AGENCIA LOGÍSTICA
FUERZAS MILITARES
La unión de nuestras Fuerzas

MANUAL DE POLÍTICAS DE USO, OPERACIÓN Y SEGURIDAD PARA LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES

ELABORO	FECHA DIA	FECHA MES	FECHA AÑO	REVISÓ	FECHA DIA	FECHA MES	FECHA AÑO	REVISÓ	FECHA DIA	FECHA MES	FECHA AÑO
	29	09	2021		29	09	2021		29	09	2021
NOMBRE: Ing. Jimmy Leonardo Caballero Herrera				**NOMBRE:** Ing. Yuri Daianny Ruiz Franco				**NOMBRE:** Ing. Cesar Adolfo Gonzalez Peña			
CARGO: Profesional de Defensa Oficial de Seguridad de La Información				**CARGO:** Coordinadora Informática				**CARGO:** Coordinador Redes e Infraestructura Tecnológica			
FIRMA				**FIRMA**				**FIRMA**			
APROBÓ	**FECHA DIA**	**FECHA MES**	**FECHA AÑO**	**APROBÓ**	**FECHA DIA**	**FECHA MES**	**FECHA AÑO**	**APROBÓ**	**FECHA DIA**	**FECHA MES**	**FECHA AÑO**
	29	09	2021		29	09	2021		29	09	2021
NOMBRE: Cr. (R) Sonia Dolly Gutiérrez Carrillo				**NOMBRE:** Abg. Martha Cortes Baquero				**NOMBRE:** Coronel (RA) Oscar Alberto Jaramillo Carrillo			
CARGO: Jefe Oficina de Tecnologías de la Información y las Comunicaciones Tics				**CARGO:** Jefe Oficina Asesora Jurídica				**CARGO:** Director General Agencia Logística de las Fuerzas Militares			
FIRMA				**FIRMA**				**FIRMA**			

TABLA DE CONTENIDO

INTRODUCCIÓN

El presente documento tiene como fin:

- Emitir políticas con relación al uso de los equipos de cómputo y los servicios tecnológicos institucionales, así como de la instalación, operación, sostenibilidad y desinstalación de software aplicativo y de oficina (ofimática) de la Agencia Logística de las Fuerzas Militares - ALFM.

- Establecer los lineamientos, restricciones y responsabilidades de los usuarios que manejan herramientas tecnológicas en la ALFM, respecto al manejo y control de la información que circula por la red institucional y el uso de los recursos informáticos.

- Garantizar por medio de lineamientos y la aplicación de buenas prácticas de seguridad digital, la integridad física y disponibilidad de los recursos tecnológicos.

- Proveer los lineamientos para el uso de los recursos tecnológicos asignados a los usuarios internos y externos de la entidad.

- Establecer un esquema de seguridad física de la información y su transferencia con responsabilidad para la ALFM.

- Prestar a la Entidad un servicio de Tecnologías de la Información y las Comunicaciones- TIC, soportado en los estándares vigentes de seguridad y calidad de la información.

- Concientizar a los todos los usuarios internos y externos de la entidad sobre la importancia de la seguridad informática y de la información, como activos sensibles y primordiales para la operación y misión de la ALFM.

OBJETIVO

Informar a los todos los usuarios internos y externos, las políticas establecidas para la seguridad de la información, el uso de los servicios tecnológicos y de la información de la Entidad y promover los mecanismos que deben cumplir y utilizar para proteger el hardware, software y la información procesada y almacenada en los sistemas de información y en la red institucional de la ALFM.

ALCANCE

Las Políticas de uso, operación y seguridad para las tecnologías de la información y las comunicaciones establecen lineamientos, restricciones, responsabilidades y compromisos que cubren todos los aspectos administrativos y de control que deben ser acatados por los usuarios internos y externos que operen los servicios de TIC de la ALFM, para el adecuado nivel de cumplimiento de sus funciones y actividades, con el fin de conseguir con ello, un apropiado nivel de protección, disponibilidad, integridad y confidencialidad, principios básicos para garantizar la seguridad de la información.

Los usuarios de las TIC de la ALFM, deben conocer y tienen la obligación de dar estricto cumplimiento a las presentes políticas emitidas y aprobadas por la Dirección General de la Entidad.

1. REFERENCIA NORMATIVA

a. 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.

b. Ley 1581 de 2012. Disposiciones Generales para tratamiento de datos personales.

c. 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.

d. 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.

e. Norma técnica colombiana NTC-ISO-IEC 27001.

f. Directiva permanente Ministerio de Defensa No. 018 de 2014.

g. 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.

h. Documento CONPES 3072 de febrero 9 de 2000, Agenda de Conectividad.

i. Documento CONPES 3701 de 2011, Lineamientos de Política para Ciberseguridad y Ciberdefensa.

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

k. Ley Estatutaria No.1581 del 17 octubre de 2012, la cual se reglamenta parcialmente por el Decreto Nacional 1377 de 2013. En la cual se dictan disposiciones generales para la protección de datos.

l. Decreto 1008 de 2018, por el cual se establecen los lineamientos generales de la política de Gobierno Digital.

m. Decreto No.491 del 28 marzo de 2020, por el cual se adoptan medidas de urgencia para garantizar la atención y la prestación de los servicios por parte de las autoridades públicas y los particulares que cumplan funciones públicas y se toman medidas para la protección laboral y de los contratistas de prestación de servicios de las entidades públicas, en el marco del Estado de Emergencia Económica, Social y Ecológica.

n. Circular Externa N° 001 del AGN del 31 de marzo de 2020. Con asunto "Lineamientos para la Administración de Expedientes y Comunicaciones Oficiales".

o. Documento CONPES 3995 de 1 de Julio de 2020, Política Nacional de Confianza y Seguridad Digital.

p. Resolución No.00500 de marzo 10 de 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".

q. Directiva Permanente de 12 de Julio de 2021 de la ALFM "Lineamientos de seguridad Digital y de la información".

2. DEFINICIONES

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

- **ALFM**: Agencia Logística de las Fuerzas Militares.

- **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, cámara, 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.

- **Adware:** Es un software no deseado diseñado para mostrar anuncios en su pantalla, normalmente en un explorador. Algunos profesionales de la seguridad lo ven como un precursor de los PUP (programas potencialmente no deseados) de hoy en día. Normalmente, recurre a un método subrepticio: bien se hace pasar por legítimo, o bien mediante otro programa para engañarlo e instalarse en su PC, tableta o dispositivo móvil.

- **Archivos:** Conjunto de datos o instrucciones que se almacenan en el Disco Duro y/o cualquier otro medio de almacenamiento con un nombre que los identifica.

- **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.

- **Botnets:** Es una red de equipos informáticos que han sido infectados con software malicioso que permite su control remoto, obligándoles a enviar spam, propagar virus o realizar ataques de denegación de servicio distribuido (DDoS) sin el conocimiento o el consentimiento de los propietarios reales de los equipos.

- **Buscador en Internet:** Son sitios web especializados en localizar información por criterios o por contenidos a través de internet. Entre los más utilizados y conocidos se encuentran Yahoo® y Google®.

- **Buzón de correo electrónico:** Depósito en el que se almacenan los mensajes de correo que llegan a un destinatario determinado.

- **CD (Compact Disc):** Disco óptico en el cual se graba información en forma digital. Permite acumular una gran cantidad de datos (aproximadamente 650 Mb.) que se leen mediante rayos láser.

