a través del establecimiento de indicadores que aseguran la eficacia de los controles; apoyado en los programas de auditoría y la revisión por la dirección, que concluyen en la identificación de oportunidades de mejora las cuales son gestionadas para mantener la mejora continua del modelo.

En atención a lo anterior, la entidad implementa el Modelo de Seguridad y Privacidad de la Información – MSPI, como habilitador de la Política de Gobierno Digital, a su vez reglamentado a través del Decreto 1078 del 26 de mayo de 2015 “Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones” y la Resolución No. 00500 del 10 de marzo 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”.

Para tal fin, la entidad ha adoptado los lineamientos normativos de la NTC/ISO/IEC 27001:2013, la cual establece los requisitos para la implementación del SGSI, buscando mejorar el desempeño y la capacidad para prestar un servicio que responda a las necesidades y expectativas de las partes interesadas.

Por otra parte, el Plan Estratégico de Tecnologías de la Información y Comunicaciones (PETI), es un documento que expresa las intenciones de la ALFM, en la implementación de iniciativas y acciones que promuevan el uso de las Tecnologías de la Información y las Comunicaciones – TIC como contribución al logro de los Objetivos y Lineamientos Estratégicos enmarcados en el Plan Estratégico Institucional, El PESI descrito en este documento está alineado completamente con el PETI.

Finalmente, los lineamientos y proyectos para el desarrollo, optimización e implementación efectiva de los Sistemas de Información, así como las iniciativas que permitirán una adecuada gestión de la Infraestructura de Hardware/Software, basados en el Modelo de Seguridad y Privacidad de la Información – MSPI y en las mejores prácticas de Gestión de Servicios y Proyectos de TI, contribuirán no solo con el logro de los objetivos institucionales, sino en la generación de confianza en el uso de los mecanismos tecnológicos.

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 1952 (enero 28) de 2019 “Por medio de la cual se expide el código general disciplinario y deroga la ley 734 de 2002 y algunas disposiciones de la ley 1474 de 2011, relacionadas con el derecho disciplinario.

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”.

NTC-ISO/IEC 27001 de 2013 “Tecnologías de la Información. Técnicas de Seguridad. 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 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 934 (agosto 18) de 2021 “Por el cual se adiciona el capítulo 7 al título 2 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 reglamentarse el parágrafo 2 del artículo 11 de la ley 1341 de 2009”.

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 de Gobierno Digital (diciembre versión. 06) de 2018 “En este documento se desarrolla el proceso de implementación de la Política de Gobierno Digital a través de los siguientes cuatro (4) momentos: 1. Conocer la política; 2. Planear la política; 3. Ejecutar la política; y 4. Medir la política; cada uno de ellos incorpora las acciones que permitirán desarrollar la Política en las entidades públicas de nivel nacional y territorial”.

Manual integrado de gestión (septiembre 27) de 2019 “Manual integrado de gestión, código: GI-MA-02, versión No. 20”.

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. 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. DEFINICIONES.

Para los efectos del presente plan se tendrán en cuenta las siguientes definiciones:

Activos tecnológicos o informáticos: Se consideran activos tecnológicos o informáticos todos los elementos de hardware, software, información y de comunicaciones entregados por la entidad al funcionario con el fin de facilitarle el desempeño de sus funciones. De esta manera, son activos tecnológicos, además de los programas (software aplicativo y de ofimática), los computadores o equipos de cómputo junto con sus periféricos (tarjeta de red, mouse, teclado, monitor, parlantes, unidades externas de almacenamiento, micrófono, entre otros), impresoras, escáneres, etc. También los equipos y elementos de comunicaciones (telefonía, switches, routers, cableado, etc.) y la información almacenada en los diversos equipos y bases de datos.

Análisis de riesgo: Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo. (ISO/IEC 27000).

Auditoría: Proceso sistemático, independiente y documentado para obtener evidencias de auditoría y obviamente para determinar el grado en el que se cumplen los criterios de auditoría. (ISO/IEC 27000).

Gobierno Digital: Es una política del Estado Colombiano encaminada a promover el uso y aprovechamiento de las tecnologías de la información y las comunicaciones para consolidar un Estado y ciudadanos competitivos, proactivos, e innovadores, que generen valor público en un entorno de confianza digital.

Modelo de Seguridad y Privacidad de la Información (MSPI): Es un conjunto de mejores prácticas que permiten a la ALFM mejorar sus estándares en seguridad de la información. Conducen a la preservación de la confidencialidad, integridad, disponibilidad de la información, permitiendo garantizar la privacidad de los datos, mediante la aplicación de un proceso de gestión del riesgo, brindando confianza a las partes interesadas acerca de la adecuada gestión de riesgos.

Modelo Integrado de Planeación y Gestión (MIPG): Es el marco de referencia para dirigir, planear, ejecutar, hacer seguimiento, evaluar y controlar la gestión de las entidades públicas con el fin de generar resultados que atiendan a los planes de desarrollo y que resuelvan las necesidades y problemas de los ciudadanos con integridad y calidad en los servicios.

Partes interesadas (Stakeholders): Personas u organizaciones que puede afectar o ser afectada por o percibirse a sí misma como afectada por una decisión o actividad.

Plan de Tratamiento de Riesgos (PTR): Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma. (ISO/IEC 27000).

Riesgo: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000).

Sistema de Gestión de Seguridad de la Información (SGSI): Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión y de mejora continua. (ISO/IEC 27000).

Tecnologías de la información y las comunicaciones (TIC): Son el conjunto de recursos, herramientas, equipos, programas informáticos, aplicaciones, redes y medios, que permiten la compilación, procesamiento, almacenamiento, transmisión de información como voz, datos, texto, video e imágenes.

Trazabilidad: Cualidad que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sean asociadas de modo inequívoco a un individuo o entidad. (ISO/IEC 27000).

Vulnerabilidad: Debilidad de un activo o control que puede ser explotada por una o más amenazas. (ISO/IEC 27000).

4. OBJETIVOS.

4.1. OBJETIVO GENERAL:

Definir la estrategia de Seguridad y Privacidad de la Información en cumplimiento del Modelo de Seguridad y Privacidad de la información (MSPI), alineado con el Modelo Integrado de Planeación y Gestión (MIPG), en las políticas de Gobierno Digital y Seguridad Digital, que responda a las necesidades de preservar la confidencialidad, la integridad y la disponibilidad sobre los activos de información.

