

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 2020

PROYECTÓ	FECHA			REVISÓ	FECHA			REVISÓ	FECHA			APROBÓ	FECHA		
	0 5	0 5	2 0		0 5	0 5	2 0		0 5	0 5	2 0		0 5	0 5	2 0
NOMBRE				NOMBRE				NOMBRE				NOMBRE			
Ing. Daris Yaneth Padilla Díaz				Ing. Yuri Daianny Ruiz Franco				Ing. César Adolfo González Peña				Cr. (RA) Sonia Dolly Gutiérrez Carrillo			
CARGO				CARGO				CARGO				CARGO			
Profesional Oficina TICs				Coordinadora Grupo de Informática				Coordinador Grupo de Redes e Infraestructura Tecnológica				Jefe Oficina TICs			
FIRMA				FIRMA				FIRMA				FIRMA			

PROCESO		GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES			
	TITULO	Código: GTI-PL-01			
		Versión No. 01		P á g i n a 2 de 1 0	
		Fecha	31	01	2019
PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 2020					

TABLA DE CONTENIDO

Introducción..... 3

Objetivos 3

1. Alcance 3

2. Referencia normativa 3

3. Definiciones..... 4

4. Descripción general del Modelo de Seguridad y Privacidad de la Información (MSPI) 6

5. Actividades a realizar en la presente vigencia 7

6. Control de cambios 8

PROCESO		GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES			
	TITULO	Código: GTI-PL-01			
		Versión No. 01		P á g i n a 3 de 1 0	
		Fecha	31	01	2019
					

INTRODUCCIÓN

La política de Gobierno Digital es uno de los pilares del Estado en el proceso de transformación y modernización de las entidades públicas. Dentro de los elementos que conforman dicha política se encuentra el de Seguridad y Privacidad, el cual busca preservar la confidencialidad, integridad y disponibilidad de los activos de información de las entidades del Estado, garantizando su buen uso y la privacidad de los datos, a través de un Modelo de Seguridad y Privacidad de la Información.

Para realizar este modelo se requieren una serie de procesos y documentos que lleven al cumplimiento de los lineamientos establecidos por el Ministerio de las Tecnologías de la Información y las Comunicaciones. Por esta razón es necesario elaborar un plan que permita adelantar el proceso de la mejor manera posible y así cumplir con ciertas metas que permitan evaluar el nivel de madurez de la ALFM en la planificación, implementación y verificación del modelo.

OBJETIVOS

El Plan de Seguridad de la Información es un documento que tiene por objetivo trazar y planificar la manera como la ALFM continuará con la implementación del Modelo de Seguridad y Privacidad de la Información (MSPI).

1. ALCANCE

Se definirán las actividades a cumplir durante la presente vigencia (2020) para avanzar en la implementación del MSPI. 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 implementación.

2. REFERENCIA NORMATIVA

- Ley 1712 de 2014. Congreso de la República. Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones.
- Ley 1581 de 2012. Disposiciones Generales para tratamiento de datos personales.
- Ley 1273 de 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 1266 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.

PROCESO		GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES					
	TITULO	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 2020		Código: GTI-PL-01			
				Versión No. 01		P á g i n a 4 de 10	
				Fecha	31	01	2019
							

- Ley 527 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.
- 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.
- Norma técnica colombiana NTC-ISO-IEC 27001.
- Directiva permanente Ministerio de Defensa No. 018 de 2014. Políticas de seguridad de la información para el Sector Defensa.
- Directiva permanente Ministerio de Defensa No. 03 de 2019. Lineamientos para la definición de la Política de Tratamiento de Datos Personales en el Ministerio de Defensa Nacional.
- Documento CONPES 3854 de abril 11 de 2016, Política Nacional de Seguridad Digital.
- Manual Operativo del Modelo Integrado de Planeación y Gestión - Consejo para la Gestión y Desempeño Institucional - Versión 3 - diciembre de 2019.
- Resolución 27 del 17 de marzo de 2020, por la cual se adoptan medidas preventivas sanitarias, por causa del coronavirus COVID-19 en la Agencia Logística de las Fuerzas Militares, y a través la cual establecen una serie de responsabilidades especial en el Artículo Cuarto Teletrabajo.

