AGENCIA LOGÍSTICA
FUERZAS MILITARES
La unión de nuestras Fuerzas

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 2019

ELABORÓ	FECHA			REVISÓ	FECHA			APROBÓ	FECHA		
	31	01	2019		31	01	2019		31	01	2019
NOMBRE Juan Carlos Ahumada Munar				**NOMBRE** Ing. Yuri Daianny Ruiz Franco Ing. César Adolfo González Peña				**NOMBRE** Cr. (RA) Sonia Dolly Gutiérrez Carrillo			
CARGO Profesional de Seguridad Informática				**CARGO** Coordinadora Grupo de Informática Coordinador Grupo de Redes e Infraestructura Tecnológica				**CARGO** Jefe Oficina TICs			
FIRMA Juan Carlos Ahumada Munar Firmado digitalmente por Juan Carlos Ahumada Munar Fecha: 2019.02.13 15:22:55 -05'00'				**FIRMAS** Ing. Yuri Daianny Ruiz Franco Firmado digitalmente por Ing. Yuri Daianny Ruiz Franco Fecha: 2019.02.13 15:35:42 -05'00' César González Firmado digitalmente por César González Fecha: 2019.02.13 15:50:50 -05'00'				**FIRMA** CR (RA) Sonia Dolly Gutiérrez Carrillo Firmado digitalmente por CR (RA) Sonia Dolly Gutiérrez Carrillo Nombre de reconocimiento (DN): cn=CR (RA) Sonia Dolly Gutiérrez Carrillo, o=Agencia Logística de las Fuerzas Militares, ou=Jefe Oficina Tecnologia y Comunicaciones, email=sonia.gutierrez@agencialogistica.gov.co, c=ES Fecha: 2019.02.14 07:50:30 -05'00'			

TABLA DE CONTENIDO

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 (2019) 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.

- Documento CONPES 3854 de abril 11 de 2016, Política Nacional de Seguridad Digital.

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 auditoria y obviamente para determinar el grado en el que se cumplen los criterios de auditoria. (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.

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

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

4. 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
  - 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 2019 se realizarán las siguientes actividades dentro del proceso de implementación del MSPI:

- Ajustar el alcance y límites del MSPI en términos de las características del servicio que presta la Entidad, su estructura interna, su ubicación, sus activos de información, tecnología, e incluir los detalles y justificación de cualquier exclusión del alcance.
  - Responsable: Profesional de seguridad de la información de la ALFM.
  - Plazo: Primer cuatrimestre de 2019.
  - Evidencia: Documento de definición del MSPI.

- Actualizar la política general de Seguridad de la Información y lograr su aprobación por la Alta Dirección y la divulgación a todo el personal de la ALFM.
  - Responsable: Profesional de seguridad de la información de la ALFM.
  - Plazo: Primer cuatrimestre de 2019.
  - Evidencia: Documento con la política general actualizada.

- Actualizar el inventario de los activos dentro del alcance del MSPI y los propietarios de estos activos de información.
  - Responsable: Todos los procesos, coordinados por el profesional de seguridad de la información de la ALFM.
  - Plazo: Diciembre de 2019.
  - Evidencia: Entrega cuatrimestral del documento con el avance del inventario levantado.

- Identificar las amenazas a los nuevos activos.
  - Responsable: Todos los procesos, coordinados por el profesional de seguridad de la información de la ALFM.
  - Plazo: Diciembre de 2019.
  - Evidencia: Entrega cuatrimestral del documento con el avance de las amenazas identificadas.

- Analizar y evaluar los riesgos asociados de acuerdo al impacto que pueden generar y a la probabilidad de ocurrencia para los nuevos activos identificados.
  - Responsable: Todos los procesos, coordinados por el profesional de seguridad de la información de la ALFM.
  - Plazo: Diciembre de 2019.
  - Evidencia: Entrega cuatrimestral del documento con el avance del análisis de riesgos.

- Obtener la aprobación de la Dirección sobre los nuevos riesgos residuales determinados.
  - Responsable: Profesional de seguridad de la información de la ALFM.
  - Plazo: Diciembre de 2019.
  - Evidencia: Entrega en el último cuatrimestre del documento aprobado.

- Elaborar la declaración de aplicabilidad (SoA).
  - Responsable: Profesional de seguridad de la información de la ALFM.
  - Plazo: Diciembre de 2019.
  - Evidencia: Entrega en el último cuatrimestre del documento SoA.

- Actualizar el Plan de Tratamiento de Riesgos (PTR).
  - Responsable: Profesional de seguridad de la información de la ALFM.
  - Plazo: Diciembre de 2019.
  - Evidencia: Entrega en el último cuatrimestre del PTR para la vigencia 2020.

- 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.
  - Plazo: Segundo cuatrimestre de 2019.
  - Evidencia: Plan de sensibilizaciones elaborado (primer cuatrimestre) y ejecutado (segundo cuatrimestre).

6. CONTROL DE CAMBIOS

VERSIÓN	DESCRIPCIÓN DE CAMBIOS
00	Documento inicial según NMO.
01	Se actualiza el plan para el año 2019.