AGENCIA LOGÍSTICA
FUERZAS MILITARES
La unión de nuestras Fuerzas

PLAN TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN – PTR.

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 13:04:40 -05'00'				**FIRMA** Ing. Daris Yaneth Padilla Díaz Firmado digitalmente por Ing. Daris Yaneth Padilla Díaz Fecha: 2023.01.30 14:20:48 -05'00'				**FIRMA** César González Firmado digitalmente por César González Fecha: 2023.01.30 13:53:38 -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 15:36:55 -05'00'				**FIRMA** Diana marlen Caicedo Benavides Firmado digitalmente por Diana marlen Caicedo Benavides Fecha: 2023.01.30 14:38:11 -05'00'				**FIRMA** Jaime Morón Barros Firmado digitalmente por Jaime Morón Barros Fecha: 2023.01.31 09:16:00 -05'00'			
PROCESO y/o DEPENDENCIA:				**Oficina Tecnologías de la Información y las Comunicaciones**							

TABLA DE CONTENIDO

1. GENERALIDADES.

Desde un principio los factores de riesgo estaban asociados principalmente a contingencias de carácter natural y tecnológico, las consecuencias derivadas de sucesos posteriores y relevantes como el terrorismo, la inestabilidad política, las pandemias y los códigos maliciosos, entre otros, han señalado la necesidad de incorporar nuevas amenazas presentes no solamente en el mundo físico sino también en el entorno digital, cuando se trate de comprender los riesgos más significativos a los activos de información.

El análisis de riesgos de los activos de información nos permite entender de una manera efectiva y eficiente los riesgos de pérdida de confidencialidad, integridad y disponibilidad sobre cada uno de los activos definidos como parte del alcance del análisis.

Gestionar eficazmente la seguridad de la información y riesgos de seguridad digital de los sistemas de información de la entidad, así como en los activos que participan en sus procesos y que se encuentran expuestos, permite garantizar la confidencialidad, integridad y disponibilidad de la información a través de la aplicación de las opciones apropiadas de tratamiento de riesgos de Seguridad de la información y seguridad digital, teniendo en cuenta la evaluación de los resultados de la valoración de los riesgos del Sistema de Gestión de Seguridad de la Información y en concordancia a la normativa aplicable.

Así mismo, este plan apoya la implementación de controles y acciones tendientes a la mitigación de los riesgos del proceso de gestión tecnológica, hallazgos de auditorías internas y apoya el cumplimiento del Modelo Integrado de Planeación y Gestión – MIPG y a la implementación del Modelo de Seguridad y Privacidad de la Información - MSPI del Ministerio de Tecnologías de la Información y las Comunicaciones MinTIC, dentro de su política de gobierno Digital.

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:

Activo: En el contexto de seguridad digital son elementos tales como aplicaciones de la organización, servicios web, redes, Hardware, información física o digital, documentación, recurso humano, entre otros, que utiliza la organización para funcionar.

Activo de Información: en el contexto de la norma ISO/IEC 27001 es: “algo que una organización valora y por lo tanto debe proteger”.

Activos tecnológicos: Se consideran activos tecnológicos 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. El análisis de riesgos proporciona la base para la estimación de riesgos y las decisiones sobre el tratamiento de riesgos. El análisis de riesgos incluye la estimación de riesgos. (ISO/IEC 27000).

Backups (copia de respaldo): Una copia de seguridad o de respaldo es una copia de los datos originales que se realiza fuera de la infraestructura original con el fin de disponer de un medio de recuperación en caso de un desastre o pérdida.

Base de Datos: Es un "almacén digital" que permite guardar grandes cantidades de información de forma organizada para luego poderla encontrar y utilizar fácilmente. Una base de datos se puede definir como un conjunto de información relacionada que se encuentra agrupada y estructurada. Desde el punto de vista informático, la base de datos es un sistema formado por un conjunto de datos almacenados en discos que permiten el acceso directo a ellos y un conjunto de programas que manipulan ese conjunto de datos. En el caso de la Agencia Logística, las bases de datos más utilizadas son Oracle y MySQL.

Buzón de correo electrónico: Depósito en el que se almacenan los mensajes de correo que llegan a un destinatario determinado.

Clasificación de la información: La información se debería clasificar en función de los requisitos legales, valor, criticidad y susceptibilidad a divulgación o a modificación no autorizada.

Confidencialidad: Propiedad de la información que la hace no disponible o sea divulgada a individuos, entidades o procesos no autorizados.

Contraseña o password: Es una clave secreta de acceso a un computador, a una cuenta de correo electrónico, a una cuenta de conexión a Internet, a un sistema de información o a una base de datos, que, en aras de maximizar los niveles de seguridad, control y privacidad, sólo debe conocer el usuario. Si se introduce una contraseña incorrecta, no se permitirá la entrada al sistema.