3. DEFINICIONES

- **Activos tecnológicos o informáticos:** Se consideran activos tecnológicos o informáticos todos los elementos de hardware, software, información y de comunicaciones entregados por la entidad al funcionario con el fin de facilitarle el desempeño de sus funciones. De esta manera, son activos tecnológicos, además de los programas (software aplicativo y de ofimática), los computadores o equipos de cómputo junto con sus periféricos (tarjeta de red, mouse, teclado, monitor, parlantes, unidades externas de almacenamiento, micrófono, entre otros), impresoras, escáneres, etc. También los equipos y elementos de comunicaciones (telefonía, switches, routers, cableado, etc) y la información almacenada en los diversos equipos y bases de datos.
- **Análisis de riesgo:** Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo. (ISO/IEC 27000).
- **Auditoría:** Proceso sistemático, independiente y documentado para obtener evidencias de auditoría y obviamente para determinar el grado en el que se cumplen los criterios de auditoría. (ISO/IEC 27000).

PROCESO		GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES			
	TITULO PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 2020	Código: GTI-PL-01		P á g i n a 5 de 1 0	
		Versión No. 01			
		Fecha	31	01	2019

- **Gobierno Digital:** Es una política del Estado Colombiano encaminada a promover el uso y aprovechamiento de las tecnologías de la información y las comunicaciones para consolidar un Estado y ciudadanos competitivos, proactivos, e innovadores, que generen valor público en un entorno de confianza digital.
- **Modelo Integrado de Planeación y Gestión (MIPG):** Es el marco de referencia para dirigir, planear, ejecutar, hacer seguimiento, evaluar y controlar la gestión de las entidades públicas con el fin de generar resultados que atiendan a los planes de desarrollo y que resuelvan las necesidades y problemas de los ciudadanos con integridad y calidad en los servicios.
- **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.
- **Partes interesadas (Stakeholders):** Persona u organización que puede afectar a, ser afectada por o percibirse a sí misma como afectada por una decisión o actividad.
- **Plan de Tratamiento de Riesgos (PTR):** Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma. (ISO/IEC 27000).
- **Riesgo:** Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000).
- **Sistema de Gestión de Seguridad de la Información (SGSI):** Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión y de mejora continua. (ISO/IEC 27000).
- **Tecnologías de la información y las comunicaciones (TIC):** Son el conjunto de recursos, herramientas, equipos, programas informáticos, aplicaciones, redes y medios, que permiten la

PROCESO		GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES			
	TITULO	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 2020			
		Código: GTI-PL-01		Página 6 de 10	
		Versión No. 01	Fecha	31	01

compilación, procesamiento, almacenamiento, transmisión de información como voz, datos, texto, video e imágenes.

- **Trazabilidad:** Cualidad que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sean asociadas de modo inequívoco a un individuo o entidad. (ISO/IEC 27000).
- **Vulnerabilidad:** Debilidad de un activo o control que puede ser explotada por una o más amenazas. (ISO/IEC 27000).
- **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.

4. DESCRIPCIÓN GENERAL DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN (MSPI)

El MSPI debe contemplar, como mínimo, los siguientes aspectos:

- ESTABLECIMIENTO Y GESTION DEL MSPI
 - Establecimiento del MSPI
 - Implementación y operación del MSPI
 - Seguimiento y revisión del MSPI
 - Mantenimiento y mejora del MSPI
- REQUISITOS DE DOCUMENTACION
 - Generalidades
 - Control de Documentos
 - Control de Registros
- RESPONSABILIDAD DE LA DIRECCION
 - Compromiso de la Dirección
 - Gestión de Recursos
 - Provisión de Recursos
 - Formación, toma de conciencia y competencia.
- AUDITORIAS INTERNAS DEL MSPI
- REVISION DEL MSPI POR LA DIRECCION

