

PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN VIGENCIA 2022

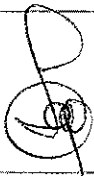
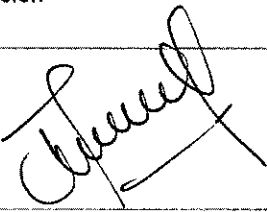

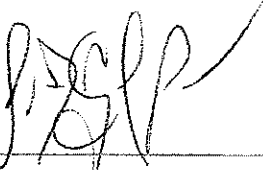
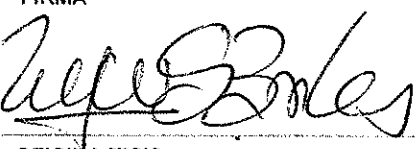

ELABORÓ	FECHA			ELABORÓ	FECHA			REVISÓ	FECHA		
	20	04	2022		20	04	2022		25	04	2022
NOMBRE: Ing. Daris Yaneth Padilla Díaz			NOMBRE: Ing. Deiby Leandro Alvarado Rodríguez			NOMBRE: Ing. Roberto Velásquez Arango					
CARGO: Profesional Oficina TIC's			CARGO: Profesional Seguridad de la Información			CARGO: Coordinador Grupo Informática (E)					
FIRMA 			FIRMA 			FIRMA 					
REVISÓ	FECHA			REVISÓ	FECHA			APROBÓ	FECHA		
	25	04	2022		25	04	2022		26	04	2022
NOMBRE: Ing. Cesar Adolfo González Peña			NOMBRE: CR. (RA) Sonia Dolly Gutiérrez Carrillo			NOMBRE: CR. Carlos Augusto Morales Hernandez					
CARGO: Coordinador Grupo de Redes e Infraestructura Tecnológica			CARGO: Jefe Oficina TIC's			CARGO: Director General Agencia Logística de las Fuerzas Militares (E)					
FIRMA 			FIRMA 			FIRMA 					
PROCESO y/o DEPENDENCIA:			OFICINA TIC'S								



TABLA DE CONTENIDO

1. GENERALIDADES	3
2. REFERENCIA NORMATIVA	3
3. DEFINICIONES	6
4. OBJETIVOS	13
5. ALCANCE	13
6. MAPA DE RIESGOS	13
7. GESTIÓN DE RIESGOS	15
7.1. Alteración o manipulación de sistemas y datos	15
7.2. Interrupción del servicio de la plataforma tecnológica	16
7.3. Pérdida, daño, manipulación o sustracción de información o de equipos tecnológicos	16
8. ACTIVIDADES	17
9. SEGUIMIENTO	19
10. ANÁLISIS Y MEDICIÓN	20
11. CONTROL DE CAMBIOS	20
12. ANEXO	21



1. GENERALIDADES

Gobierno Digital es una de las líneas de MIPG, que busca promover el uso y aprovechamiento de las Tecnologías de la Información y las Comunicaciones -TIC, para consolidar un Estado, con ciudadanos competitivos, proactivos, e innovadores, que generen valor público en un entorno de confianza digital. Esta política es uno de los pilares del Estado en el proceso de transformación y modernización de las entidades públicas.

La información es uno de los principales activos con que cuenta la Agencia Logística de las Fuerzas Militares (en adelante ALFM) para cumplir con sus objetivos misionales y estratégicos; así como para establecer relaciones con los ciudadanos, clientes y proveedores. Es por ello que resguardar la información de cualquier posibilidad de vulnerabilidad, alteración, mal uso, pérdida, entre otros muchos eventos, puede significar una buena estrategia de respaldo para el normal desarrollo de las actividades de la Entidad y para salvaguardar el buen nombre de la misma.

2. REFERENCIA NORMATIVA

Marco Normativo	Año	Descripción
Ley 527 (agosto 18)	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 1266 (diciembre 31)	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 5)	2009	Congreso de la República. 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)	2012	Disposiciones Generales para tratamiento de datos personales.
Ley 1712 (marzo 6)	2014	Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública.
NTC-ISO/IEC 27001	2013	Tecnologías de la Información. Técnicas de Seguridad. Sistemas de Gestión de la Seguridad de la Información. Requisitos.
Decreto 1078 (mayo 26)	2015	Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.