Control: Medida que permite reducir o mitigar un riesgo.

Correo electrónico o e-mail: Es un servicio mediante el cual un computador permite a los usuarios enviar y recibir mensajes e intercambiar información con otros usuarios (o grupos de usuarios), todo a través de la red.

Cortafuegos (firewall): Se trata de un dispositivo o conjunto de dispositivos configurados para permitir, limitar, cifrar, o descifrar el tráfico entre los diferentes ámbitos sobre la base de un conjunto de normas y otros criterios.

Dirección de correo electrónico o e-mail address: Conjunto de caracteres utilizado para identificar a un usuario de correo electrónico y que permiten la recepción y envío de mensajes. Generalmente está compuesta por el nombre del usuario, el signo @ como divisor entre el usuario y el nombre del proveedor del servicio en el cual se aloja la cuenta de correo (el dominio).

Disponibilidad: Propiedad de ser accesible y utilizable a demanda por una entidad.

Equipo de cómputo: Es una máquina electrónica dotada de una memoria de gran capacidad y de métodos de tratamiento de la información, que permiten resolver problemas aritméticos y lógicos, gracias

a la utilización de programas instalados en ella. Para efectos de este manual se emplea el término como sinónimo de computador (PC-Computadores personales y portátiles).

Equipo servidor: Es una máquina electrónica dotada de una alta configuración (velocidad de procesamiento, alta memoria, alta capacidad de almacenamiento. etc.), en donde están almacenados los programas de software aplicativo que operan en red y las bases de datos de la entidad.

Etiquetado de la información: Se debería desarrollar e implementar un conjunto adecuado de procedimientos para el etiquetado de la información, de acuerdo con el esquema de clasificación de información adoptado por la organización.

Gobierno Digital: es la política de MIPG que busca promover el uso y aprovechamiento de las Tecnologías de la Información y las Comunicaciones -TIC, para consolidar un Estado y ciudadanos competitivos, proactivos, e innovadores, que generen valor público en un entorno de confianza digital. La política de Gobierno Digital contribuye a la Transformación Digital del sector público, la cual implica un cambio en los procesos, la cultura y el uso te de la tecnología (principalmente tecnologías emergentes y de la Cuarta Revolución Industrial), para el mejoramiento de las relaciones externas de las entidades de Gobierno, a través de la prestación de servicios más eficientes (Manual Operativo MIPG V3).

Hardware: Conjunto de componentes físicos (cables, placas, conexiones, partes) que constituyen un computador y sus equipos periféricos. Es la parte física de un computador, lo tangible.

Ingeniería Social: Es la práctica de obtener información confidencial a través de la manipulación de usuarios legítimos. Es una técnica que pueden usar ciertas personas, tales como investigadores privados, criminales, o delincuentes computacionales, para obtener información, acceso o privilegios en sistemas de información que les permitan realizar algún acto que perjudique o exponga la persona u organismo comprometido a riesgo o abusos.

Integridad: Propiedad de exactitud y completitud.

Internet (internacional Net): Nombre de la mayor red informática del mundo. Red de telecomunicaciones nacida en 1969 en los Estados Unidos a la cual están conectadas centenares de millones de personas, organismos y empresas, en su mayoría ubicadas en los países más desarrollados, y cuyo rápido desarrollo está teniendo importantes efectos sociales, económicos y culturales, convirtiéndose de esta manera en uno de los medios más influyentes de la llamada Sociedad de la Información, siendo conocido en algunos ámbitos con el nombre de la autopista de la información.

Intranet: Se llaman así a las redes tipo internet pero que son de uso interno o corporativo.

Inventario de activos: Se deben identificar los activos asociados con la información y las instalaciones de procesamiento de información, y se debería elaborar y mantener un inventario de estos activos.

Manejo de activos: Se deberían desarrollar e implementar procedimientos para el manejo de activos, de acuerdo con el esquema de clasificación de información adoptado por la organización.

Medio compartido de información (file share): Ubicación lógica en un servidor donde una dependencia o grupo de personas pueden colocar información (archivos y carpetas) para ser compartida y actualizada por el grupo. Solo las personas pertenecientes al grupo pueden ver y consultar la información.

Mensaje de correo electrónico: Conjunto de elementos que componen un envío de correo electrónico. Además de los elementos visibles al usuario (campos de: Para: Asunto: CC: cuerpo del mensaje, firma,

archivos anexos, etc.), un mensaje de correo electrónico contiene también elementos ocultos, que solo pueden ser "abiertos" por los destinatarios a los que se le remiten.