4.2. OBJETIVOS ESPECIFICOS:

Identificar los activos de información de los procesos estratégicos de la Entidad.

Identificar y analizar los riesgos de los activos de información y establecer un plan de tratamiento de los riesgos que generan mayor impacto para la Entidad.

Sensibilizar a los funcionarios y contratistas de la ALFM acerca del Modelo de Seguridad y Privacidad de la Información, fortaleciendo el nivel de conciencia de los mismos, en cuanto a la necesidad de salvaguardar los activos de información críticos de la Entidad.

Implementar las políticas y controles de seguridad de la información y privacidad de la información alineado con el MSPI.

Implementar el modelo de gestión de incidentes de seguridad y Ciberseguridad de la Entidad.

Monitorear el cumplimiento de los requisitos de seguridad de la información.

Implementar acciones correctivas y de mejora para el Modelo de Seguridad y Privacidad de la Información.

5. ALCANCE.

El Plan Estratégico de Seguridad de la Información – PESI, tiene como finalidad el diagnóstico, análisis, definición y planeación del manejo de la seguridad de los procesos que se ejecutan en la ALFM y será actualizado anualmente; estos apoyarán el cumplimiento de los procesos y objetivos propuestos por las diferentes dependencias de la Entidad y está articulado de manera global en relación con la seguridad de la información.

6. ESTADO ACTUAL DE LA ENTIDAD FRENTE AL SGSI.

El Modelo de Seguridad y Privacidad de la Información – MSPI, define los lineamientos para la implementación de la estrategia de seguridad digital definidos por MinTIC, el cual contempla su operación basada en un ciclo PHVA (Planear, Hacer, Verificar y Actuar), así como los requerimientos legales, técnicos, normativos, reglamentarios y de funcionamiento; el modelo consta de cinco (05) fases las cuales permiten gestionar y mantener adecuadamente la seguridad y privacidad de los activos de información. Por ello se deben abordar las siguientes fases:

Diagnostico:

Realizar un diagnóstico o un análisis GAP, cuyo objetivo es identificar el estado actual de la Entidad respecto a la adopción del MSPI. Se recomienda usar este diagnóstico al iniciar el proceso de adopción, con el fin de que su resultado sea un insumo para la fase de planificación y luego al finalizar la fase cuatro de mejora continua.

Planificación:

Determinar las necesidades y objetivos de seguridad y privacidad de la información teniendo en cuenta su mapa de procesos, el tamaño y en general su contexto interno y externo. Esta fase define el plan de valoración y tratamiento de riesgos, siendo esta la más importante del ciclo.

Operación:

Implementar los controles que van a permitir disminuir el impacto o la probabilidad de ocurrencia de los riesgos de seguridad de la información identificados en la etapa de planificación.

Evaluación de desempeño:

Determinar el sistema y forma de evaluación de la adopción del modelo.

Mejoramiento continuo:

Establecer procedimientos para identificar desviaciones en las reglas definidas en el modelo y las acciones necesarias para su solución y no repetición.

En la ALFM, estas fases se han trabajado durante dos (02) vigencias, lo que ha permitido implementar gradualmente el Sistema de Gestión de Seguridad de la Información – SGSI, conforme a la normatividad y las necesidades de la entidad, a continuación, se presentan los resultados del autodiagnóstico realizado en la vigencia 2022.

Como se puede observar en la siguiente evaluación del avance del ciclo de funcionamiento del modelo de operación (PHVA) para el SGSI, la entidad ha cumplido en un 60% el modelo de operación y en adelante se gestionará el 40% pendiente y se seguirá con las fases de Efectivo y Gestionado.

AVANCE PHVA		
COMPONENTE	**% DE AVANCE ACTUAL ENTIDAD**	**% AVANCE ESPERADO**
Planificación	33%	40%
Implementación	11%	20%
Evaluación de desempeño	8%	20%
Mejora continúa	8%	20%
TOTAL	**60%**	**100%**

Fuente: Autodiagnóstico implementación MSPI ALFM – Vigencia 2022.

De igual manera la evaluación de efectividad de los controles de la NTC/ISO/IEC 27001:2013, es la siguiente para la vigencia 2022.

DOMINIO		CALIFICACIÓN ACTUAL	CALIFICACIÓN OBJETIVO	EFECTIVIDAD DE CONTROL
A.5	Políticas de Seguridad de la Información.	100	100	OPTIMIZADO
A.6	Organización de la Seguridad de la Información.	78	100	GESTIONADO
A.7	Seguridad de los Recursos Humanos.	84	100	OPTIMIZADO
A.8	Gestión de Activos.	66	100	GESTIONADO
A.9	Control de Acceso.	90	100	OPTIMIZADO
A.10	Criptografía.	60	100	EFECTIVO
A.11	Seguridad Física y del Entorno.	74	100	GESTIONADO
A.12	Seguridad de las Operaciones.	81	100	OPTIMIZADO
A.13	Seguridad de las Comunicaciones.	75	100	GESTIONADO
A.14	Adquisición, Desarrollo y Mantenimiento de Sistemas.	71	100	GESTIONADO
A.15	Relaciones con los proveedores.	80	100	GESTIONADO
A.16	Gestión de Incidentes de Seguridad de la Información.	66	100	GESTIONADO
A.17	Aspectos de Seguridad de la Información de la Gestión de la Continuidad del Negocio.	80	100	GESTIONADO
A.18	Cumplimiento.	66.5	100	GESTIONADO
PROMEDIO EVALUACIÓN DE CONTROLES		**77**	**100**	**GESTIONADO**

Fuente: Autodiagnóstico implementación MSPI ALFM – Vigencia 2022.

Con base en estos resultados, a continuación, se presenta un análisis de brechas, que es un método para evaluar las diferencias entre el desempeño real y el desempeño esperado en la implementación del SGSI en la ALFM; el término “brecha” se refiere al espacio entre “donde estamos ahora” (el estado actual) y donde “queremos estar” (el estado objetivo).

Fuente: Autodiagnóstico implementación MSPI ALFM – Vigencia 2022.

