
PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 2021



**AGENCIA LOGÍSTICA
FUERZAS MILITARES**
— La unión de nuestras Fuerzas —



ELABORÓ	FECHA		
	DÍA	MES	AÑO
	21	01	2021

Ing. Jimmy Leonardo Caballero Herrera

REVISÓ	FECHA		
	DÍA	MES	AÑO
	27	01	2021

Cr. (RA) Sonia Dolly Gutiérrez Carrillo

CARGO Jefe Oficina TICs

APROBÓ	FECHA		
	DÍA	MES	AÑO
	28	01	2021

Cr. (RA) Oscar Alberto Jaramillo

FIRMA

CARGO Profesional Oficina TICs Oficial de Seguridad de la Información

CARGO Director General

NOMBRE Ing. Daris Yaneth Padilla Diaz

FIRMA

CARGO Coordinadora Grupo de Informática (E)

FIRMA

NOMBRE Ing. Jorge Armando Rivas Rojas

CARGO Coordinador Grupo de Redes e Infraestructura Tecnológica (E)

FIRMA

FIRMA



TITULO

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA
INFORMACIÓN 2020

Código: GTI-PL-01

Versión No. 01

Página
3 de 14



Fecha


31

01

2019

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			
	TÍTULO	Código: GTI-PL-01			
		Versión No. 01		Página 4 de 14	
		Fecha	31	01	2019

INTRODUCCIÓN

El Ministerio de Tecnologías de la Información y las Comunicaciones - MinTIC a través de la Dirección de Gobierno Digital, dando cumplimiento a sus funciones; publica “El Modelo de Seguridad y Privacidad de la Información (MSPI)”, el cual se encuentra alineado con el Marco de Referencia de Arquitectura TI, el Modelo Integrado de Planeación y Gestión (MIPG) y La Guía para la Administración del Riesgo y el Diseño Controles en entidades Públicas (Documento de noventa y un (91) páginas emitido por el Departamento Administrativo de la Función Pública, última actualización Diciembre 2020), este modelo pertenece al habilitador transversal de Seguridad y Privacidad, de la Política de Gobierno Digital.

Guía para la administración del riesgo y el diseño de controles en entidades...

Descarga: [Formato PDF](#)

Guía para la administración del riesgo y el diseño de controles en entidades públicas - Versión 5 - Diciembre de 2020



+ Subido por Nelson Adriano Góchez, Proffia, 3/08/18 12:12

El Departamento Administrativo de la Función Pública, como entidad técnica, estratégica y transversal del Gobierno Nacional, pone a disposición de las entidades la metodología para la administración del

riesgo. En esta versión 5 se actualizó con el fin de algunos elementos metodológicos para mejorar el ejemplo de (dentro de la clasificación de riesgo). Es importante resaltar que se mantiene la estructura general bajo tres ejes principales los cuales fundamentan la estructura metodológica que desde las primeras versiones de la guía se ha venido desarrollando.


Etiquetas: [Gestión de Riesgos](#) [Seguridad](#) [Privacidad](#) [Control](#) [Administración](#)

Ilustración 1: Fuente: https://www.funcionpublica.gov.co/web/eva/biblioteca-virtual/-/document_library/bGsp21jUBdeu/view_file/34316499

El Modelo de Seguridad y Privacidad para estar acorde con las buenas prácticas de seguridad es actualizado periódicamente; **reuniendo los cambios técnicos de la norma 27001 del 2013, legislación de la Ley de Protección de Datos Personales, Transparencia y Acceso a la Información Pública**, entre otras, las cuales se deben tener en cuenta para la gestión de la información.

A nivel metodológico es importante tener presente que el (MSPI) cuenta con una veinte un (21) de guías anexas que ayudan a las entidades a cumplir lo solicitado permitiendo abordar de manera detallada cada una de las fases del modelo, buscando a su vez comprender cuáles son los resultados a obtener y como desarrollarlos, incluyendo los nuevos lineamientos que permiten la adopción del protocolo IPv6 en el Estado Colombiano.