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 un marco de referencia para dirigir, planear, ejecutar, hacer seguimiento, evaluar y controlar la gestión de las entidades y organismos públicos, con el fin de generar resultados que atiendan los planes de desarrollo y resuelvan las necesidades y problemas de los ciudadanos, con integridad y calidad en el servicio. Es en sí mismo un modelo de gestión de calidad ya que se fundamenta en generar resultados que satisfagan las necesidades y atiendan los problemas de los ciudadanos. Es en torno a estos resultados que deben girar todas sus actuaciones y decisiones (Manual Operativo MIPG V3).

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).

Red: Conjunto de computadores o de equipos informáticos conectados entre sí de tal manera que pueden intercambiar información.

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

Riesgo de Corrupción: Posibilidad de que, por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado

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).

Spam: Mensajes que sin ser solicitados llegan al buzón de correo, provenientes de direcciones desconocidas en la mayoría de los casos, muy frecuentemente encaminados a ofrecer productos y servicios. También son conocidos como "correo basura" y algunos de ellos, por ser mensajes que se distribuyen masivamente, son utilizados para transmitir virus informáticos.

Software: Es un conjunto de instrucciones detalladas que controlan la operación de un sistema computacional. En general, designa los diversos tipos de programas, instrucciones y reglas informáticas para ejecutar distintas tareas en un computador. Dentro de sus funciones están el administrar los recursos de cómputo, proporcionar las herramientas para optimizar estos recursos y actuar como intermediario entre el usuario y la información almacenada.

Software aplicativo: Programas que son escritos para realizar una tarea específica mediante el computador y está orientado a dar cubrimiento a un proceso específico. Son los denominados "software de aplicación específica". Este tipo de software está desarrollado sobre los denominados lenguajes de

programación (C, Cobol, Developer, .Net, Java, PHP, entre otros), y los de mayor prestación y alto manejo de volúmenes de información están implementados sobre Bases de Datos (Oracle, MySQL, PosgreSql, etc.) en donde reside organizadamente la información que es manejada por intermedio del software aplicativo.

Software de ofimática: Son programas existentes en el mercado y que basados en un computador, dan cubrimiento a necesidades específicas que se gestionan normalmente en una oficina: procesamiento de textos, hojas de cálculo, diseño de gráficos, resolución de problemas matemáticos, elaboración de presentaciones, entre otras. Tanto el software aplicativo como el de ofimática, deben estar sobre el software del sistema (sistema operativo) para poder operar.

Software del sistema: Es un conjunto de programas que administran y controlan los recursos del computador, como son la unidad central de proceso, dispositivos de comunicaciones y los dispositivos periféricos. Es el denominado Sistema Operativo (Windows, Unix, Linux, Android, IOS entre otros).

Software libre: Es aquel que no tiene ningún tipo de restricciones de uso, distribución, modificación o elaboración de copias. Es de denominado software GPL-General Public License, el cual permite a cualquier entidad en el hacer uso de la herramienta, estudiarla, modificarla y redistribuirla.

Software licenciado: Programas o aplicativos que han sido registrados y patentados, sobre los que existen derechos de autor y normas acerca de su uso, distribución, elaboración de copias, etc. Como consecuencia, para su utilización es necesario cumplir las restricciones establecidas por la ley.

Software no licenciado: Es aquel que aún no ha sido patentado o registrado.

Software pirata: Es una copia ilegal de un software (del sistema, aplicativo, o de ofimática), cuya utilización se está efectuando sin tener la licencia otorgada por el fabricante y proveedor del mismo.

Suplantación: Es la acción para referirse a los abusos informáticos cometidos por delincuentes para estafar, obtener información personal, contraseñas, etc. de forma ilegal o no autorizada.

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.

Teletrabajo: Es una forma flexible de organización del trabajo que consiste en el desempeño de la actividad profesional sin la presencia física del trabajador en la empresa durante una parte importante de su horario laboral. Engloba una amplia gama de actividades y puede realizarse a tiempo completo o parcial.

Transacción: Es una interacción entre el usuario final del software y el sistema (software y bases de datos), la cual está compuesta por varios procesos internos que se han de aplicar uno después del otro.

Unidad de almacenamiento fija: Dispositivo(s) no removible(s) por el usuario final que permite(n) registrar y guardar información en un equipo de cómputo. Generalmente conocida como disco duro, tiene una gran capacidad, lo que le permite almacenar una gran cantidad de información, programas y datos.

Unidad de almacenamiento portátil (CD, DVD, memoria USB): Dispositivos removibles por el usuario final, que permiten registrar y guardar información, programas y datos para ser utilizados en un computador. Entre los más usados y conocidos están el CD, el DVD y la memoria USB.