- **CD-R** (Recordable): Es un Compact Disc en el que se únicamente se puede grabar información hasta que se alcance la capacidad total del CD por una sola vez.

- **CD-RW** (Recordable-Writable): Es un Compact Disc en el que se puede grabar información y también borrar o modificar la ya existente (reescribidle).

- **DVD** (Digital Video Disc): Disco digital mejorado, con una capacidad muy superior al CD. Al igual que en los CD, hay distintas variantes según si sólo puede leer, leer y escribir, etc.: DVD-ROM, DVD-RAM, etc. La capacidad de un DVD va desde los 4,7 Gb (una cara, una capa) hasta los 17 Gb (doble cara, doble capa).

- **Chat (Conversational Hypertext Access Technology):** Comunicación simultánea en línea, que permite a dos o más usuarios interactuar a través de Internet mediante el teclado, la voz y el video. Requiere la coincidencia temporal de los dos o más interlocutores.

- **Código malicioso (malware):** Es un tipo de software que tiene como objetivo infiltrarse o dañar una computadora sin el consentimiento de su propietario. El término malware es muy utilizado por profesionales de la informática para referirse a una variedad de software hostil, intrusivo o molesto. El término virus informático suele aplicarse de forma incorrecta para referirse a todos los tipos de malware, incluidos los virus verdaderos.

- **Confidencialidad:** Consiste en garantizar que el activo de información no esté disponible o sea accesado y/o divulgado por o hacia personas, 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.

• **Correo electrónico o e-mail:** Es un servicio tecnológico que 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 ALFM este correo institucional corresponde al que se accede a través de Outlook o bien mediante el link al sitio de Correo Zimbra que se encuentra en el Portal Web de la Entidad.

• **Corriente regulada:** Es aquella que proviene de una fuente o unidad de poder ininterrumpida, que garantiza su estabilidad y permanencia, evitando sobre voltaje que pueda dañar los equipos. Para la operación de los equipos de cómputo es recomendable utilizar corriente regulada.

• **Corriente no regulada:** Es aquella proporcionada directamente por la empresa proveedora del servicio de energía.

• **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.

• **Cuenta de Usuario:** Es el identificador que utiliza la red o un Sistema de Información en la autenticación de un usuario.

• **Disponibilidad:** Se trata de la capacidad de un servicio, de unos datos o de un sistema, a ser accesible y utilizable por los usuarios (o procesos) autorizados cuando estos lo requieran. Supone que la información pueda ser recuperada en el momento en que se necesite, evitando su pérdida o bloqueo.

• **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.

• **Exploits:** (del inglés to exploit, explotar o aprovechar) es una pieza de software o una secuencia de comandos con el fin de causar un error o un fallo en alguna aplicación, provocando un comportamiento no deseado o imprevisto en los programas informáticos, hardware, o componente electrónico (por lo general computarizado). Con frecuencia, esto incluye cosas tales como la toma de control de un sistema de cómputo o permitir la escalada de privilegios o un ataque de denegación de servicio.

• **Gusano informático (IWorm):** Es un malware que tiene la propiedad de duplicarse a sí mismo de forma automática, lo que le permite propagarse e infectar una red informática sin ayuda externa.

- **Hacker:** Término utilizado incorrectamente para definir a un delincuente informático. Realmente un hacker es cualquier experto en tecnología informática capaz de desarrollar software para cualquier propósito. El hacker dedicado a producir y propagar malware se define realmente como cracker.

- **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 social y de relaciones personales 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.

- **Incidente:** Se define como un acceso, intento de acceso, uso, divulgación, modificación o destrucción no autorizada de información; un impedimento en la operación normal de las redes, sistemas o recursos informáticos; o cualquier otro acto que implique una violación a la Política de Seguridad de la Información.

- **Integridad:** hace referencia a la cualidad de la información para ser correcta y no haber sido modificada, manteniendo sus datos exactamente tal cual fueron generados, sin manipulaciones ni alteraciones por parte de terceros.

- **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, 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 o la Web.

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

- **Log:** Archivo que registra movimientos y actividades de un determinado programa, utilizado como mecanismo de control y estadística.

- **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.

- **Memoria USB:** (**U**niversal **S**erial **B**us) Dispositivo de almacenamiento portátil, de gran capacidad, que se coloca en un computador mediante un conector de tipo USB.

- **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.

- **Perfil de Navegación:** Hace referencia a las autorizaciones que tiene cada tipo de usuario para poder navegar en Internet, esto va ha encaminado al control y supervisión del tráfico que se genera en la red de la entidad.

- **Phishing:** Es un término informático que denomina un tipo de delito encuadrado dentro del ámbito de las estafas cibernéticas, y que se comete mediante el uso de un tipo de ingeniería social caracterizado por intentar adquirir información confidencial (como puede ser una contraseña o información detallada sobre tarjetas de crédito u otra información bancaria) de forma fraudulenta. El estafador, conocido como phisher, se hace pasar por una persona o empresa de confianza en una aparente comunicación oficial electrónica, por lo común un correo electrónico o algún sistema de mensajería instantánea, o incluso utilizando también llamadas telefónicas.

- **Puertas traseras:** (o en inglés backdoor), en un sistema informático es una secuencia especial dentro del código de programación, mediante la cual se pueden evitar los sistemas de seguridad del software (autentificación) para acceder al sistema. Aunque estas puertas pueden ser utilizadas para fines maliciosos y espionaje no siempre son un error, pueden haber sido diseñadas con la intención de tener una entrada secreta para administración y mantenimiento.

- **Ransomware:** Es un tipo de código malicioso que cifra los archivos del sistema infectado y pide un rescate a cambio de la llave de descifrado. El usuario no puede acceder a los archivos cifrados perdiendo la información contenida en ellos.

- **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.

- **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 y/o no se tiene permiso del fabricante para su uso.

- **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 usuario 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 o proveedor del mismo.

- **Spoofing:** en términos de seguridad de redes hace referencia al uso de técnicas de suplantación de identidad generalmente con usos maliciosos o de investigación. Se pueden clasificar los ataques de spoofing en función de la tecnología utilizada. Entre ellos tenemos el IP spoofing (quizás el más conocido), ARP spoofing, DNS spoofing, Web spoofing o email spoofing, aunque en general se puede englobar dentro de spoofing cualquier tecnología de red susceptible de sufrir suplantaciones de identidad.

- **Tecnologías de la información y las comunicaciones (TICs):** Son todos aquellos recursos, herramientas y programas que se utilizan para procesar, administrar y compartir la información mediante diversos soportes tecnológicos, tales como: computadoras, teléfonos móviles, equipos de audio y video, etc.

- **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.

- **Troyano:** Es un software malicioso que se presenta al usuario como un programa aparentemente legítimo e inofensivo, pero que, al ejecutarlo, le brinda a un atacante acceso remoto al equipo infectado.

- **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, disco externo):** 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, la memoria USB y los discos externos.

- **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.

- **Zip (comprimir):** Acción de empaquetar en un solo archivo, uno o más ficheros, que habitualmente son también objeto de compresión, con el fin de que ocupen menos espacio en disco y requieran menor tiempo para enviarlos por la red. Existen aplicaciones de compresión de este tipo muy populares: 7ZIP®, WinZip®, Winrar® y NetZIP® para Windows®; MacZip® para Macintosh® y Zip® y UnZip® para UNIX®. El resultado es un solo fichero con un sufijo ".zip", ".7z" o ".rar".