TÍTULO

FORMATO DE PLANES

Código: GI-FO-24

Versión: No. 00

Página 4 de 22

Fecha:

01

12

2021



Decreto 1413 (agosto 25)	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 4)	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)	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 088 (enero 24)	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.
Directiva Permanente Ministerio de Defensa No. 018 (junio 19)	2014	Políticas de seguridad de la información para el Sector Defensa.
Directiva Permanente Ministerio de Defensa No. 03 (enero 23)	2019	Lineamientos para la definición de la Política de Tratamiento de Datos Personales en el Ministerio de Defensa Nacional.
Directiva Presidencial No. 03 (marzo 15)	2021	Lineamientos para el uso de servicios en la nube, inteligencia artificial, seguridad digital y gestión de datos.
Directiva Presidencial No. 02 (febrero 24)	2022	Reiteración de la política pública en materia de seguridad digital.



TÍTULO

FORMATO DE PLANES

Código: GI-FO-24

Versión: No. 00

Página 5 de 22

Fecha:

01

12

2021



Resolución 001519 (agosto 24)	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 500 (marzo 10)	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)	2022	Por la cual se define el uso de las Tecnologías en la Nube para el Sector Defensa y se dictan otras disposiciones.
Resolución 000460 (febrero 15)	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)	2022	Por la 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
Circular 018 (septiembre 22)	2021	Implementación de la Resolución 1519 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." Del Ministerio de las Tecnologías de la Información y las Comunicaciones (MINTIC) y la aplicación de la Matriz ITA.
CONPES 3854 (abril 11)	2016	Política Nacional de Seguridad Digital.
CONPES 3920 (abril 17)	2018	Política nacional de explotación de datos (BIG DATA).
CONPES 3995 (julio 1)	2020	Nacional de confianza y seguridad Digital.
Manual de Gobierno Digital (diciembre versión. 6)	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)	2019	Manual integrado de gestión, código: GI-MA-02, versión No. 20



TÍTULO

FORMATO DE PLANES

Código: GI-FO-24

Versión: No. 00

Página 6 de 22

Fecha:

01

12

2021



GUIA ADCP
(diciembre
versión. 5)

2020

Guía para la Administración del Riesgo y el Diseño Controles en entidades Públicas, (Documento emitido por el Departamento Administrativo de la Función Pública, última actualización diciembre.

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).
- **Backup (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 institucional:** Es el servicio de correo electrónico que provee y administra directamente la entidad a sus funcionarios como herramienta de apoyo a las funciones y responsabilidades de los mismos. En el caso de la Agencia este correo institucional corresponde al que tiene como dominio @agencialogistica.gov.co.
- **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 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

 <p>AGENCIA LOGÍSTICA PLANIFICACIÓN MILITAR ... LEJOS DE NUESTROS PAISES ...</p>	<p>TÍTULO</p> <p>FORMATO DE PLANES</p>	Código: GI-FO-24			 <p>Ministerio de Defensa ... LEJOS DE NUESTROS PAISES ...</p>
		Versión: No. 00		Página 9 de 22	
		Fecha:	01	12	

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



TÍTULO

FORMATO DE PLANES

Código: GI-FO-24

Versión: No. 00

Página 10 de 22

Fecha:

01

12

2021



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



TÍTULO

FORMATO DE PLANES

Código: GI-FO-24

Versión: No. 00

Página 11 de 22

Fecha:

01



12

2021



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

 <p>AGENCIA LOGÍSTICA FUERZAS MILITARES LA FUERZA DE LOS SERVICIOS LOGÍSTICOS</p>	<p>TÍTULO</p> <p>FORMATO DE PLANES</p>	Código: GI-FO-24			 <p>Secretaría de Defensa ARMADA ARGENTINA</p>
		Versión: No. 00		Página 12 de 22	
		Fecha:	01	12	

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).



TÍTULO

FORMATO DE PLANES

Código: GI-FO-24

Versión: No. 00

Página 13 de 22

Fecha:

01

12

2021



4. OBJETIVOS

El presente plan de tratamiento de riesgos de seguridad y privacidad de la información y seguridad digital establece las actividades que se ejecutarán en la vigencia 2022 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.

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 (2022) 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



TÍTULO

FORMATO DE PLANES

Código: GI-FO-24

Versión: No. 00

Página 14 de 22

Fecha:

01

12

2021



RIESGO	DESCRIPCIÓN	CAUSAS	EFECTOS	ANTES DE LOS CONTROLES			CONTROLES	DESPUÉS DE LOS CONTROLES			OPCIÓN DE MANEJO	INSTITUCIONAL	DECORUPCIÓN	
				PROBABILIDAD	IMPACTO	ZONA INHERENTE		PROBABILIDAD	IMPACTO	ZONA RESIDUAL				
Alteración o manipulación de sistemas y datos	<p>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.</p> <p>Por falta de capacitación del personal.</p> <p>Por fallas técnicas no previstas.</p> <p>Por un mantenimiento deficiente y falta de soporte</p>	<p>Interés de agentes externos de perjudicar la imagen institucional.</p> <p>Posibilidad de obtener beneficios económicos.</p>	<p>Afectación económica</p> <p>Pérdida de imagen institucional</p> <p>Perdida de la calidad y confiabilidad de la información</p> <p>Lecciones aprendidas</p> <p>Falla parcial o total de la SAN</p> <p>Falla total o parcial del servidor de Respaldo</p>	P	M	Z	Permisos de acceso y uso a Dispositivos extraíbles y funcionarios autorizados <p>Sensibilización a usuarios sobre seguridad de la información</p> <p>Lecciones aprendidas</p>	R	I	Z	Insignificante	Reducir el riesgo	SI	SI
Interrupción del servicio de la plataforma tecnológica	<p>Por mala manipulación de hardware o software informático.</p> <p>Por ataques informáticos.</p> <p>Por presencia de malware.</p> <p>Por falta de capacitación del personal.</p> <p>Por fallas técnicas no previstas.</p> <p>Por un mantenimiento deficiente y falta de soporte.</p> <p>Fallas en Sistemas de Energía Eléctrica</p> <p>Desastre Natural</p> <p>Incendio</p> <p>Terrorismo</p> <p>Daños de Aire Acondicionado</p>	<p>Interrupción de servicios tercerizados y/o proveedores.</p> <p>Interrupciones y fallas del fluido eléctrico que afectan la plataforma tecnológica de la entidad.</p> <p>Desastres naturales, ataques terroristas y eventos catastróficos.</p> <p>Insuficiente cubrimiento de equipos de resguardo ante interrupción y fallas del fluido eléctrico.</p> <p>Plataforma tecnológica, hardware y software</p>	<p>Afectación de procesos y cumplimiento de la misión institucional</p> <p>Necesidad de adquirir nuevos activos tecnológicos no planificados</p> <p>Indisponibilidad de la plataforma tecnológica.</p>	P	M	Z	Parches y actualizaciones de software <p>Lecciones aprendidas</p> <p>Indicador de disponibilidad</p>	R	M	Z	Moderada	Reducir el riesgo	SI	NO



		<i>desactualizada. Continuo avance tecnológico que puede repercutir en la obsolescencia de la infraestructura tecnológica</i>																																												
<i>Pérdida, daño, manipulación o sustracción de información o de equipos tecnológica</i>	<i>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</i>	<i>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</i>	<i>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.</i>	<i>Mod</i>	<i>er</i>	<i>a</i>	<i>d</i>	<i>a</i>	<i>d</i>	<i>a</i>	<i>Zona de riesgo extremo</i>	<i>Parches y actualizaciones de software Lecciones aprendidas</i>	<i>Política General Seguridad de la Información y Seguridad Digital. Gestión de los riesgos asociados a la seguridad digital</i>	<i>R</i>	<i>a</i>	<i>r</i>	<i>o</i>	<i>M</i>	<i>a</i>	<i>y</i>	<i>o</i>	<i>Z</i>	<i>o</i>	<i>n</i>	<i>a</i>	<i>d</i>	<i>e</i>	<i>r</i>	<i>i</i>	<i>e</i>	<i>s</i>	<i>g</i>	<i>o</i>	<i>R</i>	<i>e</i>	<i>d</i>	<i>u</i>	<i>c</i>	<i>i</i>	<i>r</i>	<i>e</i>	<i>l</i>	<i>S</i>	<i>I</i>	<i>N</i>	<i>O</i>



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.

PROCESO		DESARROLLO ORGANIZACIONAL Y GESTIÓN INTEGRAL			
 AGENCIA LOGÍSTICA FUERZAS MILITARES <small>LA UNIÓN DE NUESTRAS FUERZAS</small>	TÍTULO	Código: GI-FO-24			
		Versión: No. 00		Página 16 de 22	
		Fecha:	01	12	2021
FORMATO DE PLANES		 <small>Oficina Asesora de Planeación e Innovación Institucional</small>			

- 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 Backup de la información contenida en los servidores y bases de datos.
- Realización de Backup 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 Backup.



- Seguimiento y monitoreo a reportes generados por WAF (Web Application Firewall) y FortiAnalyzer.
- Sensibilización a usuarios sobre seguridad de la información.