Virus: Programa o rutina de software, cuyo objetivo generalmente es causar daños en un sistema informático. Con tal fin se oculta o se disfraza para no ser detectado. Estos programas son de diferentes tipos y pueden causar problemas de diversa gravedad en los sistemas a los que afectan, desde borrar un tipo de archivos, hasta borrar toda la información contenida en el disco duro. Hoy en día se propagan fundamentalmente mediante el uso del correo electrónico y de medios de almacenamiento de información portátiles infectados como CD, DVD y memorias USB. Se combaten con la instalación de un antivirus que debe ser actualizado periódicamente.

VPN: (Virtual Private Network): Es una tecnología de red que se utiliza para conectar una o más computadoras a una red privada utilizando servicio de conexión a Internet.

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:

Establecer las actividades que se ejecutarán en la vigencia 2023 para mitigar y hacer seguimiento a los riesgos de seguridad y privacidad de la información que se puedan presentar en la ALFM, con el fin de proteger y preservar la información, así como los elementos tecnológicos que la soportan. Este documento es el resultado de la identificación del riesgo y su tratamiento, así como el manejo y seguimiento a los controles establecidos en la ALFM para la protección de los activos informáticos.

4.2. OBJETIVOS ESPECIFICOS:

Definir y aplicar los lineamientos para tratar de manera integral los riesgos de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación que la ALFM pueda estar expuesto, y de esta manera alcanzar los objetivos, la misión y la visión institucional, protegiendo y preservando la integridad, confidencialidad, disponibilidad y autenticidad de la información.

Cumplir con los requisitos legales y reglamentarios pertinentes a la legislación colombiana.

Gestionar riesgos de Seguridad y Privacidad de la información, Seguridad Digital y Continuidad de la Operación, de acuerdo con los contextos establecidos en la Entidad.

Fortalecer y apropiar conocimiento referente a la gestión de riesgos Seguridad y Privacidad de la información, Seguridad Digital y Continuidad de la Operación.

5. ALCANCE.

El Modelo de Seguridad y Privacidad de la Información (MSPI) establece los lineamientos, actividades y responsabilidades que deben ser cumplidos por los directivos, funcionarios, contratistas y terceros que presten sus servicios o tengan algún tipo de relación con la Agencia Logística de las Fuerzas Militares – ALFM, para el tratamiento, manejo y seguimiento a los riesgos de seguridad y privacidad de la información.

En el análisis realizado se tuvieron en cuenta aspectos que involucraron a todos los procesos, y el tratamiento de los riesgos y la aplicación de controles se hizo sobre aquellos riesgos que se encuentran en un nivel de criticidad medio y alto. Los riesgos de nivel bajo hacen parte del riesgo residual aceptado por la ALFM dentro de su política de seguridad informática y también hacen parte del tratamiento de riesgos presente en este plan.

Se definirán las actividades a cumplir durante la presente vigencia (2023) para avanzar en la implementación del MSPI, aplicando el tratamiento, manejo y seguimiento a los riesgos identificados y de acuerdo a los controles establecidos. Para esta labor se involucrarán todos los procesos de la ALFM, los cuales deberán entregar la información que se requiera al grupo encargado de adelantar la gestión de los riesgos identificados.

6. MAPA DE RIESGOS.

RIESGO	***DESCRIPCIÓN***	***CAUSAS***	***EFECTOS***	***ANTES DE LOS CONTROLES***			***CONTROLES***	***DESPUÉS DE LOS CONTROLES***			***OPCIÓN DE MANEJO***	***INSTITUCIONAL***	***DE CORRUPCIÓN***
				PROBABILIDAD	***IMPACTO***	***ZONA INHERENTE***		***PROBABILIDAD***	***IMPACTO***	***ZONA RESIDUAL***			
Alteración o manipulación de sistemas y datos	*Por ofrecimiento de terceros de dinero o beneficios a personal de la ALFM para manipular o alterar los sistemas o la información de la Agencia Logística Por presencia de malware. Por falta de capacitación del personal. Por fallas técnicas no previstas. Por un mantenimiento deficiente y falta de soporte.*	*Interés de agentes externos de perjudicar la imagen institucional. Posibilidad de obtener beneficios económicos.*	*Afectación económica Pérdida de imagen institucional Perdida de la calidad y confiabilidad de la información Lecciones aprendidas Falla parcial o total de la SAN Falla total o parcial del servidor de Respaldo*	*Posible*	*Moderado*	*Zona de Riesgo Alta*	*Permisos de acceso y uso a Dispositivos extraíbles y funcionarios autorizados Sensibilización a usuarios sobre seguridad de la información Lecciones aprendidas*	*Raro*	*Insignificante*	*Zona de Riesgo Baja*	*Reducir el Riesgo*	*SI*	*SI*