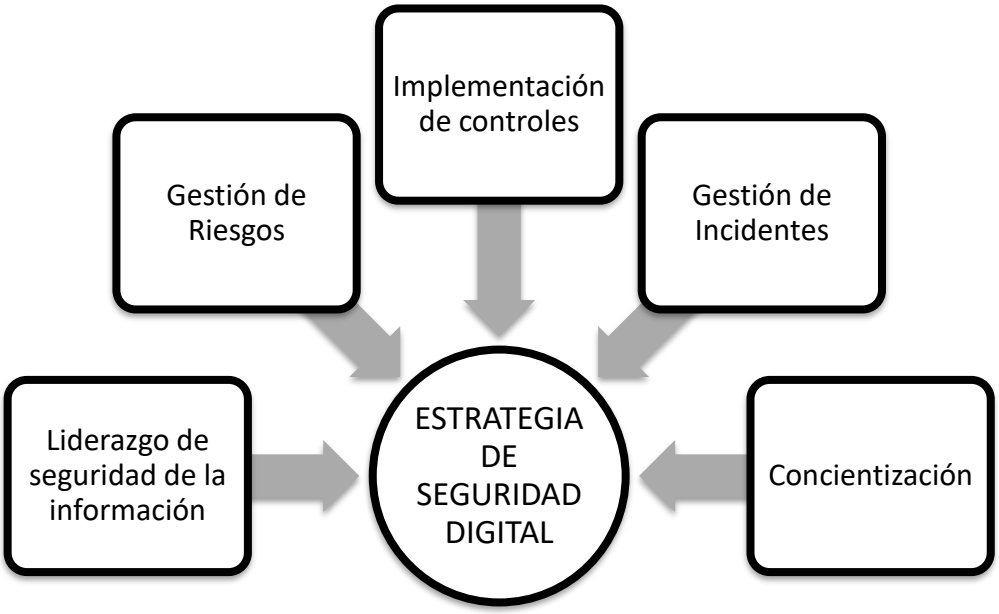
Alineación con el Plan Estratégico de Tecnologías de la Información – PETI.

Continuando con la ejecución de los proyectos descritos en el Plan Estratégico de Tecnologías de la Información – PETI y teniendo en cuenta los resultados y avances obtenidos anteriormente, para la vigencia 2023, se dará continuidad al desarrollo de actividades de fortalecimiento y mejoramiento al Sistema de Gestión de Seguridad de la Información -SGSI dentro del proyecto de Política de Gobierno Digital de la entidad; de igual forma con la ejecución de actividades aquí señaladas también se dará cumplimiento a la implementación y gestión de las políticas institucionales de Seguridad de la Información, Seguridad Digital y la Política de Gobierno Digital.

7. ESTRATEGIA DE SEGURIDAD DIGITAL

La ALFM establecerá una estrategia de seguridad digital en la que se integren los principios, políticas, procedimientos, guías, manuales, formatos y lineamientos para la gestión de la seguridad de la información, teniendo como premisa que dicha estrategia gira entorno a la implementación del Modelo de Seguridad y Privacidad de la Información – MSPI, así como la guía de gestión de riesgos de seguridad de la información y del procedimiento de gestión de incidentes establecido por la entidad.

Por tal motivo, la ALFM define las siguientes cinco (05) estrategias específicas, que permitirán establecer en su conjunto una estrategia general de seguridad digital:



7.1. DESCRIPCIÓN DE LAS ESTRATEGIAS ESPECÍFICAS (EJES)

A continuación, se describe el objetivo de cada una de las estrategias específicas a implementar, alineando las actividades a lo descrito dentro del MSPI y la resolución 500 de 2021:

ESTRATEGIA / EJE	DESCRIPCIÓN / OBJETIVO
Liderazgo de seguridad de la información.	Asegurar que se establezca el Modelo de Seguridad y Privacidad de la Información (MSPI) a través de la aprobación de la política general y demás lineamientos que se definan buscando proteger la confidencialidad, integridad y disponibilidad de la información teniendo como pilar fundamental el compromiso de la alta dirección y de los líderes de las diferentes dependencias y/o procesos de la Entidad a través del establecimiento de los roles y responsabilidades en seguridad de la información.
Gestión de riesgos.	Determinar los riesgos de seguridad de la información a través de la planificación y valoración que se defina buscando prevenir o reducir los efectos indeseados teniendo como pilar fundamental la implementación de controles de seguridad para el tratamiento de los riesgos.
Concientización.	Fortalecer la construcción de la cultura organizacional con base en la seguridad de la información para que convierta en un hábito, promoviendo las políticas, procedimientos, normas, buenas prácticas y demás lineamientos, la transferencia de conocimiento, la asignación y divulgación de responsabilidades de todo el personal de la entidad en seguridad y privacidad de la información.
Implementación de controles.	Planificar e implementar las acciones necesarias para lograr los objetivos de seguridad y privacidad de la información y mantener la confianza en la ejecución de los procesos de la Entidad, se pueden subdividir en controles técnicos y Administrativos.

Gestión de incidentes.	Garantizar una administración de incidentes de seguridad de la información con base a un enfoque de integración, análisis, comunicación de los eventos e incidentes y las debilidades de seguridad en pro de conocerlos y resolverlos para minimizar el impacto negativo de estos en la entidad.

8. RESPONSABLES

ROL Y/O CARGO FRENTE AL SGSI.	RESPONSABILIDADES
Alta Dirección.	Conocer el diseño e implementación del Sistema de Gestión de Seguridad de la Información – SGSI de la ALFM. Garantizar el cumplimiento de los objetivos y políticas institucionales a través del cumplimiento del SGSI. Asegurar mediante la revisión por la dirección que el SGSI sea conveniente, adecuado y eficaz para la entidad. Asegurar que se establezcan y mantengan los procesos necesarios para asegurar la confidencialidad, integridad y disponibilidad de los activos de información. Definir, asignar y aprobar los recursos financieros, técnicos, económicos y el personal necesario para el diseño, implementación, evaluación y mejora del SGSI. Establecer la Política de seguridad de la información, para garantizar la divulgación y la comunicación de esta a la ALFM. Garantizar el cumplimiento de la normatividad legal vigente aplicable en materia de Seguridad de la Información. Evaluar mínimo una vez al año la implementación de políticas y lineamientos en materia de seguridad de la información al interior de la ALFM. Conocer los avances, resultados, operación y efectividad de las acciones emprendidas en Seguridad de la Información.
Comité Institucional de Gestión y Desempeño.	Análisis de los resultados obtenidos en el diagnóstico inicial del Modelo de Seguridad y Privacidad de la Información – MSPI. Conocer y analizar la política de Seguridad establecida en la ALFM. Apoyo en la implementación de los estándares de seguridad necesarios, que garanticen la confidencialidad, integridad y disponibilidad de los activos de información. Participar en la investigación de incidentes de seguridad materializados. Conocer, entender y aplicar las políticas, normas, reglamentos, instrucciones e instructivos definidos en el SGSI. Proponer a la alta dirección la opción de medidas y desarrollo de actividades que procuren y mantengan el aseguramiento de los activos de información, preservando la confidencialidad, integridad y disponibilidad, en lo referente al SGSI. Vigilar el desarrollo de las actividades llevadas a cabo frente a la implementación y mejora del SGSI. Conocer los avances, resultados, operación y efectividad de las acciones emprendidas en Seguridad de la información. Realizar seguimiento a los indicadores del SGSI y el análisis de estos.
Jefe Oficina Gestión de TIC	Orientar y coordinar con los funcionarios requeridos, los procesos de implementación, desarrollo y mantenimiento del SGSI. Proponer acciones correctivas o de mejora a la alta dirección, ante la aparición de problemas potenciales o reales en la implementación y sostenibilidad del SGSI. Representar a la ALFM, en asuntos relacionados con el SGSI, ante organismos externos. Informar a la alta Dirección sobre el desempeño y las oportunidades de mejora del SGSI (NTC/ISO 27001:2013).