- **Vpn:** tecnología de red privada virtual, que crea una conexión cifrada desde una conexión externa a una plataforma o servicio de la entidad. El propósito de utilizar una VPN segura es que garantiza el nivel de seguridad adecuado para los accesos de personal autorizado que se encuentra fuera de red LAN o WAN de la Entidad.

- **Vulnerabilidad:** una debilidad o fallo en un sistema de información que pone en riesgo la seguridad de la información posibilitando que un atacante pueda comprometer la integridad, disponibilidad o confidencialidad de la misma.

3. POLÍTICAS QUE DEFINEN ESTÁNDARES DE SEGURIDAD Y ADMINISTRACIÓN DE OPERACIONES EN INFRAESTRUCTURA TIC

Los usuarios deberán utilizar los mecanismos y herramientas establecidas por la entidad para producir, mantener y proteger la información soportándose desde la infraestructura tecnológica de la ALFM. De igual forma, deberán salvaguardar la información reservada o confidencial que por necesidades institucionales deba ser almacenada o transmitida, ya sea dentro de la red interna o hacia redes externas como internet u otros canales de comunicación para el intercambio de información entre dos o más partes interesadas.

Los usuarios de la ALFM que hagan uso de un equipo de cómputo donde operar plataformas, software o información de la entidad, deben conocer y aplicar todas las medidas y buenas prácticas para prevenir la instalación y ejecución de código malicioso, tal como pueden ser virus, troyanos, gusanos de red o ransomware, botnets, apps maliciosas, spyware, adware, entre otros.

3.1 Manejo de medios e información

a. Toda solicitud para utilizar un medio de almacenamiento de información compartido (file share), uso de unidad de CD/DVD o uso de puertos USB, deberá efectuarse mediante el formato "SOLICITUD DE EXCEPCIONES DE SEGURIDAD INFORMÁTICA", debidamente autorizado por el Jefe de la Dependencia y con la respectiva Justificación de la solicitud, registrar el caso en la "mesa de ayuda" y hacer entrega de dicho formato en la Oficina de TICs de la entidad.

b. Los usuarios deberán respaldar (salvaguardar) permanentemente la información sensible y crítica que se encuentre en sus computadoras o estaciones de trabajo asignadas y de requerir apoyo de personal de TIC para ello, pueden registrar el caso en la "mesa de ayuda informática".

c. Los usuarios de la Agencia Logística deben conservar los registros o información que se encuentra activa y aquella que ha sido clasificada como reservada o confidencial, de conformidad a las disposiciones que emita la ALFM y la Ley 1712 de 2014 de Acceso a la Información Pública Nacional.

d. Las actividades que realicen los usuarios a través de los servicios e infraestructura tecnológica de la ALFM son registradas y susceptibles de auditoría conforme a los logs de trazabilidad de los sistemas de información y plataformas.

3.2 Control de software operacional y de ofimática

Los funcionarios, al utilizar los equipos de cómputo y el software allí instalado, deben observar y cumplir con las siguientes directrices respecto a la instalación, desinstalación y uso de software:

a. Solamente está permitido el uso de software licenciado por la entidad y/o aquel que, sin requerir licencia por ser software libre y de código abierto (GNU –GPL), y debe ser expresamente autorizado e instalado por el personal de la Oficina de TICs.

b. El único autorizado para instalar o desinstalar software de ofimática en las estaciones de trabajo de la ALFM son los funcionarios de soporte técnico de la Oficina de TICs, o a través de esta Oficina los terceros (proveedores) que brinden soporte al hardware y software operando en la entidad.

c. Mantener en todos los equipos de la ALFM solamente software licenciado y autorizado por la Oficina de TICs, por tanto, está prohibido mantener o intentar instalar cualquier otro tipo de software. El infringir esta disposición acarreará la apertura de las investigaciones respectivas, en razón a que este tipo de prácticas pueden generar sanciones para la ALFM al vulnerar los "Derechos de Autor".

d. Está estrictamente prohibido para los funcionarios (excluyendo de esta prohibición al personal debidamente autorizado de la Oficina de Tics, que de acuerdo a su rol y o funciones requiera y esté debidamente autorizado), instalar, ejecutar y/o utilizar programas o herramientas de software o hardware que:

- Monitoreen la actividad de los sistemas de información, plataformas de red y equipos locales o remotos. Se excluye de esta prohibición las herramientas de software y hardware que utilice la Oficina de TICs con el único propósito de administrar la funcionalidad y la seguridad de los recursos informáticos institucionales.

- Rastreen vulnerabilidades en sistemas de cómputo (hardware o software). Se excluye de esta prohibición las herramientas que utilice la Oficina de TICs con el único propósito de constatar los niveles de la seguridad de los recursos informáticos institucionales.

- Tengan un carácter de juegos y/o contenidos pornográficos.

e. El software y hardware instalado en los equipos de cómputo de la ALFM no debe ser utilizado con propósitos ilegales, mal intencionado, no autorizado, con fines o propósitos personales o ajenos a la misión de la entidad y a las funciones asignadas en el cargo del funcionario.

f. Se considera una falta grave el que los usuarios no autorizados instalen o intenten instalar cualquier tipo de programa (software) en las estaciones de trabajo asignadas, servidores, o cualquier equipo conectado a la red de la ALFM. Cualquier software instalado debe estar previamente autorizado por la Oficina de TICs y estar relacionado en el inventario de software que la entidad reporta a la Dirección Nacional de Derechos de Autor.

3.3 Servicio de correo electrónico institucional

El servicio de correo electrónico institucional es una herramienta de apoyo a las funciones y responsabilidades de los funcionarios de la ALFM y en tal virtud, su uso debe sujetarse a la Guía de Manejo de los Medios

Tecnológicos de Comunicación de la entidad, mediante las siguientes directrices:

a. El servicio de correo electrónico institucional de la ALFM, debe ser empleado únicamente para enviar y recibir mensajes de orden institucional.

b. El usuario que tiene asignado una cuenta de correo de la entidad, es el único responsable de todas las acciones y mensajes que se lleven a cabo en su nombre. Por lo tanto, el usuario debe abstenerse de suministrar el usuario/password de correo a terceros y efectuar el cambio de la clave de acceso periódicamente (junto con el password de red).

c. Las cuentas de usuario y sus respectivos buzones de correo electrónico asignados, tendrán vigencia limitada y serán administrados por la Oficina de TICs.

d. Todo usuario de correo electrónico deberá revisar periódicamente su correo durante su permanencia en la Entidad, descargando al disco duro del equipo asignado la información que considere pertinente y útil para su trabajo y eliminando aquellos correos e información que considere no importante para sus funciones, tal como correos Spam, correos duplicados, correos innecesarios, entre otros. Aquellas cuentas de correo que tengan más de 2 meses sin ser revisadas serán desactivadas automáticamente y el usuario tendrá que solicitar de nuevo su activación al administrador de correo mediante la radicación del respectivo caso de soporte en la plataforma de "mesa de ayuda".

e. Todo usuario puede cambiar su clave de red (password), en cualquier momento; en todo caso el sistema le pedirá cambio de contraseña de red mínimo cada 15 días obligatoriamente.