Interrupción del servicio de la plataforma tecnológica	*Por mala manipulación de hardware o software informático.* *Por ataques informáticos.* *Por presencia de malware.* *Por falta de capacitación del personal.* *Por fallas técnicas no previstas.* *Por un mantenimiento deficiente y falta de soporte.* *Fallas en Sistemas de Energía Eléctrica* *Desastre Natural* *Incendio* *Terrorismo* *Daños de Aire Acondicionado*	*Interrupción de servicios tercerizados y/o proveedores.* *Interrupciones y fallas del fluido eléctrico que afectan la plataforma tecnológica de la entidad.* *Desastres naturales, ataques terroristas y eventos catastróficos.* *Insuficiente cubrimiento de equipos de resguardo ante interrupción y fallas del fluido eléctrico.* *Plataforma tecnológica, hardware y software desactualizada.* *Continuo avance tecnológico que puede repercutir en la obsolescencia de la infraestructura tecnológica*	*Afectación de procesos y cumplimiento de la misión institucional* *Necesidad de adquirir nuevos activos tecnológicos no planificados* *Indisponibilidad de la plataforma tecnológica.*	*Posible*	*Moderado*	*Zona de Riesgo Alta*	*Parches y actualizaciones de software* *Lecciones aprendidas* *Indicador de disponibilidad*	*Raro*	*Moderado*	*Zona de Riesgo moderada*	*Reducir el Riesgo*	*SI*	*NO*
Pérdida, daño, manipulación o sustracción de información o de equipos tecnológica	*Por pérdida, daño o robo de equipos informáticos.* *Por mala manipulación de hardware o software informático.* *Por ataques informáticos.* *Por presencia de malware.* *Por falta de capacitación del personal*	*Bajo cubrimiento en la cobertura de la salvaguarda de la información.* *Interrupciones y fallas del fluido eléctrico que afectan la plataforma tecnológica de la entidad.* *Uso inadecuado de las herramientas tecnológicas por parte del usuario.* *Incremento del cibercrimen.* *Virus y/o ataques informáticos por agentes externos.* *Desastres naturales, ataques terroristas y eventos catastróficos.* *Plataforma tecnológica, hardware y software desactualizada.* *Procedimientos ineficaces de registro de entrada y salida, por parte del personal de Seguridad física*	*Necesidad de adquirir nuevos activos tecnológicos no planificados.* *Afectación de procesos y cumplimiento de la misión institucional* *Incumplimiento de metas e indicadores.* *Indisponibilidad de la plataforma tecnológica.*	*Moderado*	*Mayor*	*Zona de Riesgo Extrema*	*Parches y actualizaciones de software* *Lecciones aprendidas* *Política General Seguridad de la Información y Seguridad Digital.* *Gestión de los riesgos asociados a la seguridad digital*	*Raro*	*Mayor*	*Zona de Riesgo Alta*	*Reducir el Riesgo*	*SI*	*NO*

Explotación de vulnerabilidades de los sistemas de información o sistemas operativos, por parte de ciberatacantes.	*Por el aprovechamiento de vulnerabilidades de los sistemas de información o sistemas operativos usados en la ALFM, para obtener información por parte de terceros (Ciberatacantes).*	*Surgimiento de nuevas amenazas cibernéticas, o accionamiento delictivo de las amenazas internas y externas. Vulneración de los protocolos de seguridad digital e institucionales. Limitación en el acceso a sistemas de información. Acelerado desarrollo tecnológico (obsolescencia). Negligencia en el cumplimiento de instrucciones y coordinaciones, emitidas por los diferentes canales de comunicación interna.*	*Perdida de Confidencialidad Perdida de Integridad Perdida de Disponibilidad*	*Frecuente*	*Mayor*	*Zona de Riesgo Extrema*	*Elaboración de boletines de información, sensibilizando a los funcionarios de la entidad sobre ciberseguridad. Verificación de eventos e incidentes de seguridad (Fortisandbox) Restricciones de acceso a direccionamientos IP y enlaces web reportados como fraudulentos.*	*Posible*	*Moderado*	*Alta*	*Reducir el Riesgo*	*SI*	*NO*

7. GESTIÓN DE RIESGOS

Controles que se ejecutan en la Oficina TIC, las cuales se integran con el Plan de Acción de la Entidad.