	Propender la concientización de los requisitos, necesidades y expectativas de las partes interesadas e involucradas en el SGSI en todos los niveles de la ALFM. Trabajar en coordinación con los Directores, Subdirectores, Jefes de Oficina y coordinadores de la ALFM, en el proceso de implementación y sostenibilidad del SGSI, diseñando planes y acciones necesarias para el cumplimiento del propósito.
Profesional Seguridad de la Información	Evaluar por lo menos una vez al año el desarrollo de las políticas y lineamientos establecidos en el SGSI. Coordinar las actividades definidas para la sensibilización y capacitación a los funcionarios, contratistas y terceros relacionados con la ALFM, en temas de seguridad de la información. Establecer, cumplir y hacer cumplir las políticas definidas en el SGSI. Identificar, evaluar y valorar los riesgos, así como contribuir en el control de estos. Establecer y socializar los planes de seguridad y privacidad de la información establecidos al interior de la ALFM. Diseñar e implementar el SGSI en la ALFM. Diseñar y gestionar la aprobación de los planes de seguridad de la información por parte de la alta dirección, así como ejecutarlo y hacer seguimiento para alcanzar los objetivos del SGSI. Informar a la alta dirección y a los funcionarios, sobre el funcionamiento, avances y los resultados del SGSI. Promover la participación de los funcionarios de la ALFM, en la implementación del SGSI. Elaborar, actualizar y divulgar normas de seguridad, instructivos, programas, procedimientos, reglamentos, objetivos y metas del SGSI. Participar como invitado en las reuniones del Comité Integral de Gestión y Desempeño, apoyando su gestión. Participar y liderar en la investigación y detección de los Incidentes, reportándolos, documentándolos y generando buenas prácticas al respecto mediante la difusión de boletines de seguridad. Garantizar la gestión del cumplimiento normativo y de las divulgaciones referentes al SGSI. Realizar verificaciones de la implementación y adopción de políticas de seguridad, al interior de la entidad, preservando la confidencialidad, integridad y disponibilidad de los activos de información. Capacitar y motivar a los funcionarios para el cumplimiento de las normas y políticas de seguridad de la información en la ALFM. Solicitar los recursos requeridos para el diseño e implementación del SGSI.
Líderes de Proceso.	Revisar los procedimientos y demás documentos propios de sus procesos frente a la ejecución del SGSI y ajustarlos si es necesario. Asegurar el cumplimiento de las políticas de seguridad establecidas en cada uno de los procesos que lidera y los transversales en lo que le compete. Verificar la identificación, evaluación, tratamiento y seguimiento de los riesgos sobre la seguridad de la información en su proceso, así mismo su pertinencia. Garantizar que todo su personal cumpla con las políticas, lineamientos y demás documentos generados en el SGSI. Motivar y permitir la asistencia de los funcionarios a cargo, a las sesiones de sensibilización y capacitación en temas relacionados con la seguridad de la información. Conocer los avances, resultados, operación y efectividad de las acciones emprendidas en el SGSI. Reportar oportunamente los incidentes de seguridad de la información a la Oficina Gestión de TIC, incumplimientos de políticas de seguridad y condiciones inseguras al

	interior de sus procesos, así mismo, motivar al personal a su cargo el reporte oportuno de los mismos. Responsabilizarse por la seguridad de los activos de información de su proceso, apoyándose en cada uno de los custodios (funcionarios) delegados en la protección de estos. Cumplir y hacer cumplir las normas, reglamentos, instrucciones, programas, políticas y planes establecidos en el SGSI, dentro del área a su cargo. Mantener retroalimentación de los procesos bajo su responsabilidad mediante la implementación de acciones correctivas, preventivas y de mejora del SGSI.
Funcionarios – Contratistas.	Participar activamente de las actividades establecidas en cada uno de los procedimientos que hacen parte del SGSI. Dar cumplimiento a las políticas establecidas en el SGSI. Participar de las capacitaciones y actividades relacionadas con el SGSI. Utilizar adecuadamente los activos de información suministrados para el desarrollo de sus labores, dándole el uso debido. Velar por la conservación de los activos de información de la ALFM, siguiendo las recomendaciones establecidas en los programas de SGSI aplicables a cada proceso. Informar oportunamente a su Jefe inmediato y el profesional de seguridad de la información sobre los riesgos de seguridad informática latentes en su sitio de trabajo. Establecer con el líder del proceso la necesidad de capacitaciones relacionadas con la seguridad de la información de acuerdo con las actividades a realizar. Reportar oportunamente los incidentes de seguridad, incumplimientos de políticas de seguridad y condiciones inseguras al interior de sus procesos. Conocer, entender y aplicar las políticas, normas, reglamentos, instrucciones e instructivos definidos en el SGSI. Participar en las actividades de sensibilización y capacitación sobre temas relacionados con la seguridad de la información. Dar cumplimiento de los objetivos del SGSI. Mantener limpio y ordenado el puesto de trabajo, preservando la confidencialidad de la información bajo su responsabilidad. Cumplir con todos los requisitos, cláusulas y demás parámetros legales y contractuales establecidos por la ALFM para el buen desempeño del SGSI.
Responsabilidades de los Visitantes.	Cumplir las normas, reglamentos, instrucciones, programas, políticas y planes establecidos en el SGSI al interior de la ALFM.