8. ACTIVIDADES

ACTIVIDAD	RESPONSABLE	TAREA	ENTREGABLES
1 Sensibilización a usuarios sobre seguridad de la información.	Oficial de Seguridad	Elaboración y ejecución del plan.	Primer cuatrimestre: Documento con el plan de capacitación y Listados de asistencia
		Ejecución del plan.	Segundo y Tercer cuatrimestre: Listados de asistencia a las capacitaciones brindadas.
		Ejecución y Finalización del Plan	
2 Seguimiento y monitoreo a reportes generados por WAF (Web Application Firewall).	Oficial de Seguridad	Realizar seguimiento a los eventos reportados por WAF de la actividad en la web y generar alerta a funcionarios que evidencien ingresos a sitios web fraudulento o maliciosos.	Entrega cuatrimestral de documento con los reportes de seguimiento generados.
3 Revisión de permisos de acceso y uso a Dispositivos extraíbles y funcionarios autorizados.	Oficial de Seguridad	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).	Entrega cuatrimestral de documento con los reportes de seguimiento generados.
4 Definir los protocolos y herramientas de seguridad que deben tener los canales de comunicación e	Administrador Red	Generar informe técnico que contemple los protocolos de seguridad requeridos,	Primer Semestre: Informe técnico Contrato.



TÍTULO

FORMATO DE PLANES

Código: GI-FO-24

Versión: No. 00

Página 18 de 22

Fecha:

01

12

2021



ACTIVIDAD	RESPONSABLE	TAREA	ENTREGABLES
internet que contrata la Oficina TIC anualmente.		dentro de la estructuración del proceso de contratación de canales de comunicación e internet.	
5 Actualización Directiva Permanente Política General Seguridad de la Información.	Oficial de seguridad de la información	Actualizar y consolidar directiva, Política General de Seguridad de la Información.	Segundo semestre: Directiva actualizada.
6 Seguimiento a la realización de las copias de respaldo de la información y a las políticas de copias de respaldo acordadas.	Grupo de Informática	Realización de Backup Centralizado	Reporte cuatrimestral de realización de Backup - reporte de la SAN-NAS.
7 Seguimiento a los procesos de Mantenimientos preventivos y correctivos a la Infraestructura tecnológica.	Lider de Mesa de Ayuda	Elaboración de estudios técnicos y estructuración del proceso de contratación de mantenimiento.	Reporte cuatrimestral de Seguimiento a los procesos de Mantenimientos preventivos y correctivos.
		Ejecución del contrato de mantenimiento por parte del proveedor.	Actividad controlada mediante el Plan de Acción - Plan Estratégico de Tecnologías de la Información y las Comunicaciones PETI (2022)
		Recibo a satisfacción del contrato de mantenimiento.	
8 Seguimiento a los controles establecidos para el control de acceso físico en las áreas de procesamiento de la entidad.	Oficial de Seguridad	Hacer seguimiento al cumplimiento del registro de ingreso a DATA CENTER y Centro Alterno, como al registro biométrico de ingreso.	Cuatrimestral: Informes de seguimiento
9 Revisión del Directorio Activo y de las políticas aplicadas a nivel de seguridad en las principales plataformas informáticas de seguridad.	Oficial de Seguridad	Análisis de las diferentes políticas, permiso y roles establecidas en la plataforma tecnológica.	Semestral Informe con el análisis y observaciones de mejora.



ACTIVIDAD	RESPONSABLE	TAREA	ENTREGABLES	
10	Revisión de aplicación de reglas o restricciones sobre la instalación de software.	Administrador Red	Hacer seguimiento a la aplicación restricciones sobre la instalación de software al Grupo de Usuarios de Active Directory correspondiente. (Formato Excepciones de Seguridad).	Semestral Informe que evidencien su aplicabilidad
11	Revisión y actualización de las Políticas de Seguridad de la Información y Política de Tratamiento de Riesgos.	Oficial de Seguridad	Revisar y Actualizar manuales, guías, procedimientos y directivas.	Primer Semestre Manuales, guías, procedimientos y directivas actualizados.
12	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 y Oficial de seguridad	Actualización de los riesgos y controles establecidos.	Segundo Semestre Matriz de Riesgos actualizados
13	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.	Oficial de Seguridad	Reporte de correos tipo SPAM	Trimestral Mensajes de correo electrónico generados

9. SEGUIMIENTO

Soporte de las actividades publicadas en la plataforma SUITE VISION.