f. El usuario es responsable en la eliminación, cambio de lugar o cambio de nombre del archivo **".pst"**, en el cual la herramienta de correo electrónico Outlook guarda automáticamente todo lo que se realice en esa cuenta de correo. Este archivo se creará en la misma carpeta donde se encuentran los archivos de trabajo del usuario, con el fin de que cuando se realice el backup de información quede un respaldo de este archivo de correo en caso de daño de la máquina o del software. Para cualquier cambio referente a la ubicación de archivo **".pst"** el usuario debe solicitar a través de la "mesa de ayuda" el respectivo soporte y acompañamiento de la Oficina de TICs, con el fin de evitar la posible pérdida de información.

g. El usuario puede acceder al buzón de correo institucional por la herramienta Outlook desde el computador ubicado en las instalaciones de ALFM o bien si se encuentra fuera de las instalaciones de la ALFM, vía Internet, desde al acceso al correo en el portal web de la entidad. En cualquiera de estos casos se deberán respetar las políticas establecidas en este documento para el uso adecuado del servicio de correo.

h. En caso que el usuario reciba un correo no deseado y/o contenido de procedencia desconocida, este deberá de inmediato notificar el hecho a la Oficina de TICs, a fin de hacer el respectivo seguimiento y tomar las medidas pertinentes de bloqueo a ese remitente y al o los links que contenga y generar las alertas de seguridad para evitar que se materialicen amenazas por motivo de la recepción de ese contenido malicioso.

i. Los correos que por ser considerados riesgosos o sospechosos, serán catalogados como "Spam" por la plataforma de seguridad de la ALFM y serán colocados en "cuarentena" y al usuario destinatario le llegará un email con la relación de estos correos bloqueados.

j. Si el usuario considera que un correo entrante que está en la lista de "cuarentena" corresponde a un correo válido, no riesgoso y de remitente conocido, puede solicitar la liberación de este, enviando un email a la cuenta de correo electrónico liberarspam@agencialogistica.gov.co , el cual la Oficina TIC procederá a liberarlo y le llegará normalmente ese correo al usuario destinatario que lo solicitó, para que pueda gestionarlo.

k. A través del servicio de correo no se podrá ejecutar ningún tipo acto de espionaje (hacking o cracking), o envío de cadenas masivas, ya que pueden comprometer, afectar y/o a saturar los servicios TIC propios de la entidad y de terceros.

l. Los usuarios no deberán suscribir el correo institucional asignado por la ALFM a grupos de noticias, listas de correo, sitios de comercio electrónico y demás servicios que utilicen el correo institucional para la recepción de mensajes de carácter personal, comercial y de índole diferente a las funciones asociadas al cargo, en razón a que esto propicia la llegada de "Spam" (correo masivo no deseado), congestionando y saturando el normal funcionamiento del servicio de correo. La utilización del mecanismo de listas o cadenas, solo puede llevarse a cabo cuando se trate de la comunicación de un mensaje de orden estrictamente institucional oficial y solo por las personas que están previamente autorizadas para realizar dicho envío.

m. El buzón de correo electrónico institucional debe consultarse constantemente, con el propósito de atender con celeridad los asuntos a cargo, apoyar la política de Cero Papel y también evitar que el buzón de correo se llene e impida el ingreso y salida de mensajes hacia y desde ese buzón.

n. Los mensajes según su utilidad, deberán ser eliminados o almacenados de manera organizada por carpetas o temas en la herramienta Outlook y/o en el disco duro del computador o en cualquier otro medio de almacenamiento previamente autorizado.

o. Permanentemente se debe abrir el software Outlook (donde se tiene configurado el correo) en el equipo institucional asignado, para que se descarguen los correos entrantes que están en el correo de Zimbra; de lo contrario el buzón de correo se llena e impide el ingreso y salida de mensajes hacia y desde ese buzón del usuario.

p. Todo mensaje sospechoso respecto de su remitente o contenido debe ser reportado al área de tecnología para realizar el respectivo análisis, posterior a ello deberá ser eliminado sin abrirlo y sin ejecutar el contenido, en razón a que puede contener virus o alguna otra forma de contenido malicioso.

q. Se prohíbe el envío de correos tipo "cadena", puesto que generalmente son utilizados por ciberdelincuentes para ingresar código malicioso e infectar la plataforma tecnológica.

r. La cuenta de correo no debe utilizarse para enviar o recibir música, programas, material pornográfico, fotos, vídeos o cualquier otro tipo de mensajes y archivos ajeno a los fines de la Entidad.

s. La cuenta asignada o el buzón electrónico, no puede ser ofrecido o facilitado a personas no autorizadas o ajenas a la entidad y con interés diferentes a las establecidas por la ALFM.

t. Los usuarios deben ser conscientes de las implicaciones que tiene la utilización del correo electrónico de la ALFM, en términos de responsabilidad e imagen institucional, por lo tanto se abstendrán de cualquier uso indebido que ponga en riesgo la imagen corporativa y la seguridad informática y de la información de la Entidad.

u. El correo no debe ser usado para la transmisión masiva de información voluminosa (archivos grandes), para lo cual se debe optar por otro tipo de herramientas informáticas (ejemplo: publicar la información en la Intranet o en una carpeta pública). Si es el caso se debe solicitar el respectivo apoyo a la Oficina de TICs para establecer el canal que cumpla con las condiciones apropiadas para garantizar que la transferencia o publicación sea efectiva.

v. La Oficina de TICs asignará las direcciones de correo electrónico al personal, única y exclusivamente al momento de estar formalizado el ingreso a la Entidad, de acuerdo con las novedades reportadas por la Dirección Administrativa y de Talento Humano y el envío del formato correspondiente de "creación de usuario", debidamente diligenciado y firmado.
w. Al crear las cuentas de correo electrónico Institucional, la Oficina de TICs establecerá criterios de restricción, de acuerdo a las funciones, rol o perfil del usuario, a efectos de racionalizar la capacidad del buzón, delimitar la posibilidad de enviar mensajes colectivos o a distintos grupos, orígenes o destinatarios, entre otras medidas.

x. Cuando quien tenga asignado una cuenta de correo institucional y sea desvinculado de la entidad u ordenada la restricción de acceso por uso indebido a través de la Dirección Administrativa y de Talento Humano; esta Dirección es responsable de reportar periódicamente y cada vez que exista cambios o movimientos de personal informando todas las novedades del personal para garantizar la desvinculación de usuarios de los sistema y plataformas. La Oficina de TICs cancelará de forma inmediata la dirección electrónica asignada y cesará el derecho de uso para el usuario. De igual forma, se cancelará el servicio a aquellos buzones que no hayan tenido actividad por el término de tiempo destinado en las políticas de administración de este servicio (2 meses o más).