9. MATRIZ DE ACTIVIDADES

ESTRATEGIA / EJE	METAS	RESULTADOS	INSTRUMENTO	SEGUIMIENTOS Y MONITOREO
Liderazgo de seguridad de la información.	Implementación MSPI.	Seguimiento al estado de avance del MSPI.	Anexo 1. Modelo de Seguridad y Privacidad de la Información. Instrumento evaluación MSPI. Modelo de Seguridad y Privacidad de la Información.	Plazo: Semestral. Evidencia: Informe semestral de los avances al MSPI, anexando el instrumento de evaluación del MSPI actualizado.

			Instructivo No. 1 – Diligenciamiento de la Herramienta de diagnóstico de Seguridad y Privacidad de la Información.	
	Inventario de Activos de Información.	Actualización del inventario de activos de información.	Guía No. 5 – Gestión Clasificación de Activos. Inventario y clasificación de Activos de información e Infraestructura critica Cibernética Nacional.	Plazo: Semestral. Evidencia: Matriz de activos de información actualizada.
	Creación e implementación del Plan Institucional de Continuidad del negocio.	Documentos creados, actualizados y aprobados ante el SIG.	Guía No. 10 – Guía para la preparación de las TIC para la continuidad del negocio. Guía No. 11 - Guía para realizar el Análisis de Impacto de Negocios BIA. Plan de Continuidad del Negocio ALFM	Plazo: Primer Semestre. Evidencia: Documento creado (En caso de requerirse).
	Gestión Plan de Continuidad del Negocio ALFM	Seguimiento al estado avance del Plan.		Plazo: Semestral. Evidencia: Informe de seguimiento al cumplimiento de actividades en la herramienta SVE.
Gestión de riesgos.	Gestión Plan de Tratamiento de Riesgos de seguridad y privacidad de la información.	Seguimiento al estado avance del Plan.	Guía No. 07 – Guía de gestión de riesgos.	Plazo: Cuatrimestral. Evidencia: Informe de seguimiento. (Actividad que se encuentra integrada al Plan de Acción Institucional.)
Concientización.	Plan de sensibilización anual funcionarios de la ALFM.	Plan de actividades de sensibilización y concientización en temas relacionados a seguridad digital y de la información dirigido a todos los funcionarios de la entidad.	Guía No. 14 – Plan de Capacitación, Sensibilización y Comunicación de Seguridad de la Información. Convocatorias vigentes lideradas por MinTIC,	Plazo: Cuatrimestral. Evidencia: Plan de sensibilización y capacitación a los funcionarios de la ALFM – Informes de seguimiento a las capacitaciones.

			Gobierno Digital, entidades de seguridad nacional.	
Implementación de controles.	Madurez dominio política de seguridad de la información.	Política de Seguridad de la información "General" aprobada por la Alta Dirección.	Guía No. 2 - Elaboración de la política general de seguridad y privacidad de la información. Guía No. 8 - Controles de Seguridad y Privacidad de la Información	Plazo: Primer Trimestre. Evidencia: Documento Política Seguridad de la Información aprobado.
		Revisión y actualización manual de políticas de seguridad de la información de acuerdo con la actualización de la norma NTC/ISO/IEC 27001:2022.		Plazo: Segundo Semestre. Evidencia: Manual de políticas de seguridad de la información actualizado.
		Revisión de la política de seguridad de la información por la alta dirección.		Plazo: Segundo Semestre. Evidencia: Acta de reunión revisión con la participación de la Oficina TIC.
		Revisión de aplicación de controles establecidos en el Manual de Políticas de Seguridad de la Información por parte de los funcionarios.		Plazo: Semestral. Evidencia: Informe de seguimiento a la adopción de controles.
Implementación de controles.	Madurez dominio responsabilidades y organización seguridad de la información.	Revisión matriz de roles y responsabilidades del SGSI.	Guía No. 4 - Roles y Responsabilidades. Guía No. 5 - Guía para la Gestión y Clasificación de Activos de Información. Guía No. 8 - Controles de Seguridad de la Información.	Plazo: Segundo Trimestre. Evidencia: Matriz de Roles y responsabilidades ajustada. (En caso de requerirse).
		Asignación de responsables por cada activo de información definido, documentando detalles de su responsabilidad frente al activo.		Plazo: Cuarto Trimestre. Evidencia: Soportes de la asignación de responsables por los activos de información definidos.

		Definir y documentar los niveles de autorización.		Plazo: Tercer Trimestre. Evidencia: Documento niveles de autorización aprobado.
		Revisión política para dispositivos móviles (incluyendo registros de ingresos a la entidad, protección física, restricción instalación de software, controles de acceso, des habilitación remota, borrado y cierre).		Plazo: Primer Semestre. Evidencia: Documento con los lineamientos para dispositivos móviles ajustado. (En caso de requerirse).
		Seguimiento a la implementación de la Política de Teletrabajo.		Plazo: Semestral. Evidencia: Informe de seguimiento a la implementación de la Política de Teletrabajo.
Implementación de controles.	Madurez dominio Seguridad de los recursos humano.	Revisión acuerdos de confidencialidad y no divulgación a funcionarios y contratistas.	Guía No. 3 - Procedimiento de Seguridad de la Información Guía No. 4 - Roles y responsabilidades. Guía No. 8 - Controles de Seguridad de la Información. Guía No. 14 - Plan de comunicación, sensibilización, capacitación.	Plazo: Segundo Trimestre. Evidencia: Acuerdos de confidencialidad y no divulgación ajustados. (En caso de requerirse).
		Revisiones manuales de personal, donde se documenten los derechos y deberes como funcionarios en cuanto a la seguridad de la información.		Plazo: Segundo Semestre. Evidencia: Manuales de personal ajustados.
		Promover el uso de canales habilitados para el reporte anónimo de incumplimiento a las políticas y procedimientos de seguridad de la información		Plazo: Segundo Trimestre. Evidencia: Soportes socialización de canales habilitados con los funcionarios.