7.1. ALTERACIÓN O MANIPULACIÓN DE SISTEMAS Y DATOS.

Acciones:

Obj4. Modernizar y Desarrollar la Infraestructura Física y Tecnológica Estrategia 4.5 Fortalecer la conectividad e infraestructura tecnológica.

- Plan de tratamiento de riesgos de seguridad y privacidad de la información 2022.
- Revisión de la Directiva Política de Tratamiento de Riesgos que gestiona la Oficina Asesora de Planeación e Innovación Institucional.
- Efectuar valoración e identificación de riesgos a partir de la matriz de activos actualizada e incorporar los controles de acuerdo a la reglamentación nacional.

7.2. INTERRUPCIÓN DEL SERVICIO DE LA PLATAFORMA TECNOLÓGICA.

Acciones:

- Protección de la Información de Aplicativos y Usuarios.
- Realización de Backups de la información contenida en los servidores y bases de datos.
- Realización de Backups de la información de Usuario (ofimática).
- Disponibilidad de servicios
    - ✓ Disponibilidad de servicios Amazonia
    - ✓ Disponibilidad de servicios-Antioquia Choco
    - ✓ Disponibilidad de servicios – Caribe
    - ✓ Disponibilidad de servicios-Centro
    - ✓ Disponibilidad de servicios-Llanos Orientales

- ✓ Disponibilidad de servicios-Norte
- ✓ Disponibilidad de servicios-Nororiente
- ✓ Disponibilidad de servicios-Pacifico
- ✓ Disponibilidad de servicios-Sur
- ✓ Disponibilidad de servicios-Suroccidente
- ✓ Disponibilidad de servicios-Tolima Grande
- ✓ Disponibilidad de servicios-Oficina Principal

7.3. PÉRDIDA, DAÑO, MANIPULACIÓN O SUSTRACCIÓN DE INFORMACIÓN O DE EQUIPOS TECNOLÓGICOS.

Acciones:

- Actualización y Socialización Directiva Permanente “Política General Seguridad de la Información”.
- Identificación de Riesgos de Seguridad.
- Monitoreo y revisión de los riesgos identificados.
- Revisión de permisos de acceso y uso a Dispositivos extraíbles a funcionarios autorizados.
- Revisión del Directorio Activo y de las políticas aplicadas a nivel de seguridad en las principales plataformas informáticas de la Entidad.
- Seguimiento a la realización periódica de Backups.
- Seguimiento y monitoreo a reportes generados por WAF (Web Aplication Firewall) y FortiAnalyzer.
- Sensibilización a usuarios sobre seguridad de la información.

7.4. EXPLOTACIÓN DE VULNERABILIDADES DE LOS SISTEMAS DE INFORMACIÓN O SISTEMAS OPERATIVOS, POR PARTE DE CIBERATACANTES.

Acciones:

- Elaboración de boletines de información, sensibilizando a los funcionarios de la entidad sobre ciberseguridad.
- Verificación de eventos e incidentes de seguridad (Fortisandbox).
- Restricciones de acceso a direccionamientos IP y enlaces web reportados como fraudulentos.

8. MATRIZ DE ACTIVIDADES

ACTIVIDAD		RESPONSABLE	TAREA	ENTREGABLES
1	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.

ACTIVIDAD		RESPONSABLE	TAREA	ENTREGABLES
2	Seguimiento y monitoreo a eventos de seguridad (FortiAnalyzer).		Realizar seguimiento a los eventos reportados por la herramienta FortiAnalyzer de la actividad en la web y generar alerta a funcionarios que evidencien ingresos a sitios web fraudulento o maliciosos.	Plazo: Cuatrimestral. Evidencia: Informes de los reportes de seguimiento generados.
3	Revisión de permisos de acceso y uso a Dispositivos extraíbles y funcionarios autorizados.	Profesional Defensa	Hacer seguimiento al Grupo de Usuarios-USB del Active Directory y la plataforma Antivirus para el control de uso de dispositivos extraíbles, previamente a la validación de la justificación y autorización correspondiente. (Formato Excepciones de Seguridad).	Plazo: Cuatrimestral. Evidencia: Informes de seguimiento generados.
4	Definir los protocolos y herramientas de seguridad que deben tener los canales de comunicación e internet que contrata la Oficina TIC anualmente.	Profesional Defensa	Generar informe técnico que contemple los protocolos de seguridad requeridos, dentro de la estructuración del proceso de contratación de canales de comunicación e internet.	Plazo: Primer Semestre. Evidencia: Informe técnico – Contrato.
5	Revisión y actualización manual de políticas de seguridad de la información de acuerdo a	Profesional Defensa	Documento Manual de políticas de seguridad de la información	Actividad que se encuentra integrada al Plan Estratégico de Seguridad de la Información – PESI, con un plazo de

