AGENCIA LOGÍSTICA
FUERZAS MILITARES
La unión de nuestras Fuerzas

PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN VIGENCIA 2019

ELABORÓ	FECHA			REVISÓ	FECHA			APROBÓ	FECHA		
	30	01	2019		30	01	2019		30	01	2019
NOMBRE Ing. 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 15:24:10 -05'00'				**FIRMAS** Ing. Yuri Daianny Ruiz Franco Firmado digitalmente por Ing. Yuri Daianny Ruiz Franco Fecha: 2019.02.13 15:35:10 -05'00' César González Firmado digitalmente por César González Fecha: 2019.02.13 15:51:54 -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 Tecnología y Comunicaciones, email=sonia.gutierrez@agencialogistica.gov.co, c=ES Fecha: 2019.02.14 07:51:56 -05'00'			

TABLA DE CONTENIDO

Introducción 3

Objetivos 3

1. Alcance 3
2. Referencia normativa 3
3. Definiciones 4
4. Actividades a realizar 8
5. Control de cambios 9

INTRODUCCIÓN

La información es el principal activo con que cuenta la Agencia Logística de las Fuerzas Militares (en adelante ALFM) para cumplir con sus objetivos misionales y estratégicos y también en su relación con los ciudadanos, sus clientes y sus proveedores. Es por ello que resguardar la información de cualquier posibilidad de alteración, mal uso, pérdida, entre otros muchos eventos, puede significar un respaldo para el normal desarrollo de las actividades de la Entidad y para el buen nombre de la misma.

OBJETIVOS

El presente plan de tratamiento de riesgos establece las actividades a realizar en la vigencia 2019 para mitigar y hacer seguimiento a los riesgos de seguridad y privacidad de la información que se puedan presentar en la ALFM, a fin de proteger y preservar la información y los elementos tecnológicos que la soportan. Este documento es el resultado de la estimación del riesgo y aplicación de controles realizados en la ALFM para la protección de los activos informáticos.

1. 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 de 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 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.

2. REFERENCIA NORMATIVA

- Ley 1712 de 2014. Congreso de la Republica**.** 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 Republica. 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.

- 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

Para los efectos del presente plan se tendrán en cuenta las siguientes definiciones:

- **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.

- **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.

- **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.

- **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.

- **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 se accede a través de Outlook o bien mediante el sitio: http://agencia.mail (internamente en la Agencia) o http://mail.agencialogistica.gov.co (equipos con Internet externos a la Agencia).

- **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).

- **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.

- **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.

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

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

- **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 o e-mail message:** 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.

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

- **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 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 aplicativo:** Programas que son escritos para realizar una tarea específica mediante el computador y está orientado a dar cubrimiento a un proceso específico. Son los denominados "software de aplicación específica". Este tipo de software está desarrollado sobre los denominados lenguajes de programación (C, Cobol, Developer, .Net, Java, PHP, entre otros), y los de mayor prestación y alto manejo de volúmenes de información están implementados sobre Bases de Datos (Oracle, MySQL, PosgreSql, etc.) en donde reside organizadamente la información que es manejada por intermedio del software aplicativo.

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

- **Software 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 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 re-distribuirla.

- **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.

- **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.

- **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):** Dispositivo(s) removible(s) por el usuario final, que permite(n) 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.

4. ACTIVIDADES A REALIZAR

En coordinación con coordinadores de los grupos de Informática y de Redes e Infraestructura Tecnológica se establecieron las siguientes actividades para la presente vigencia:

- Sensibilización a usuarios sobre seguridad de la información. Se hará un plan de capacitación y sensibilización a usuarios sobre temas de seguridad informática y riesgos informáticos.
  - Responsable: Profesional de seguridad de la información de la ALFM.
  - Actividades: Primer cuatrimestre: Elaboración del plan. Segundo cuatrimestre: Ejecución del plan.
  - Entregables: Primer cuatrimestre: Documento con el plan de capacitación. Segundo cuatrimestre: Listados de asistencia a las capacitaciones.

- Adquisición de un WAF (web application firewall). Se realizará proceso de contratación para adquirir el dispositivo, el cual protegerá los aplicativos web de la ALFM.
  - Responsable: Grupo de Redes e Infraestructura Tecnológica.

- Actividades: Primer cuatrimestre: Elaboración de pliegos y contratación del proveedor. Segundo cuatrimestre: Puesta en funcionamiento del WAF.
- Entregables: Primer cuatrimestre: Contrato firmado. Segundo cuatrimestre: acta de entrega a satisfacción del objeto contractual.

- Migración de IPv4 a IPv6. Se realizará proceso de contratación para realizar la migración de la red de la ALFM del protocolo IPv4 al protocolo IPv6.
  - Responsable: Grupo de Redes e Infraestructura Tecnológica.
  - Actividades: Primer cuatrimestre: Elaboración de pliegos y contratación del proveedor. Segundo cuatrimestre: Ejecución del contrato por parte del proveedor. Tercer cuatrimestre: Finalización del proceso de migración y cierre del contrato.
  - Entregables: Primer cuatrimestre: Contrato firmado. Segundo cuatrimestre: informe de avance de acuerdo al cronograma. Tercer cuatrimestre: Acta de entrega a satisfacción del objeto contractual.

- Realización periódica de backups. Se continúa con la realización de backups a nivel nacional.
  - Responsable: Grupo de Informática.
  - Actividades: Permanente en todos los cuatrimestres: Realización de backups a nivel nacional.
  - Entregables: Formatos de realización de backups a nivel nacional.

- Mantenimientos preventivos y correctivos. Proceso de contratación para la realización de los mantenimientos a nivel nacional.
  - Responsable: Grupo de Redes e Infraestructura Tecnológica.
  - Actividades: Primer cuatrimestre: Elaboración de pliegos y contratación del proveedor. Segundo cuatrimestre: Ejecución del contrato por parte del proveedor. Tercer cuatrimestre: Finalización y cierre del contrato.
  - Entregables: Primer cuatrimestre: Contrato firmado. Segundo cuatrimestre: Informe de avance de acuerdo al cronograma. Tercer cuatrimestre: Acta de entrega a satisfacción del objeto contractual.

5. CONTROL DE CAMBIOS

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