		"denuncias internas, PQRS".		
Implementación de controles.	Madurez dominio gestión de activos.	Ejecución guía dominio de sistemas de información.	Guía No. 5 - Gestión Clasificación de Activos. Guía No. 8 - Controles de Seguridad de la Información. Guía Dominio sistemas de información ALFM.	Plazo: Tercer Trimestre. Evidencia: Documentos creados y ajustados de acuerdo con los lineamientos establecidos.
		Revisión control establecido para la devolución de activos físicos y electrónicos entregados previamente por la entidad.		Plazo: Segundo Trimestre. Evidencia: Control y documentos ajustados (En caso de requerirse).
		Protocolos para la gestión de medios removibles, de acuerdo con el esquema de clasificación adoptado en la entidad, (Verificación implementación para el uso de red wifi).		Plazo: Tercer Trimestre. Evidencia: Ajuste y/o creación de procedimientos. (En caso de requerirse).
Implementación de controles.	Madurez dominio cumplimiento.	Revisión proceso para salvaguardar los registros, donde se deben emitir directrices para la retención, almacenamiento, manejo y disposición de registros (logs) e información.	Guía No. 6 - Gestión Documental.	Plazo: Primer Semestre. Evidencia: Lineamientos y/o documentos ajustados (En caso de requerirse).
		Actualización política de tratamiento de datos personales.	Ley 1581 del 17 de octubre de 2022.	Plazo: Trimestral. Evidencia: Documentos identificación de brechas, identificación de áreas involucradas en su aplicación y Política tratamiento

				de datos personales actualizada.
Implementación de controles.	Madurez dominio relaciones con los proveedores.	Revisión control seguridad de la información para las relaciones con los proveedores, incluyendo el tratamiento de la seguridad dentro de los acuerdos, cadena de suministro de tecnología de la información y comunicación.	Guía No. 8 - Controles de Seguridad de la Información.	Plazo: Primer Semestre. Evidencia: Control y documentos ajustados (En caso de requerirse).
Implementación de controles.	Madurez dominio control de acceso.	Revisión política control de acceso, con base en los requisitos de negocio y de seguridad de la información.	Guía No. 8 - Controles de Seguridad de la Información.	Plazo: Primer Semestre. Evidencia: Control y documentos ajustados (En caso de requerirse).
		Revisión y/o ajuste al uso de redes y servicios de red.		Plazo: Primer Semestre. Evidencia: Documento de lineamientos revisado y/o ajustado.
		Revisión y seguimiento al uso de navegación web, de acuerdo con los perfiles asignados a los funcionarios.		Plazo: Semestral. Evidencia: Informes de revisión y seguimiento al uso de red (Perfiles de navegación medio y alto).
		Reporte de novedades de personal (retiros, incapacidades, licencias, vacaciones, entre otros).		Plazo: Bimestral. Evidencia: Soportes del reporte previo mediante correo electrónico de las novedades de personal emitidos a la Oficina TIC.
Implementación de controles.	Madurez dominio Criptografía.	Revisión lineamientos para la aplicación de controles criptográficos.	Guía No. 8 - Controles de Seguridad de la Información.	Plazo: Segundo Semestre. Evidencia: Registro de verificaciones.

Implementación de controles.	Madurez dominio Seguridad física y del entorno.	Revisión y/o ajustes perímetros de seguridad física, con el fin de proteger áreas que contengan información sensible o critica, e instalaciones de manejo de información.	Guía No. 8 - Controles de Seguridad de la Información.	Plazo: Segundo Semestre. Evidencia: Control y documentos ajustados (En caso de requerirse).
		Revisión y/o ajuste del formato de mantenimiento preventivo y/o correctivo a hardware y software.		Plazo: Primer Semestre. Evidencia: Formatos ajustados, aprobados y socializados. (En caso de requerirse).
		Revisión y/o elaboración plan de mantenimiento a la infraestructura tecnológica de la entidad, asegurando la disponibilidad e integridad continua.		Plazo: Primer Trimestre. Evidencia: Plan de mantenimiento a la infraestructura tecnológica.
		Revisión y/o ajuste de formatos para la salida de elementos de la entidad.		Plazo: Segundo Trimestre. Evidencia: Formatos ajustados (En caso de requerirse).
Implementación de controles.	Madurez dominio seguridad de las operaciones.	Revisión, ajuste y/o creación de formatos para la gestión de cambios.	Guía No. 8 - Controles de Seguridad de la Información.	Plazo: Segundo Trimestre. Evidencia: Formatos ajustados (En caso de requerirse).
		Definición y/o ajuste de documentos para la separación de ambientes de desarrollo, pruebas y operación.		Plazo: Segundo Trimestre. Evidencia: Formatos ajustados (En caso de requerirse).
		Revisión periódica del funcionamiento del antivirus adquirido por la entidad.		Plazo: Semestral. Evidencia: Informes de seguimiento al funcionamiento del antivirus.
Gestión de incidentes.	Prevención de eventos de	Intercambiar y/o compartir con el	Guía No. 3 - Procedimiento de	Plazo: Trimestral.

	seguridad informática.	CSIRT, COLCERT, CAIVIRUTAL, (DIJIN) y CCOC para apoyar la gestión de riesgos y la toma de decisiones (priorización, tratamiento y aceptación, respuesta a incidentes), especialmente, para prevenir interna y externamente amenazas cibernéticas.	Seguridad de la Información. Guía No. 8 - Controles de Seguridad de la Información.	Evidencia: Mensajes de correos electrónicos generados. (Actividad que se encuentra integrada al Plan de Tratamiento de Riesgos de Seguridad de la Información – PTR.)
		Informes de seguimiento a los eventos de seguridad presentados (Fortisandbox).		Plazo: Trimestral. Evidencia: Informes de seguimiento eventos de seguridad. (Actividad que se encuentra integrada al Plan de Tratamiento de Riesgos de Seguridad de la Información – PTR.)

10. SEGUIMIENTO

Articulación con el Plan de Acción Institucional 2022.

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 seguridad y privacidad de la información - PESI.

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

11. ANALISIS Y MEDICIÓN

Seguimiento mediante el instrumento de Autodiagnóstico de MINTIC.

12. CONTROL DE CAMBIOS

VERSIÓN	DESCRIPCIÓN DE CAMBIOS
00	Documento inicial según NMO.
01	Se actualiza el Plan para el año 2019
02	Se actualiza el Plan para el año 2020
03	Se actualiza el Plan para el año 2021
04	Se actualiza el Plan para el año 2022
05	Se actualiza Normativa de acuerdo a Decretos, Resoluciones y Directivas presidenciales para la vigencia 2022 Ajuste de fechas para la ejecución de actividades
06	Se actualiza el Plan para el año 2023.