3.4 Protección contra códigos maliciosos

a. Para prevenir infecciones por malware, los usuarios de la ALFM no deben hacer uso de software que no haya sido proporcionado y validado por la Oficina de TICs.

b. Los usuarios de la entidad son responsables de verificar que la información y los medios de almacenamiento (USB, DVD, etc.) estén libres de cualquier tipo de código malicioso, para lo cual deben ejecutar con frecuencia el escaneo de estos medios de almacenamiento con el software antivirus de uso institucional y también deben autorizar los escaneos automáticos de antivirus que se realizan de manera controlada.

c. Los usuarios que están previamente autorizados para el uso de dispositivos extraíbles como (USB, disco duro externo, entre otros), deben analizar dichos dispositivos previamente a la apertura de sus archivos.

d. Todos los archivos de computadora que sean proporcionados por personal externo o interno (programas de software, bases de datos, documentos, hojas de cálculo, etc.), que tengan que ser descomprimidos (archivos .zip), deben ser verificados utilizando el software antivirus autorizado, antes de ejecutarse o abrirlos.

e. Ningún usuario de la ALFM debe, intencionalmente, escribir, generar, compilar, copiar, propagar, ejecutar o tratar de introducir código de computadora diseñado para auto replicarse, dañar, modificar o impedir el funcionamiento de cualquier equipo de cómputo, memoria, archivos o software. Mucho menos probarlos en cualquiera de los ambientes o plataformas informáticas de la Entidad. El incumplimiento de

esta política será considerado una falta grave y se tomarán las medidas pertinentes frente al caso.

f. Cualquier usuario que sospeche de algún tipo de afectación por infección de virus en la estación de trabajo asignada, deberá dejar de usar inmediatamente el equipo y llamar a la Oficina de TICs para la detección y erradicación del virus.

g. Los usuarios no deberán alterar o eliminar las configuraciones de seguridad que sean implementadas en la ALFM para detectar y/o prevenir la propagación de virus en herramientas de trabajo tales como: Antivirus, Outlook, Office, Navegadores u otras plataformas y sistemas de información.

3.5 Uso del Servicio de Internet Institucional

El servicio de Internet suministrado por la ALFM es una herramienta de apoyo a las funciones y responsabilidades de los usuarios, por lo tanto, al utilizarlo, deben observar y cumplir las directrices de la entidad referentes a:

a. El uso de los recursos de red para el acceso al servicio de Internet es de índole institucional y deberá ser utilizado con el propósito expreso de realizar tareas relacionadas con las actividades de la entidad y funciones asignadas al cargo.

b. El acceso a Internet no podrá ser utilizado para ingresar a cuentas de correo personales (no institucionales), salvo en casos excepcionales que se requiera de la utilización de este servicio y que esté debidamente autorizado por la Oficina de TICs, caso en el cual se deberá remitir la solicitud en el formato establecido y cumpliendo con los protocolos para tal fin.

c. La Oficina de TICs asignará el uso de Internet a los usuarios que lo requieran de acuerdo a las funciones y responsabilidades de su trabajo, tan solo con motivos de interés institucional y con previa autorización del jefe inmediato del usuario.

d. El servicio de Internet no debe ser utilizado para:

- Enviar, descargar o recibir archivos de video, audio, texto, fotos, etc., con contenidos insultantes, ofensivos, injuriosos, obscenos o violatorios de los derechos de autor, no propios del cumplimiento de los propósitos institucionales o de las funciones laborales asignadas.

- Escuchar música conectado directamente al sitio en Internet que provee este servicio o mediante el acceso directo a un equipo de la red local institucional.
- Descargar, instalar o ejecutar archivos o software no autorizado por la Oficina de TICs y que comprometa la seguridad y el normal funcionamiento de los equipos, servicios y plataformas de la Entidad.

- El uso de Internet en cualquier actividad que sea lucrativa o comercial de carácter individual; así como el uso del servicio de correo para propósitos fraudulentos, publicitarios o para la propagación de mensajes SPAM no relacionados con la actividad laboral.

- Utilizar los recursos de la ALFM para ganar acceso no autorizado a redes y sistemas remotos a través de puertas traseras de sistemas (backdoor).

- La suplantación o uso no autorizado de la cuenta de acceso de otra persona para efectuar navegación

a internet, será considerado como falta grave conforme a lo establecido en la ley y las directivas internas de seguridad establecidas por la ALFM en temas de seguridad digital.

- El acceso a sitios de contenidos obscenos, que distribuyan libremente material pornográfico, material subversivo o de grupos al margen de la ley, ofensivo, en perjuicio de terceros, que riñan contra la moral y las buenas costumbres, y así como la redistribución de dicho material a través de correo electrónico o medio similar canales de comunicación institucional.

- Realizar actos de espionaje (hacking, cracking, ingeniería social), que lesionen o no y que pongan en riesgo la información y los derechos de funcionarios y de terceros.

- Violar o intentar violar los sistemas de seguridad de los equipos a los cuales se tenga acceso, tanto a nivel local como externo.

- Decodificar el tráfico de la red o cualquier intento no autorizado de obtención de la información que se transmita a través de la misma o de los canales de comunicación institucionales.

- Violar o intentar violar los sistemas de seguridad para realizar labores propias de los administradores de la plataforma tecnológica.

- Acceder mediante el servicio de Internet asignado a contenidos que puedan estar relacionados con plataformas y servidores generadores de spam o malware, o que puedan contener programas que permitan romper o descifrar claves de acceso, u otros que puedan entenderse corno contenidos que puedan utilizarse con fines no lícitos o no autorizados y en consecuencia de ello sean dañinos y que puedan comprometer tanto a la Entidad como a terceros.

e. La conexión a Internet siempre debe cerrarse o desconectarse cuando no se esté navegando, cerrando el navegador de Internet para de esa manera evitar consumir innecesariamente el canal de internet.

f. Todas las Oficinas, Direcciones y Regionales están obligadas a cumplir con lo establecido en el Decreto 1151 del 14 de abril de 2008 (Agenda de Conectividad) de acuerdo con los lineamientos y estándares que para tal fin desarrolle el líder de Gobierno en Digital de la ALFM.

g. La Oficina de TICs está autorizada para limitar el acceso a Internet, utilizando los filtros necesarios para restringir el acceso a determinadas páginas y contenidos, de igual manera también utilizando la aplicación de horarios de conexión, los servicios ofrecidos por la red, la descarga de archivos y cualquier otro contenido ajeno a los fines institucionales, con el fin de salvaguardar la confidencialidad, integridad y disponibilidad de la información y la efectividad de los controles establecidos en la administración de las redes y plataformas de la ALFM, por medio de la aplicación de los siguientes perfiles de navegación:

- **Perfil de navegación Bajo:** Perfil configurado a las necesidades de la mayoría de los usuarios de la Entidad, pensado en los permisos únicamente de portales y páginas web que estén alineados en la misión de la ALFM, bloqueando o interrumpiendo categorías que no estén encaminadas a las funciones de la entidad (permite el acceso a páginas del Estado, .GOV, .MIL).

- **Perfil de navegación Medio**: Perfil configurado con características de navegación más altas que el perfil Bajo. Dichas propiedades se proyectaron para personal con funciones específicas de cotizaciones,

pagos, consultas en blogs, portales especializados y todo aquel sitio que no es de común acceso para la mayoría de los funcionarios, bloqueando o interrumpiendo únicamente las categorías de streaming (contenido audiovisual), entretenimiento y las relacionadas a estas.

- **Perfil de navegación Tecnología:** Perfil configurado con características de navegación similar al perfil Medio, pero orientado para el personal de la Oficina de TICs y agentes de soporte en las Regionales, con funciones técnicas específicas, que permiten la navegación a portales especializados de tecnologías y asociados a las funciones asignadas, la instalación y configuración del software autorizado en la entidad.