- Guía 1 - Metodología de pruebas de efectividad
- Guía 2 - Política General MSPI v1
- Guía 3 - Procedimiento de Seguridad de la Información
- Guía 4 - Roles y responsabilidades
- Guía 5 - Gestión Clasificación de Activos
- Guía 6 - Gestión Documental

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 5 de 14	
		Versión No. 01			
		Fecha	31	01	2019



- Guía 7 - Gestión de Riesgos
- Guía 8 - Controles de Seguridad de la Información
- Guía 9 - Indicadores Gestión de Seguridad de la Información
- Guía 10 - Continuidad de Negocio
- Guía 11 - Análisis de Impacto de Negocio
- Guía 12 - Seguridad en la Nube
- Guía 13 - Evidencia Digital (En actualización)
- Guía 14 - Plan de comunicación, sensibilización, capacitación
- Guía 15 - Auditoria
- Guía 16 - Evaluación de Desempeño
- Guía 17 - Mejora continua
- Guía 18 - Lineamientos terminales de áreas financieras de entidades públicas
- Guía 19 - Aseguramiento de protocolo IPv4_IPv6
- Guía 20 - Transición IPv4_IPv6
- Guía 21 - Gestión de Incidentes

Adicionalmente se cuenta con el "Instrumento de Evaluación MSPI", que es una herramienta que fue creada con el fin de identificar el nivel de madurez en la implementación del Modelo de seguridad y Privacidad de la Información, permitiendo establecer el estado de la gestión y adopción de controles técnicos y administrativos al interior de las Entidades Públicas, según lo definido en la Estrategia de Gobierno en Línea en su cuarto componente "Seguridad y Privacidad de la Información". Creada por el Ministerio de Tecnologías de la Información y las Comunicaciones.

La implementación del Modelo de Seguridad y Privacidad de la Información - MSPI, en la Entidad está determinado por las necesidades objetivas, los requisitos de seguridad, procesos, el tamaño y la estructura de la misma, todo con el objetivo de preservar la confidencialidad, integridad, disponibilidad de los activos de información, garantizando su buen uso y la privacidad de los datos, trabajo que se viene adelantado y madurando año tras año.

Mediante la adopción del Modelo de Seguridad y Privacidad por parte de las Entidades del Estado se busca contribuir al incremento de la transparencia en la Gestión Pública, promoviendo el uso de las mejores prácticas de Seguridad de la Información como base de la aplicación del concepto de Seguridad Digital.

Por lo todo anterior y en consecuencia con lo trabajado en los años anteriores en la Agencia Logística de las Fuerzas Militares, se plantea para 2021, lo siguiente:

PROCESO		GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES			
	TITULO	Código: GTI-PL-01			
		Versión No. 01		Página 6 de 14	
		Fecha	31	01	2019
PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 2020					

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 (2021) 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.
- 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.

PROCESO		GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES			
 AGENCIA LOGÍSTICA FUERZAS MILITARES <small>La unión de nuestras Fuerzas</small>	TÍTULO PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 2020	Código: GTI-PL-01		Página	
		Versión No. 01		7 de 14	
		Fecha	31	01	2019

- Documento CONPES 3854 de abril 11 de 2016, Política Nacional de Seguridad Digital.
- Documento COMPEPES 3995 de Julio 1 de 2020 Política Nacional de confianza y 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.
- 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 2020)



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).
- **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.

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		Página 8 de 14		
					Fecha	31	01	2019	

- **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 compilación, procesamiento, almacenamiento, transmisión de información como voz, datos, texto, video e imágenes.
- **Trazabilidad:** Calidad 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)

PROCESO					
GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES					
 AGENCIA LOGÍSTICA FUERZAS MILITARES <small>La unión de nuestras Fuerzas</small>	TÍTULO PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 2020	Código: GTI-PL-01		 <small>de la Defensa</small>	
		Versión No. 01	P á g i n a 9 de 14		
		Fecha	31		01

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
 - 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

El 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", señala en su artículo 1:

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

PROCESO		GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES			
	TITULO	Código: GTI-PL-01			
		Versión No. 01		Página 10 de 14	
		Fecha	31	01	2019
PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 2020					

Plan de Acción de que trata el artículo 74 de la Ley 1474 de 2011, deberán integrar los planes institucionales y estratégicos (...)