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 de que se requiera)	Responsable de Aprobar la Tarea en la SVE
Seguimiento a la implementación del Modelo de Seguridad y Privacidad de la Información – MSPI.	Informe de seguimiento a la implementación del MSPI – Instrumento del MSPI actualizado.	01-01-2023 01-07-2023	07-07-2023 05-01-2024	Oficina TIC.	Gestión de TIC.	Profesional Defensa.	N/A	Jefe Oficina TIC.
Actualización inventario de activos de información.	Matriz de activos de información.	01-01-2023 01-07-2023	07-07-2023 05-01-2024	Oficina TIC.	Gestión de TIC.	Profesional Defensa. Técnicos Regionales.	N/A Profesional Defensa Oficina TIC.	Jefe Oficina TIC. Jefe Oficina TIC.
Creación e implementación del Plan Institucional de Continuidad del negocio.	Documentos creados, actualizados y aprobados ante el SIG.	01-01-2023	07-07-2023	Oficina Asesora de Planeación e Innovación Institucional.	Gestión de Direccionamiento Estratégico.	Profesional Defensa.	Profesional Defensa Oficina Asesora de Planeación e Innovación Institucional.	Jefe Oficina TIC.
Gestión plan de continuidad del negocio – Gestión TIC	Seguimiento al estado avance del Plan.	01-01-2023 01-07-2023	07-07-2023 05-01-2024	Oficina TIC.	Gestión de TIC.	Profesional Defensa.	N/A	Jefe Oficina TIC.
Plan de actividades de sensibilización y concientización en temas relacionados a seguridad digital y de la	Plan de sensibilización y capacitación a los funcionarios de la ALFM – Informes	01-01-2023 01-05-2023 01-09-2023	05-05-2023 08-09-2023 05-01-2024	Oficina TIC.	Gestión de TIC.	Profesional Defensa.	N/A	Jefe Oficina TIC.

información dirigido a todos los funcionarios de la entidad.	de seguimiento a las capacitaciones.							
Política de seguridad de la información “General” aprobada por la Alta Dirección.	Documento Política seguridad de la información aprobado.	01-01-2023	05-04-2023	Oficina TIC.	Gestión de TIC.	Profesional Defensa.	N/A	Jefe Oficina TIC.
Revisión y actualización manual de políticas de seguridad de la información de acuerdo con la actualización de la norma NTC/ISO/IEC 27001:2022.	Documento Manual de políticas de seguridad de la información actualizado.	01-07-2023	05-01-2024	Oficina TIC.	Gestión de TIC.	Profesional Defensa.	N/A	Jefe Oficina TIC.
Revisión de la política de seguridad de la información por la alta dirección.	Acta de reunión revisión alta dirección.	01-07-2023	05-01-2024	Oficina TIC.	Gestión de TIC.	Profesional Defensa.	N/A	Jefe Oficina TIC.
Revisión de aplicación de controles establecidos en el Manual de Políticas de Seguridad de la Información por parte de los funcionarios.	Informe de seguimiento a la adopción de controles.	01-01-2023 01-07-2023	07-07-2023 05-01-2024	Oficina Control Interno	Gestión Control Interno.	Profesional Defensa.	Profesional Defensa Oficina TIC.	Jefe Oficina TIC.
Revisión matriz de roles y responsabilidades del SGSI.	Matriz de Roles y responsabilidades ajustada. (En caso de requerirse).	01-04-2023	07-07-2023	Oficina TIC.	Gestión de TIC.	Profesional Defensa.	N/A	Jefe Oficina TIC.
Asignación de responsables por cada activo de información definido, documentando	Soportes de la asignación de responsables por los activos de	01-09-2023	05-01-2024	Oficina TIC.	Gestión de TIC.	Profesional Defensa.	N/A	Jefe Oficina TIC.

detalles de su responsabilidad frente al activo.	información definidos.							
Definir y documentar los niveles de autorización.	Documento niveles de autorización aprobado.	01-07-2023	06-10-2023	Oficina TIC.	Gestión de TIC.	Profesional Defensa.	Profesional Defensa Oficina TIC.	Jefe Oficina TIC.
Revisión lineamientos para dispositivos móviles (incluyendo registros de ingresos a la entidad, protección física, restricción instalación de software, controles de acceso, des habilitación remota, borrado y cierre).	Documento con los lineamientos para dispositivos móviles ajustado. (En caso de requerirse).	01-01-2023	07/07/2023	Dirección Administrativa y de Talento Humano. Oficina TIC.	Gestión Administrativa. Gestión de TIC.	Profesional Defensa.	Profesional Defensa Oficina TIC.	Jefe Oficina TIC.
Seguimiento a la implementación de la Política de Teletrabajo.	Informe de seguimiento a la implementación de la Política de Teletrabajo.	01-01-2023 01-07-2023	07-07-2023 05-01-2024	Dirección Administrativa y de Talento Humano.	Gestión de Talento Humano	Profesional Defensa.	Profesional Defensa Oficina TIC.	Jefe Oficina TIC.
Revisión acuerdos de confidencialidad y no divulgación a funcionarios y contratistas.	Acuerdos de confidencialidad y no divulgación ajustados. (En caso de requerirse).	01-04-2023	07-07-2023	Oficina TIC. Dirección Administrativa y de Talento Humano.	Gestión de TIC. Gestión de Talento Humano.	Profesional Defensa.	N/A	Jefe Oficina TIC.
Revisiones manuales de personal, donde se documenten los derechos y deberes como funcionarios en	Manuales de personal ajustados.	01-07-2023	05-01-2024	Dirección Administrativa y de Talento Humano.	Gestión de Talento Humano.	Profesional Defensa.	Profesional Defensa Oficina TIC.	Jefe Oficina TIC.

cuanto a la seguridad de la información.								
Promover el uso de canales habilitados para el reporte anónimo de incumplimiento a las políticas y procedimientos de seguridad de la información “denuncias internas, PQRS”.	Soportes socialización de canales habilitados con los funcionarios.	01-04-2023	07-07-2023	Secretaria General.	Grupo de Atención y Orientación Ciudadana.	Profesional Defensa.	Profesional Defensa Oficina TIC.	Jefe Oficina TIC.
Ejecución guía dominio de sistemas de información.	Documentos creados y ajustados de acuerdo con los lineamientos establecidos.	01-07-2023	06-10-2023	Oficina TIC.	Gestión de TIC.	Profesional Defensa.	N/A	Jefe Oficina TIC.
Revisión control establecido para la devolución de activos físicos y electrónicos entregados previamente por la entidad.	Control y documentos ajustados (En caso de requerirse).	01/07/2023	06/10/2023	Dirección Administrativa y de Talento Humano.	Gestión de Talento Humano.	Profesional Defensa.	Profesional Defensa Oficina TIC.	Jefe Oficina TIC.
Protocolos para la gestión de medios removibles, de acuerdo con el esquema de clasificación adoptado en la entidad, (Verificación implementación para el uso de red wifi).	Ajuste y/o creación de procedimientos. (En caso de requerirse).	01-07-2023	06-10-2023	Oficina TIC.	Gestión de TIC.	Profesional Defensa.	Profesional Defensa Oficina TIC.	Jefe Oficina TIC.