TÍTULO

FORMATO DE PLANES

Código: GI-FO-24

Versión: No. 00

Página 20 de 22

Fecha:

01

12

2021



10. ANÁLISIS 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

PROCESO

DESARROLLO ORGANIZACIONAL Y GESTIÓN INTEGRAL

TÍTULO

FORMATO DE PLANES

Código: GI-FO-24

Versión: No. 00 Página 21 de 22

Fecha: 01 12 2021



AGENCIA LOGÍSTICA
FUERZAS MILITARES

12. 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
Sensibilización a usuarios sobre seguridad de la información.	<ul style="list-style-type: none"> - Plan de capacitación - Ejecución del plan. - Listados de asistencia a las capacitaciones brindadas 	01-03-2022 01-07-2022 01-09-2022	06-05-2022 09-09-2023 02-01-2023	Oficina TIC's	Gestión TIC	Oficial de seguridad	N/A	Jefe Oficina TIC's
Seguimiento y monitoreo a reportes generados por WAF (web application firewall).	Informes de seguimiento generados	02-05-2022 01-05-2022 01-09-2022	13-05-2022 09-09-2022 13-01-2023	Oficina TIC's	Gestión TIC	Oficial de seguridad	N/A	Jefe Oficina TIC's
Revisión de permisos de acceso y uso a Dispositivos extraíbles y funcionarios autorizados.	Informes de seguimiento generados.	02-05-2022 01-05-2022 01-09-2022	13-05-2022 09-09-2022 13-01-2023	Oficina TIC's	Gestión TIC	Oficial de seguridad	N/A	Jefe Oficina TIC's
Definir los protocolos y herramientas de seguridad que deben tener los canales de comunicación e internet que contrata la Oficina TIC anualmente	<ul style="list-style-type: none"> - Informe técnico - Contrato 	01-06-2022	08-07-2022	Oficina TIC's	Gestión TIC	Oficial de seguridad	N/A	Jefe Oficina TIC's
Actualización Directiva Permanente No. 07 Política General Seguridad de la Información 1207 21.	Directiva actualizada.	01-07-2022	13-01-2023	Oficina TIC's	Gestión TIC	Oficial de seguridad	N/A	Jefe Oficina TIC's
Seguimiento a la realización de las copias de respaldo de la información y a las políticas de copias de respaldo acordadas.	<ul style="list-style-type: none"> - Realización de Backup - Reporte de la SAN-NAS 	02-05-2022 01-05-2022 01-09-2022	13-05-2022 09-09-2022 13-01-2023	Oficina TIC's	Gestión TIC	Oficial de seguridad	N/A	Jefe Oficina TIC's
Seguimiento a los controles establecidos para el control de acceso físico en las áreas de procesamiento de la entidad.	<ul style="list-style-type: none"> - Informe de seguimiento 	02-05-2022 01-05-2022 01-09-2022	13-05-2022 09-09-2022 13-01-2023	Oficina TIC's	Gestión TIC	Oficial de seguridad	N/A	Jefe Oficina TIC's

PROCESO

DESARROLLO ORGANIZACIONAL Y GESTIÓN INTEGRAL

TÍTULO

FORMATO DE PLANES



Código: GI-FO-24

Versión: No. 00 Página 22 de 22

Fecha: 01 12 2021

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
Revisión del Directorio Activo y de las políticas aplicadas a nivel de seguridad en las principales plataformas informáticas de seguridad	Informe con el análisis y observaciones de mejora	01-06-2022 01-07-2022	08-07-2022 02-01-2023	Oficina TIC's	Gestión TIC	Oficial de seguridad	N/A	Jefe Oficina TIC's
Revisión de aplicación de reglas o restricciones sobre la instalación de software	Informe que evidencien su aplicabilidad	01-06-2022 01-07-2022	08-07-2022 02-01-2023	Oficina TIC's	Gestión TIC	Oficial de seguridad	N/A	Jefe Oficina TIC's
Revisión y actualización de las Políticas de Seguridad de la Información y Política de Tratamiento de Riesgos.	Manuales, guías, procedimientos y Directivas actualizados	01-06-2022	08-07-2022	Oficina TIC's	Gestión TIC	Oficial de seguridad	N/A	Jefe Oficina TIC's
Efectuar valoración e identificación de riesgos a partir de la matriz de activos actualizada e incorporar los controles de acuerdo a la reglamentación nacional.	Matriz de Riesgos actualizados	01-08-2022	15-11-2022	Oficina TIC's	Gestión TIC	Oficial de seguridad	N/A	Jefe Oficina TIC's
Intercambiar y/o compartir con el CSIRT, COLCERT, CAIVRITAL (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.	Mensajes de correo electrónico generados	01-01-2022 11-04-2022 11-07-2022 10-10-2022	04-04-2022 08-07-2022 07-10-2022 13-01-2023	Oficina TIC's	Gestión TIC	Oficial de seguridad	N/A	Jefe Oficina TIC's