Teniendo en cuenta lo anterior y de conformidad con las mesas de trabajo adelantadas se realizará la integración del presente plan al plan de acción de la vigencia 2021; mediante las siguientes actividades:

Objetivo 4 *Modernizar y desarrollar la infraestructura física y tecnológica*
Estrategia 4.5 *Fortalecer la conectividad e infraestructura tecnológica*

- 1) Continuar la adopción del *plan de sensibilización, capacitación y apropiación del MSPI* para la ALFM (funcionarios operativos y administrativos) de la ALFM para la presente vigencia, para el fortalecimiento de en la conciencia relacionadas a la seguridad digital, mejores prácticas de seguridad digital y mitigación de riesgos y amenazas cibernéticas para continuar minimizando la brecha en seguridad de la información.

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

Plazo: Primer y segundo semestre 2021

Evidencia: Plan de sensibilizaciones en seguridad elaborado (primer semestre) y ejecutado (segundo semestre).

Nota: Para el desarrollo y con el fin de dar cumplimiento a lo establecido en la guía 14 de Mintic que corresponde al plan de Capacitación, Sensibilización Y Comunicación De Seguridad De La Información se solicitara el apoyo a la Dirección Administrativa y de Talento Humano para promover y divulgar las diferentes capacitaciones, y actividades identificadas por la Oficina TIC'S, que son relevantes para la entidad en temáticas relacionados a seguridad digital y que depende de los cronogramas depende de las fechas estipuladas por las diferentes entidades durante la vigencia, dicha actividad se alinea a la estrategia 1.3 del plan de capacitación de la entidad, pero corresponde al modelo de seguridad y privacidad que promueve el uso de las mejores prácticas de Seguridad de la Información como base de la aplicación del concepto de Seguridad Digital.

Metas	Resultado	Instrumento
Plan de sensibilización en temas relacionados a riesgos cibernéticos a regionales ALFM.	Documento de Plan de actividades de sensibilización en temas relacionadas a seguridad digital y de la información dirigido a las Regionales de la ALFM con el fin de capacitar a todos los funcionarios en todos los niveles de la entidad, lo anterior teniendo en cuenta las condiciones técnicas y adaptando las estrategias implementadas en oficina principal a las de cada regional. Jornada de Capacitación de nuevas	Apoyo Guía No 14 - Plan de Capacitación, Sensibilización Y Comunicación De Seguridad De La Información Solicitud de capacitación a través correo



TÍTULO

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 2020

Código: GTI-PL-01

Versión No. 01

Página
11 de 14



Fecha

31

01

2019


	<p>tendencias en riesgos cibernéticos, ingeniería social, y prevención orientado con el centro cibernético de la Policía Nacional.</p> <p>Socialización de talleres, cursos, diplomados, orientados a fortalecer habilidades, entrenamiento y desarrollo profesional de funcionarios de la ALFM en temas relacionados a Seguridad digital con el apoyo del proceso de Talento Humano.</p> <p>Seguimiento al estado de avance del MSPI</p>	<p>electrónico a 'dijin.cecip-jef@policia.gov.co' (7/01/2021)</p> <p>Reunión (llamada Telefónica con CENTRO CIBERNETICO DE LA POLICIA NACIONAL) de contextualización ALFM sobre actividades y estrategias implementadas para sensibilización, además de solicitar aprobación para y establecer y temáticas y cronogramas (13/01/2021).</p> <p>Convocatorias vigentes lideradas por Mintic, Gobierno Digital, OEA, entidades de Seguridad Nacional.</p> <p>Instrumento MSPI actualizado</p> <p>Auditoría al MSPI</p>
--	---	---

En esta fase se pretende alcanzar las siguientes metas:

- ✓ Aplicar las estrategias de sensibilización en seguridad digital a nivel de usuario a todos los niveles de la ALFM.
- ✓ Fortalecer las habilidades en temas relacionados en seguridad de la información por parte de los funcionarios de la ALFM para mitigar riesgos y amenazas cibernéticas.
- ✓ Integrar junto con el apoyo de entidades de seguridad digital del Gobierno Nacional - Centro Cibernético de la Policía estrategias de sensibilización para aplicarlas en la ALFM orientadas a la prevención de amenazas.
- ✓ Promover la continuidad del uso de buenas prácticas en seguridad que permitan mantener la disponibilidad, confidencialidad y privacidad de la información y fortalecer el modelo de seguridad y privacidad de la información.
- ✓ Revisión y seguimiento del estado de avance del instrumento del MSPI.