PROCESO		GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES			
	TITULO PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 2020	Código: GTI-PL-01		Página 7 de 10	
		Versión No. 01			
		Fecha	31	01	2019
					

- Generalidades
- Información para la revisión
- Resultados de la revisión
- MEJORA DEL MSPI
 - Mejora continua
 - Acción correctiva
 - Acción preventiva

5. ACTIVIDADES A REALIZAR EN LA PRESENTE VIGENCIA

Para la vigencia 2020 se realizarán las siguientes actividades dentro del proceso de implementación del MSPI:

- 1) Elaborar el plan de sensibilización, capacitación y apropiación del MSPI para toda la entidad para la presente vigencia.
 - **Responsable:** Profesional de seguridad de la información de la ALFM.P
 - **Plazo:** Segundo semestre 2020
 - **Evidencia:** Plan de sensibilizaciones elaborado (primer semestre) y ejecutado (segundo semestre).
- 2) Determinar el estado actual de la gestión y el nivel de madurez del Modelo de Seguridad y Seguridad de la Información.

DIAGNÓSTICO			
Metas	Resultado	Instrumento	MRAE
Determinar el estado actual de la gestión de la Seguridad y Privacidad de la Información al interior de la ALFM	Diligenciamiento de la herramienta	Herramienta de diagnóstico	LI.ES.01 LI.ES.02
Identificar el nivel de madurez de Seguridad y Privacidad de la información en la ALFM	Diligenciamiento de la herramienta, identificación del nivel de madurez de la Entidad	Herramienta de diagnóstico	LI.GO.01 LI.GO.04 LI.GO.05 LI.GO.07 LI.ST.14
Identificar vulnerabilidades técnicas y administrativas que sirvan como insumo para la fase de planificación.	Documento con los hallazgos encontrados en las pruebas de vulnerabilidad.	Herramienta de diagnóstico	

En esta fase se pretende alcanzar las siguientes metas:

- ✓ Determinar el nivel de madurez de los controles de seguridad de la información.
- ✓ Identificar el avance de la implementación del ciclo de operación al interior de la entidad.

PROCESO		GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES				
	TITULO PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 2020	Código: GTI-PL-01		P á g i n a 8 de 10		
		Versión No. 01				
		Fecha	31	01	2019	
						

- ✓ Identificar el nivel de cumplimiento con la legislación vigente relacionada con protección de datos personales.
- ✓ Identificación del uso de buenas prácticas en Ciberseguridad.

Para ello se utilizará los siguientes instrumentos:

- ✓ Herramienta de diagnóstico.
- ✓ Instructivo para el diligenciamiento de la herramienta.
- ✓ Guía No 1 MINTIC - Metodología de Pruebas de Efectividad.

Responsable: todos los procesos en coordinación con el profesional de seguridad de información de la ALFM la actividad será realizada por procesos; se iniciará para la presente vigencia con caracterización de activos de Información de la Oficina TIC.

Plazo: El **Segundo Semestre de 2020.**

Evidencia: Entrega **Semestral** de los avances del inventario de activos y la herramienta de diagnóstico del MSPI diligenciada

3) Revisión de las Políticas ante el MIPG.

PLANIFICACIÓN			
Metas	Resultado	Instrumento	MRAE
Revisión de la Política de Seguridad y Privacidad de la Información	Documento con la Política de seguridad de la información, debidamente aprobado por la alta Dirección y socializada al interior de la Entidad	Guía No 2 – Política General MSPI (Numeral 6): Política general de Seguridad y Privacidad de la Información	LI.ES.02, LI.ES.06, LI.ES.07, LI.ES.08, LI.ES.09, LI.ES.10,
Revisión de las Políticas de seguridad y privacidad de la información	Manual con las políticas de seguridad y privacidad de la información, debidamente aprobadas por la alta dirección y socializadas al interior de la Entidad.	Guía No 2 – Política General MSPI (Numeral 9): Políticas específicas recomendadas para la implementación de controles de seguridad de la información.	LI.GO.01, LI.GO.04, LI.GO.07, LI.GO.08, LI.GO.09, LI.GO.10, LI.INF.01,
Revisión de los Procedimientos de Seguridad de la Información.	Procedimientos, debidamente documentados, socializados y aprobados por el comité.	Guía No 3 – (Numeral 6): Procedimientos de Seguridad y Privacidad de la Información	LI.INF.02, LI.INF.09, LI.INF.10, LI.INF.11,
Revisión de Roles y responsabilidades de Seguridad y Privacidad de la Información.	Acto administrativo a través del cual se crea o se modifica las funciones del comité gestión institucional (o el que haga sus veces), en donde se incluyan los temas de seguridad de la información en la entidad, revisado y	Guía No 4 - Roles y responsabilidades de seguridad y privacidad de la información.	LI.INF.14, LI.SIS.22, LI.SIS.23, LI.SIS.01, LI.ST.05, LI.ST.06, LI.ST.09, LI.ST.10,