ACTIVIDAD		RESPONSABLE	TAREA	ENTREGABLES
	la actualización de la norma NTC/ISO/IEC 27001:2022.		actualizado.	cumplimiento para el segundo semestre.
6	Seguimiento a la realización de las copias de respaldo de la información y a las políticas de copias de respaldo acordadas para las herramientas y sistemas de información.	Profesional Defensa	Realización de Backups Centralizado.	Plazo: Cuatrimestral. Evidencia: Reporte realización de Backups.
7	Seguimiento a la realización de las copias de respaldo de la información y a las políticas de copias de respaldo acordadas para los usuarios finales.	Profesional Defensa	Realización Backups Centralizado.	Plazo: Cuatrimestral. Evidencia: Reporte realización de Backups.
8	Seguimiento a los procesos de Mantenimientos preventivos y correctivos a la Infraestructura tecnológica.	Profesional Defensa	Elaboración de estudios técnicos y estructuración del proceso de contratación de mantenimiento.	Plazo: Cuatrimestral. Evidencia: Soportes del seguimiento a los procesos de mantenimiento preventivo y correctivo.
9	Seguimiento a los controles establecidos para el control de acceso físico en las áreas de procesamiento de la entidad.	Profesional Defensa	Hacer seguimiento al cumplimiento del registro de ingreso a DATA CENTER y Centro Alterno, como al registro biométrico de ingreso.	Plazo: Cuatrimestral. Evidencia: Informes de seguimiento.
10	Revisión del Directorio Activo y de las políticas aplicadas a nivel de seguridad en las principales plataformas informáticas de seguridad.	Profesional Defensa	Análisis de las diferentes políticas, permiso y roles establecidas en la plataforma tecnológica.	Plazo: Semestral. Evidencia: Informes de seguimiento.
11	Revisión de aplicación de reglas o restricciones sobre la instalación de software.	Profesional Defensa	Hacer seguimiento a la aplicación restricciones sobre la instalación de software al Grupo de	Plazo: Semestral. Evidencia: Informes de seguimiento.

ACTIVIDAD		RESPONSABLE	TAREA	ENTREGABLES
			Usuarios de Active Directory correspondiente. (Formato Excepciones de Seguridad).	
12	Revisión y actualización de documentos y lineamientos establecidos en el proceso Gestión de TIC.	Profesional Defensa	Revisar y Actualizar manuales, guías, procedimientos y directivas, entre otros.	Plazo: Primer Semestre. Evidencia: Manuales, guías, procedimientos y documentos relacionados con los lineamientos emitidos por el proceso Gestión de TIC actualizados.
13	Efectuar valoración e identificación de riesgos a partir de la matriz de activos actualizada organizada por Procesos e incorporar los controles de acuerdo a la reglamentación nacional.	Líderes de proceso.	Actualización de los riesgos de seguridad.	Plazo: Segundo Semestre. Evidencia: Matriz de riesgos actualizada.
14	Intercambiar y/o compartir con el 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.	Profesional Defensa	Reporte de correos tipo SPAM.	Plazo: Trimestral. Evidencia: Mensajes de correos electrónicos generados.
15	Verificación de eventos e incidentes de seguridad (Fortisandbox).	Profesional Defensa	Seguimiento de los eventos e incidentes de seguridad presentados.	Plazo: Trimestral. Evidencia: Informes de seguimiento a los eventos de seguridad presentados.
16	Restricciones de acceso a direccionamientos IP y enlaces web reportados como fraudulentos.	Profesional Defensa	Seguimiento de restricciones de acceso de navegación.	Plazo: Trimestral. Evidencia: Informes de seguimiento.

9. 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 a mesas de trabajo adelantadas se realizará la articulación del: Plan de tratamiento de riesgos de seguridad y privacidad de la información - PTR.

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

10. ANALISIS Y MEDICIÓN

Seguimiento mediante el instrumento de Autodiagnóstico de MINTIC.

11. 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 que se requiera)	Responsable de Aprobar la Tarea en la SVE
Seguimiento y monitoreo a eventos de seguridad (FortiAnalyzer).	Informe de los reportes de seguimiento generados.	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.
Revisión de permisos de acceso y uso a Dispositivos extraíbles y funcionarios autorizados.	Informes de seguimiento generados.	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.
Definir los protocolos y herramientas de seguridad que deben tener los canales de comunicación e internet que contrata la Oficina TIC anualmente.	Informe técnico - Contrato.	01-01-2023	07/07/2023	Oficina TIC.	Gestión de TIC.	Profesional Defensa.	N/A	Jefe Oficina TIC.
Seguimiento a la realización de las copias de respaldo de la información y a las políticas de copias de respaldo acordadas para las herramientas y sistemas de	Reporte realización de Backups.	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.	Profesional Defensa.	Jefe Oficina TIC.