Para ello se utilizará los siguientes instrumentos:

- ✓ Guía No 14 MINTIC – Plan de comunicación y Sensibilización.

PROCESO		GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES			
	TITULO	Código: GTI-PL-01			
		Versión No. 01		Página 12 de 14	
		Fecha	31	01	2019
PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 2020					

Responsable: Profesional Oficial de seguridad de la información y personal apoyo Agentes de Soporte regionales ALFM.

Plazo: El primer y Segundo semestre 2021.

Evidencia: Informe semestral de los avances del plan de sensibilización aplicado.

- 2) **Inventario de Activos: Matriz de Activos de Información, continuar con su completitud y maduración con el levantamiento y aprobación de los procesos y todas las dependencias de la ALFM.**

Metas	Resultado	Instrumento
Inventario de activos de información	<p>Documento de apoyo con la metodología para valoración y clasificación de activos de acuerdo a lo establecido en la Guía 5 de Mintic.</p> <p>Actualizar y completar el inventario de activos de información de acuerdo a la Matriz con la identificación, valoración y clasificación de activos de información actualizada por líderes de proceso o por persona designado.</p>	<p>Guía No 5 - Gestión De Activos</p> <p>Matriz de Activos de Información actualizada según Tablas de retención documental con asignación de custodio y valoración de confidencialidad, disponibilidad e integridad de acuerdo a lo establecido en la GUIA 5 de clasificación de activos de información.</p>


Responsable: Todos los procesos, coordinados por el profesional de seguridad de la información de la ALFM, se realizarán acompañamientos y seguimientos a cada proceso para la respectiva verificación, valoración y asignación de responsables (propietarios y custodios), de activos de información llevada a cabo en el levantamiento información respecto a las tablas de retención documental ALFM (Oficina Principal y regionales).

Plazo: El primer y segundo Semestre de 2021

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

- 3) **Actualización Plan de Continuidad del Negocio**

Metas	Resultado	Instrumento
Plan de continuidad de negocio ALFM	Plan de continuidad de negocio actualizado.	Guía 10 para la preparación de las TIC Para la continuidad de negocio

PROCESO		GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES			
 AGENCIA LOGÍSTICA FUERZAS MILITARES <small>La unión de nuestras Fuerzas</small>	TITULO PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 2020	Código: GTI-PL-01			
		Versión No. 01		P á g i n a 1 3 de 1 4	
		Fecha	31	01	2019

En esta fase se pretende alcanzar los siguientes objetivos:

- ✓ Revisión ajuste y actualización del plan de continuidad de negocio aprobado.
- ✓ Levantamiento de información, documentar, y socializar.

Para logro de los objetivos se requiere:

- ✓ Reunión con la Oficina TIC, para levantamiento de información de la ALFM

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

Plazo: Segundo semestre de 2021

Evidencia: Entrega de los avances del levantamiento de información para consolidación y actualización.



4) Seguimiento a la implementación de la política de gobierno digital

Metas	Resultado	Instrumento
Incrementar el índice de la Política de Gobierno Digital a 96 puntos.	Soportes y registros del seguimiento al estado de implementación de la política de gobierno digital al interior de la ALFM	Herramienta en línea autodiagnóstico política gobierno digital. FURAG 2020 Recomendaciones DAFP

Responsable: Profesional Oficial de seguridad de la información y Oficina Asesora de Planeación e Innovación Institucional

Plazo: Seguimiento trimestral

Evidencia: Actas de reunión, reporte de autodiagnóstico

PROCESO		GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES			
 AGENCIA LOGÍSTICA FUERZAS MILITARES <small>LA UNIÓN DE NUESTRAS FUERZAS</small>	TÍTULO PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 2020	Código: GTI-PL-01		 <small>de la Defensa</small>	
		Versión No. 01		Página 14 de 14	
		Fecha	31	01	2019

6. 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

5990