- **Perfil de navegación Alto:** Perfil configurado con las características de navegación más alta que el perfil Medio, dichas propiedades se proyectaron para personal con funciones concretas (contratistas ERP-SAP, personal Directivo en Principal y Regionales) que por las funciones del cargo no deben tener limitantes en la navegación. Sin embargo, se bloquean las categorías como Hacking, remote Tools, Religión, Armas, Pornografía y demás relacionadas a estas.

h. La Oficina de TICs realizará monitoreo y control a las conexiones de Internet y reportará, en caso de requerirse, a la Secretaría General, los sitios visitados por quienes tienen asignados accesos a internet, que no correspondan a las funciones propias del cargo, con el fin de que se inicien las acciones disciplinarias a que haya lugar.

i. El uso de Internet y del correo electrónico está restringido exclusivamente para el cumplimiento de la misión institucional por parte de los usuarios que así lo requieran por la naturaleza de sus cargos, funciones y actividades; lo cual debe ser avalado y justificado por el jefe inmediato de la dependencia.

j. La información institucional deber ser enviada por medio del correo institucional y no por otros tipos de correo electrónico y o canales no autorizados.

k. No se permite el ingreso a páginas o portales con contenidos pornográficos, musicales, videos, juegos, redes sociales, correos personales y todo aquello de carácter ocioso y ajeno a las actividades de la Entidad y/o que no estén debidamente autorizados.

l. No se permite descargar, ni instalar cualquier tipo de software utilitario o software de aplicaciones, antivirus, música, videos, p2p (aplicaciones para intercambio y búsqueda de archivos), etc., los cuales generalmente contienen código malicioso que puede infectar la red de la ALFM.

m. No está permitido el uso de cualquier tipo de software de mensajería instantánea diferente al que se establezca y sea previamente promovido y autorizado por la ALFM.

n. Cualquier instalación de software, utilitarios, antivirus, etc., previamente debe ser debidamente probado en entornos controlados y debidamente autorizado por la Oficina de TICs.

o. Se prohíbe dentro de las instalaciones de la ALFM usar como medio de salida a Internet: los asistentes digitales, los computadores portátiles, los teléfonos inteligentes personales o cualquier otro dispositivo o periférico diferente a los debidamente asignados y autorizados por la Oficina de TICs.

p. Se prohíbe que los equipos de la ALFM asignados a un usuario, se conecten a servicios de internet no suministrados por la ALFM (por ejemplo, redes inalámbricas o datos de celulares), salvo validación y autorización por parte de la Oficina de TICs.

q. No está permitido que el acceso a Internet otorgado, sea para usos diferentes a los institucionales, por ejemplo: ver videos, escuchar música, cargue/descargue de fotos, acceso a correos personales, acceso a Facebook, Twitter o cualquier otro tipo de redes sociales. Se excluye el personal debidamente autorizado en cumplimiento de sus funciones; debido a que este tipo de actividades consumen grandes recursos de ancho de banda del canal de Internet, que pueden saturar los canales de comunicación y afectar en últimas la velocidad y calidad del servicio para todos los usuarios conectados a la red.

r. Solo se podrán acceder a aquellas páginas, portales, blogs y foros afines a sus cargos, con los cuales puedan desarrollar con mayor calidad y eficiencia sus labores diarias, basados en la justificación y soportes de cada caso.

s. Se podrá utilizar Internet como fuente de crecimiento del conocimiento, capacitaciones virtuales, artículos de importancia, etc. que puedan redundar en el mejoramiento continuo los procesos de la ALFM y que sean autorizados por el personal Directivo en los días y/o horarios que así lo autoricen.

4 POLÍTICAS Y ESTÁNDARES DE SEGURIDAD FÍSICA Y PERSONAL

Establecer parámetros claros para el acceso de personal externo a la entidad, así como el ingreso de equipos tecnológicos externos y en general los procedimientos que se deben seguir para fortalecer la seguridad en el acceso a las instalaciones de la ALFM.

4.1 Medidas de seguridad preventivas y predictivas

a. Efectuar permanentes estudios de seguridad al personal que labore en la Entidad (funcionarios y terceros), encaminados a detectar y/o prevenir eventuales ataques informáticos y/o fuga de información que sea originada al interior de la ALFM.

b. Implementar medidas de control de acceso a visitantes, que eviten el ingreso y/o salida fraudulenta de equipos, portátiles, PDA, tablets u otros dispositivos o periféricos, impidiendo a su vez la conexión de estos equipos a las redes de la Entidad, salvo que medie previa autorización por parte de la Oficina de Tics.

c. Implementar medidas de seguridad encaminadas a evitar y detectar: la divulgación y empleo de documentos de la ALFM para fines personales, la violación ilícita de comunicaciones o correspondencia de la entidad (física o electrónica), revelación de información no autorizada (de forma física o electrónica), utilización indebida de información obtenida en el ejercicio de las funciones o actividades desarrolladas en la ALFM, o posibles eventos configurados como espionaje (físico o electrónico).

d. La Dirección Administrativa y de Talento Humano y el área de Seguridad Patrimonial (tanto de la sede principal como de Regionales), deben Informar periódicamente y de manera permanente a la Oficina de TICs, las novedades de personal (retiros, vacaciones, licencias, permisos, etc.), para proceder con el bloqueo de usuarios en los servicios informáticos de los funcionarios que se retiran o ausentan temporalmente de la entidad.

5 POLÍTICAS Y ESTÁNDARES DE SEGURIDAD TECNOLÓGICA

Los mecanismos de control de acceso físico para el personal de la entidad y terceros, deben permitir el acceso a las instalaciones y áreas restringidas de la ALFM únicamente a las personas previamente autorizadas, para la salvaguarda de los equipos de cómputo y de comunicaciones, y también para restringir y controlar el acceso al Centro de Cómputo de la entidad solo al personal estrictamente autorizado y en cumplimiento de sus

funciones.

5.1 Protección de la información

a. El usuario deberá reportar de forma inmediata a la Oficina de TICs y al área Administrativa, cuando detecte que existen riesgos reales o potenciales de daño de los equipos de cómputo o de comunicaciones, como pueden ser fugas de agua, comienzo de incendio, cortos eléctricos u otros.

b. El usuario tiene la obligación de proteger los dispositivos removibles y físicos que se encuentren bajo su administración y que contengan o no información reservada o confidencial, aun cuando no se estén utilizando en el momento.

c. Es responsabilidad del usuario evitar permanentemente la fuga de la información perteneciente a la ALFM que se encuentre almacenada en los equipos de cómputo personales o de la entidad que tenga asignados, teniendo en cuenta el uso y la aplicación de buenas prácticas de seguridad.

5.2 Controles de acceso físico y de equipos

a. Cualquier persona que tenga acceso a las instalaciones de la ALFM deberá registrar al momento de su entrada, el equipo de cómputo, equipo de comunicaciones, medios de almacenamiento y herramientas que no sean propiedad de la ALFM, los cuales podrá retirar el mismo día. En caso contrario deberá tramitar la autorización de salida correspondiente.

b. Los equipos de cómputo asignado, las computadoras portátiles, módems y cualquier otro activo tecnológico, podrá ingresar o salir de las instalaciones de la ALFM diligenciando el formato establecido y vigente para "Ingreso y Salida de Elementos", el cual debe ser firmado por el Jefe de Seguridad de la ALFM y por el Jefe de la Dependencia visitada.