PROCESO		GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES			
	TITULO	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 2020			
		Código: GTI-PL-01		Página 9 de 10	
		Versión No. 01	31	01	2019
		Fecha			

	aprobado por la alta Dirección, deberá designarse quien será el encargado de seguridad de la información dentro de la entidad.		LI.ST.12 ,LI.ST.13, LI.ST.14, LI.UA.01, LI.UA.02, LI.UA.03, LI.UA.04, LI.UA.05, LI.UA.06
--	--	--	--

En esta fase se pretende alcanzar los siguientes objetivos:

- ✓ Revisión de las Políticas, Procedimientos, Roles y Responsabilidades de Seguridad de la Información.
- ✓ Que se encuentren debidamente documentadas, aprobadas y socializadas.

Para logro de los objetivos se requiere:

- ✓ Reunión con la Oficina TIC de la ALFM

Responsable: Profesional de seguridad de la información de la ALFM coordinar Reunión de la Oficina TIC.

4) Inventario de Activos

PLANIFICACIÓN			
Metas	Resultado	Instrumento	MRAE
Inventario de activos de información	Documento con la metodología para identificación, clasificación y valoración de activos de información,	Guía No 5 - Gestión De Activos Guía para la administración del riesgo y el diseño de controles en entidades públicas-DAFP.	
	Matriz con la identificación, valoración y clasificación de activos de información.	Anexo 4: Lineamientos para la gestión de Riesgos de Seguridad Digital en entidades públicas-DAFP.	
	Documento con la caracterización de activos de información, que contengan datos personales Inventario de activos de IPv6	Guía No 20 - Transición Ipv4 a Ipv6.	

Responsable: Todos los procesos de la Oficina TICs, coordinados por el profesional de seguridad de la información de la ALFM, la actividad será realizada por procesos; se iniciará para la presente vigencia con caracterización de activos de Información de la Oficina TIC.

Plazo: El Segundo Semestre de 2020

Evidencia: Entrega **Semestral** de los avances del inventario de activos.



TITULO
PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 2020

Código: **GTI-PL-01**

Versión No. **01**

Página
1 0 de 1 0

Fecha

31

01

2019



5) Implementación

IMPLEMENTACIÓN			
Metas	Resultado	Instrumento	MRAE
Inventario de activos de Información	Actualizar el inventario de los Activos.	Lista de Activos de Información actualizada.	

Responsable: Todos los procesos de la Oficina TIC, en coordinación con el profesional de seguridad de la información de la ALFM. se iniciará para la presente vigencia con caracterización de activos de Información de la Oficina TIC.

Plazo: Entrega avance semestral.

Evidencia: Entrega semestral de los avances del inventario de activos.

6) Actualizar el Plan de Tratamiento de Riesgos (PTR)

✓ Responsable: Profesional de seguridad de la información de la ALFM.

6. CONTROL DE CAMBIOS

VERSIÓN	DESCRIPCIÓN DE CAMBIOS
00	Documento inicial según NMO.
01	Se actualiza el plan para el año 2019.
02	Actualización de actividades para la vigencia 2020
03	Actualización de actividades para la vigencia ABRIL 2020