TAREAS	EVIDENCIA / ENTREGABLE	Fecha Inicio (día-mes-año)	Fecha Fin (día-mes-año)	Dependencia Responsable	Proceso Asociado	Responsable de documentar y registrar la Tarea en la SVE	Responsable de revisar la Tarea (en caso que se requiera)	Responsable de Aprobar la Tarea en la SVE
información.								
Seguimiento a la realización de las copias de respaldo de la información y a las políticas de copias de respaldo acordadas para los usuarios finales.	Reporte realización de Backups.	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.	Profesional Defensa.	Jefe Oficina TIC.
Seguimiento a los procesos de Mantenimientos preventivos y correctivos a la Infraestructura tecnológica.	Soportes del seguimiento a los procesos de Mantenimientos preventivos y correctivos.	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.
						Técnicos Regionales	Profesional Defensa.	Jefe Oficina TIC.
Seguimiento a los controles establecidos para el control de acceso físico en las áreas de procesamiento de la entidad.	Informes de seguimiento.	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.
Revisión del Directorio Activo y de las políticas aplicadas a nivel de seguridad en las principales plataformas informáticas de	Informes de seguimiento.	01/01/2023 01/07/2023	07/07/2023 05/01/2024	Oficina TIC.	Gestión de TIC.	Profesional Defensa.	N/A	Jefe Oficina TIC.

TAREAS	EVIDENCIA / ENTREGABLE	Fecha Inicio (día-mes-año)	Fecha Fin (día-mes-año)	Dependencia Responsable	Proceso Asociado	Responsable de documentar y registrar la Tarea en la SVE	Responsable de revisar la Tarea (en caso que se requiera)	Responsable de Aprobar la Tarea en la SVE
seguridad.								
Revisión de aplicación de reglas o restricciones sobre la instalación de software.	Informes de seguimiento.	01/01/2023 01/07/2023	07/07/2023 05/01/2024	Oficina TIC.	Gestión de TIC.	Profesional Defensa.	N/A	Jefe Oficina TIC.
Revisión y actualización de documentos y lineamientos establecidos en el proceso Gestión de TIC.	Manuales, guías, procedimientos y documentos relacionados con los lineamientos emitidos por el proceso Gestión de TIC actualizados.	01/01/2023	07/07/2023	Oficina TIC.	Gestión de TIC.	Profesional Defensa.	N/A	Jefe Oficina TIC.
Efectuar valoración e identificación de riesgos a partir de la matriz de activos actualizada organizada por Procesos e incorporar los controles de acuerdo a la reglamentación nacional.	Matriz de Riesgos actualizados	01/07/2023	05/01/2024	Oficina TIC.	Gestión de TIC.	Profesional Defensa.	N/A	Jefe Oficina TIC.
Intercambiar y/o compartir con el CSIRT, COLCERT, CAIVIRUTAL (DIJIN) y CCOC para apoyar la	Mensajes de correo electrónico generados	01/01/2023 01/04/2023 01/07/2023 01/10/2023	05/04/2023 07/07/2023 06/10/2023 05/01/2024	Oficina TIC.	Gestión de TIC.	Profesional Defensa.	N/A	Jefe Oficina TIC.

TAREAS	EVIDENCIA / ENTREGABLE	Fecha Inicio (día-mes-año)	Fecha Fin (día-mes-año)	Dependencia Responsable	Proceso Asociado	Responsable de documentar y registrar la Tarea en la SVE	Responsable de revisar la Tarea (en caso que se requiera)	Responsable de Aprobar la Tarea en la SVE
gestión de riesgos y la toma de decisiones (priorización, tratamiento y aceptación, respuesta a incidentes), especialmente, para prevenir interna y externamente amenazas cibernéticas.								
Verificación de eventos e incidentes de seguridad presentados (Fortisandbox).	Informes de seguimiento.	01/01/2023 01/04/2023 01/07/2023 01/10/2023	05/04/2023 07/07/2023 06/10/2023 05/01/2024	Oficina TIC.	Gestión de TIC.	Profesional Defensa.	N/A	Jefe Oficina TIC.
Restricciones de acceso a direccionamientos IP y enlaces web reportados como fraudulentos.	Informes de seguimiento.	01/01/2023 01/04/2023 01/07/2023 01/10/2023	05/04/2023 07/07/2023 06/10/2023 05/01/2024	Oficina TIC.	Gestión de TIC.	Profesional Defensa.	Profesional Defensa.	Jefe Oficina TIC.