5.3 Seguridad en Datacenter o Centro de Cómputo

El Datacenter es el lugar donde se encuentran ubicados todos los servidores de redes, servidores de bases de datos, servidores de software aplicativo, los dispositivos de seguridad, almacenamiento, comunicaciones y gabinetes del cableado horizontal y vertical de la red de la ALFM, UPS, entre otros.

En consecuencia, para su utilización se establecen las siguientes directrices:

a. El Centro de Cómputo es un área restringida y por lo tanto solo se puede ingresar a ella con autorización del Jefe de la Oficina de TICs o del (los) funcionario(s) designado(s) por esa Jefatura a través de las Coordinaciones.

b. La operación de cualquiera de los dispositivos que se encuentren en el centro de cómputo, solo podrá realizarse por los funcionarios designados (autorizados) por la Jefatura de la Oficina de TICs.

c. Las personas que ingresen al Centro de Cómputo, deberán seguir las normas de seguridad que para el efecto se dispongan desde la Oficina de TICs, tales como:

- Diligenciar previamente la planilla de ingreso y autorización al Datacenter, indicando claramente las actividades a realizar en el sitio, día y horas de entrada y salida y las firmas de la persona que ingresa y del administrador del Datacenter de la ALFM.
- No ingresar ningún tipo de bebidas o alimentos.
- No accionar ninguno de los dispositivos de alarmas sin razón ni autorización.
- No encender objetos que puedan ocasionar que las alarmas y sistemas de seguridad se activen tales como: cigarrillos, fósforos, encendedores, etc.
- No conectar equipos de soldadura, aspiradora, brilladora u otro electrodoméstico o herramienta industrial.
- No operar ninguno de los diferentes equipos que en él se encuentran instalados sin autorización del Jefe de la Oficina de TICs o de alguno de los profesionales autorizados de la misma área.
- Se debe brindar acompañamiento permanente de un funcionario de la ALFM al personal externo cuando realice procesos de mantenimiento y diligenciar el formato al ingreso y salida del Datacenter, establecido para tal fin.

5.4 Protección y uso de recursos tecnológicos

Los activos tecnológicos de la ALFM son herramientas de apoyo a las labores y a las responsabilidades del personal que se encuentran relacionados a la función pública: por ello al utilizar los bienes y servicios tecnológicos, se deben observar y cumplir las siguientes directrices de uso:

a. Los activos tecnológicos institucionales se emplearán de manera exclusiva por el funcionario al cual han sido asignados y únicamente para el correcto desempeño de su cargo, por lo tanto, no pueden ser utilizados con fines personales o cedidos a terceros no autorizados.

b. Durante la jornada laboral y en todo tiempo de uso, corresponde al funcionario prestar la debida custodia y cuidado a los equipos de cómputo y demás recursos tecnológicos asignados, así como impedir su sustracción, destrucción o utilización indebida.

c. Todo funcionario debe verificar que los equipos de cómputo asignados se encuentren debidamente conectados a la toma de corriente regulada y soportada por la UPS (color rojo o naranja generalmente), diseñada exclusivamente para computadores y servicios de TIC. No está permitido realizar derivaciones eléctricas desde las fuentes de corriente regulada ni conectar multitomas a las mismas, ni conectar elementos diferentes a los equipos de cómputo en estas tomas, como por ejemplo aspiradoras.

d. Los equipos de cómputo o sus partes (CPU, monitor, teclados, impresoras, diademas, parlantes y demás elementos que se encuentren conectados a la CPU) dispuestos para el cumplimiento exclusivo de las funciones del usuario, no podrán ser reemplazados ni cambiados de puesto, sin autorización escrita de la Oficina de TICs, quien establecerá la viabilidad técnica del cambio, previa autorización del Jefe de la Dependencia en donde se encuentre ubicado el elemento e informando del traslado al Almacén General de la entidad (dado que corresponde a elementos registrados en inventarios) y para lo cual se deberá diligenciar y firmar por las partes el Formato de "Traslado de Inventario" vigente.

e. Los únicos autorizados para realizar modificaciones a la configuración original de los equipos, así como para destapar, agregar, desconectar, retirar, revisar y/o reparar sus componentes, son los funcionarios de la Oficina de TICs y/o la empresa que preste el servicio de soporte y mantenimiento de hardware y cuyo personal esté autorizado para esta labor.

f. Todos los archivos externos provenientes del correo electrónico o de medios magnéticos, ópticos, dispositivos inalámbricos y demás formas de transmisión de datos, antes de ser copiados en cualquier

equipo de la ALFM, deberán ser revisados, con el software antivirus instalado por la Oficina de TICs. En caso de detectarse cualquier tipo de virus, el archivo debe ser eliminado y se debe informar del suceso de manera inmediata a la Oficina de TICs.

g. El servicio de soporte para cualquier requerimiento o falla relacionado con el hardware, software y plataformas de TI de la ALFM, deberá ser solicitado por la "mesa de ayuda" (intranet en el link (enlace) habilitado para ello); si no es posible desde el equipo asignado, se podrá hacer desde otro equipo, previa autorización de su responsable.

h. No está permitido introducir en los equipos de cómputo elementos ajenos a su naturaleza o funcionalidad, así como ningún tipo de unidad de almacenamiento de información portátil como CD, DVD o memorias USB que estén físicamente dañadas o que no hayan sido revisadas previamente por el programa antivirus licenciado por la entidad, y para ello debe mediar previa autorización de la Oficina de TICs, previo diligenciamiento del formato de "Excepciones de Seguridad" por parte del usuario, con la respectiva justificación de la necesidad y con el aval y firma del Subdirector/Director/Jefe de la Dependencia.

i. Toda pérdida de equipos de cómputo o de algunos componentes de TI, debe ser informada de inmediato a la Oficina de Seguridad por el funcionario que tenga a cargo el equipo, generando el respectivo informe a la Dirección Administrativa y de Talento Humano y con copia a la Oficina de TICs.

j. Los equipos de cómputo, impresoras y otros periféricos siempre deben apagarse en caso de ausencias prolongadas y al final de la jornada laboral, cumpliendo las estrategias para el ahorro de energía, evitar el desgaste innecesario de los equipos y la aplicación de buenas prácticas para alargar el tiempo de vida útil de los elementos de TI.

k. Todo problema de orden técnico con los equipos debe ser reportado a la Oficina de TICs a la mayor brevedad posible para recibir el tratamiento y manejo apropiado según sea el caso, el funcionario no debe intentar manipular los elementos ni tampoco dar solución a través de terceras personas sin el consentimiento de la Oficina de TICs.

5.5 Mantenimiento de equipos

a. Únicamente el personal autorizado por la Oficina de TICs (sea personal interno o contratista), podrá llevar a cabo los servicios de atención y reparaciones a la plataforma de TIC, por lo que los usuarios deberán solicitar la identificación del personal designado antes de permitir el acceso a sus equipos y según el caso se debe contar con el acompañamiento y supervisión de personal de la Oficina Tics.

b. Los usuarios deberán asegurarse de respaldar (hacer backups/ copia de seguridad) a la información que consideren relevante cuando el equipo sea enviado a reparación (de ser posible) y también debe asegurarse de borrar aquella información sensible que se encuentre en el equipo, previendo así la pérdida involuntaria de información, derivada del proceso de reparación y/o de mantenimiento según sea el caso.