Revisión proceso para salvaguardar los registros, donde se deben emitir directrices para la retención, almacenamiento, manejo y disposición de registros (logs) e información.	Lineamientos y/o documentos ajustados (En caso de requerirse).	01-01-2023	07-07-2023	Oficina TIC.	Gestión de TIC.	Profesional Defensa.	Profesional Defensa Oficina TIC.	Jefe Oficina TIC.
Actualización política de tratamiento de datos personales.	Documento identificación de brechas de la política de tratamiento de datos personales actual vs objetivo, de acuerdo a los lineamientos establecidos por la ley 1581/2012.	1/01/2023	7/04/2023	Oficina TIC.	Gestión de TIC.	Profesional Defensa.	N/A	Jefe Oficina TIC.
	Documento identificación de áreas que capturan información correspondiente a datos personales, a nivel interno y externo.	1/04/2023	7/07/2023	Secretaria General.	Grupo de Atención y Orientación Ciudadana	Profesional Defensa.	N/A	Jefe Oficina TIC.
	Gestión mesas de trabajo para llevar a cabo la actualización de la política de	1/07/2023	5/01/2024	Oficina Asesora de Planeación e Innovación Institucional.	Gestión de Direccionamiento Estratégico.	Profesional Defensa.	N/A	Jefe Oficina TIC.

	tratamiento de datos personales.							
Revisión control seguridad de la información para las relaciones con los proveedores, incluyendo el tratamiento de la seguridad dentro de los acuerdos, cadena de suministro de tecnología de la información y comunicación.	Control y documentos ajustados (En caso de requerirse).	01-01-2023	07-07-2023	Subdirección General de Contratación.	Gestión de la Contratación	Profesional Defensa.	Profesional Defensa Oficina TIC.	Jefe Oficina TIC.
Revisión política control de acceso, con base en los requisitos de negocio y de seguridad de la información.	Control y documentos ajustados (En caso de requerirse).	01-01-2023	07-07-2023	Dirección Administrativa y de Talento Humano. Oficina TIC.	Gestión Administrativa. Gestión de TIC.	Profesional Defensa.	Profesional Defensa Oficina TIC.	Jefe Oficina TIC.
Revisión y/o ajuste al uso de redes y servicios de red.	Documento de lineamientos revisado y/o ajustado.	01-01-2023	07-07-2023	Oficina TIC.	Gestión de TIC.	Profesional Defensa.	Profesional Defensa Oficina TIC.	Jefe Oficina TIC.
Revisión y seguimiento al uso de navegación web, de acuerdo con los perfiles asignados a los funcionarios.	Informes de revisión y seguimiento al uso de red (Perfiles de navegación medio y alto).	01-01-2023 01-07-2023	07-07-2023 05-01-2024	Oficina TIC.	Gestión de TIC.	Profesional Defensa.	Profesional Defensa Oficina TIC.	Jefe Oficina TIC.
Reporte de novedades de personal (retiros, incapacidades,	Soportes del reporte previo mediante correo	01/01/2023 01/03/2023 01/05/2023	07/03/2023 05/05/2023 07/07/2023	Dirección Administrativa	Gestión de Talento Humano.	Profesional Defensa.	Profesional Defensa Oficina TIC.	Jefe Oficina TIC.

licencias, vacaciones, entre otros).	electrónico de las novedades de personal emitidos a la Oficina TIC.	01/07/2023 01/09/2023 01/11/2023	07/09/2023 09/11/2023 05/01/2024	y de Talento Humano.				
Revisión lineamientos para la aplicación de controles criptográficos.	Registro de verificaciones.	01-07-2023	05-01-2024	Oficina TIC.	Gestión de TIC.	Profesional Defensa.	N/A	Jefe Oficina TIC.
Revisión y/o ajuste del formato de mantenimiento preventivo y/o correctivo a hardware y software.	Formatos ajustados, aprobados y socializados. (En caso de requerirse).	01-01-2023	07/07/2023	Oficina TIC.	Gestión de TIC.	Profesional Defensa.	Profesional Defensa Oficina TIC.	Jefe Oficina TIC.
Revisión y/o elaboración plan de mantenimiento a la infraestructura tecnológica de la entidad, asegurando la disponibilidad e integridad continua.	Plan de mantenimiento a la infraestructura tecnológica.	01-01-2023	10/04/2023	Oficina TIC.	Gestión de TIC.	Profesional Defensa.	Profesional Defensa Oficina TIC.	Jefe Oficina TIC.
Revisión y/o ajuste de formatos para la salida de elementos de la entidad.	Formatos ajustados (En caso de requerirse).	01-04-2023	07-07-2023	Dirección Administrativa y de Talento Humano.	Gestión de Talento Humano.	Profesional Defensa.	Profesional Defensa Oficina TIC.	Jefe Oficina TIC.
Revisión, ajuste y/o creación de formatos para la gestión de cambios.	Formatos ajustados (En caso de requerirse).	01-04-2023	07-07-2023	Oficina TIC.	Gestión de TIC.	Profesional Defensa.	N/A	Jefe Oficina TIC.
Definición y/o ajuste de documentos para la separación de ambientes de desarrollo, pruebas y operación.	Formatos ajustados (En caso de requerirse).	01-04-2023	07-07-2023	Oficina TIC.	Gestión de TIC.	Profesional Defensa.	Profesional Defensa Oficina TIC.	Jefe Oficina TIC.

Revisión periódica del funcionamiento del antivirus adquirido por la entidad.	Informes de seguimiento al funcionamiento del antivirus.	01-01-2023 01-07-2023	07-07-2023 05-01-2024	Oficina TIC.	Gestión de TIC.	Profesional Defensa	Profesional Defensa Oficina TIC.	Jefe Oficina TIC.