6 POLÍTICAS DE SEGURIDAD EN LA RED

Política

Será considerado como un ataque a la seguridad informática y de la información y una falta grave, cualquier actividad no autorizada por la Oficina de TICs, en la cual los usuarios realicen la exploración de los recursos informáticos en la red de la ALFM, así como de las aplicaciones que sobre dicha red operan, con fines de

detectar y explotar una posible vulnerabilidad que ponga en riesgo el normal funcionamiento, así como disponibilidad, integridad y confidencialidad de la información.

6.1 Instauración de mecanismos de protección de la información

a. Los Funcionarios y Terceros que cometan violaciones a la seguridad de la información y/o que generen pérdida o daño de bienes (software o hardware) de la Entidad, deberán someterse a los procedimientos, investigaciones y auditorias establecidos por la Oficina de Control Interno Disciplinario de la ALFM.

b. Todos los usuarios, personal en comisión, contratistas y terceros, tienen la obligatoriedad de reportar a la Oficina de TICs cualquier tipo de incidente y/o vulnerabilidad a la seguridad de la información, que evidencien o que sospechen, respecto a los servicios que se prestan a través de la red de datos de la entidad y que podrían tener un eventual impacto en la seguridad de los activos tecnológicos y de la información de la ALFM.

c. No se otorgará ningún acceso a servicios de la plataforma tecnológica que no venga avalado y autorizado única y exclusivamente por los señores Subdirectores Generales, directores nacionales, Jefes de Oficina y Directores Regionales, de acuerdo al formato establecido y vigente en la Suite Visión.

d. Se administrarán de forma controlada y restrictiva las conexiones remotas que se puedan requerir a través de herramientas como VPN (red privada virtual), otorgando así los permisos de acceso y privilegios y suprimiéndolos una vez culminados los trabajos remotos solicitados; y estableciendo un mecanismo para control de los mismos (lapso de tiempo, horarios, etc.).

e. Se implementarán controles criptográficos en los siguientes casos:
- Protección de claves de acceso a sistemas, datos y servicios.
- Transmisión de información clasificada a entes externos que así lo requieran.
- Acceso a sistemas de información o software aplicativo desde Internet.

f. Se realizará la oportuna actualización de las bases de datos de antivirus y de los parches al sistema operativo y software requerido para servidores, estaciones de trabajo, portátiles, terminales y demás equipos que pertenezcan a la Entidad.

g. Los contratistas y terceros que laboren en las instalaciones de la ALFM o que accesan desde equipos remotos a la plataforma de la ALFM (ejemplo vía VPN), deberán garantizar que sus equipos personales de trabajo estén debidamente protegidos con un antivirus y adicional que estén actualizados en cuanto a los parches de seguridad y actualizaciones del sistema operativo.

h. Existirán controles y redundancia adicional de seguridad física y lógica para la plataforma tecnológica (hardware, software y conectividad) catalogada como de alta criticidad y sensibilidad de acuerdo a la disponibilidad de los recursos presupuestales asignados.

i. Se supervisará y monitoreará permanentemente que los equipos de cómputo que contengan información clasificada o sensible, sean operados únicamente por las personas autorizadas y que se dé cumplimiento a todas las normas y lineamientos de seguridad establecidas para la protección y operación de las plataformas TIC de la entidad.

6.2 Monitoreo de uso de equipos de computación y canales de comunicaciones

a. Se controlará permanentemente toda conexión interna, externa o de acceso remoto, requerida por funcionarios y/o contratistas, para impedir que se establezcan conexiones externas que pudieran permitir a usuarios ajenos obtener acceso a las plataformas tecnológicas de la ALFM.

b. Se implementarán mecanismos de control que restrinjan posibles brechas en la seguridad de la plataforma tecnológica de la Entidad, producto de malas prácticas por parte de los usuarios internos, bien sea desde las estaciones de trabajo asignados o sus equipos personales.

c. Se divulgarán periódicamente, mediante el uso de "tips", recomendaciones, boletines y, alertas, todos los aspectos contemplados en el presente manual y toda aquella información encaminada a concientizar usuarios y blindar y proteger la seguridad de la información en la ALFM.

7. POLÍTICAS DE ESCRITORIO LIMPIO

Todo el personal está obligado a proteger la información de la ALFM, en cualquiera de sus formas, que se puede encontrar en escritorios, equipos de cómputo, computadores portátiles, medios ópticos, medios magnéticos, documentos en papel y, en general, toda la información que es utilizada por los funcionarios para apoyar la realización de sus actividades laborales en la Entidad.

7.1. Ubicación de escritorios y equipos

Los equipos que queden ubicados cerca de zonas de atención o tránsito de público, deben situarse de forma que las pantallas no puedan ser visualizadas por personas externas y/o ajenas a las funciones de la entidad.

7.2. Escritorios limpios

a. Toda vez que un funcionario, personal en comisión o contratista se ausenta de su lugar de trabajo, debe bloquear su equipo de cómputo asignado y/o equipo personal, deberá guardar en lugar seguro cualquier documento, medio magnético u óptico removible que contenga información confidencial y sensible.

b. Al finalizar la jornada laboral el funcionario o tercero debe guardar en un lugar seguro los documentos y medios que contengan información confidencial o de uso interno, además debe cerrar sesión en los aplicativos que utiliza y debe apagar el equipo de cómputo asignado.

7.3. Pantallas limpias

a. Los computadores de escritorio y equipos portátiles, deben tener aplicado el estándar relativo (fondo de pantalla) y/o protector de pantalla definido por el Grupo de Marketing y la Oficina de TICs.

b. La pantalla de autenticación a la red de la institución debe requerir como mínimo la identificación de la cuenta y una clave asignada.

c. Los funcionarios, personal en comisión y contratistas, al ausentarse de su lugar de trabajo deben bloquear su equipo de cómputo, para de esta forma proteger la información alojada en aplicaciones, servicios y plataformas de la ALFM.

7.4. Equipos de reproducción de información

Los equipos de reproducción como son: fotocopiadoras e impresoras, deben estar ubicados en lugares con acceso controlado y cualquier documentación confidencial, con información clasificada o sensible, se deberá retirar inmediatamente de estos equipos luego de realizadas las tareas.

8. POLÍTICA PARA LA GESTIÓN Y ACCESO DE USUARIOS

Cada usuario es responsable del mecanismo de control de acceso que le sea proporcionado; esto hace referencia al usuario y contraseña asignado, necesarios para acceder a la información y a la infraestructura tecnológica de la ALFM, por lo cual deberá mantenerlo de forma confidencial y no suministrarlo a terceras personas. La cuenta de usuario es de carácter personal e intransferible, y como consecuencia su titular es el único responsable de su uso.

8.1. Registro y cancelación del registro de usuarios

a. La Dirección Administrativa y de Talento Humano debe informar inmediatamente a la Oficina de TICs, el ingreso, traslado y/o retiro (transitorio o definitivo) de personal de planta, personal de comisión y personal de prestación de servicio, para que se proceda a la creación, modificación o cancelación de las cuentas del sistema, aplicativos, servicios de internet, intranet, correo y demás herramientas tecnológicas. Así mismo, ante la ausencia temporal de un funcionario (por vacaciones, excusas médicas, entre otras), deberá informar a la Oficina de TICs para la suspensión transitoria de sus cuentas de usuario (red, aplicativos y demás servicios informáticos).

b. La creación de las cuentas de usuario (red, aplicativos y demás herramientas informáticas) y su acceso correspondiente, solo puede ser otorgado por la Oficina de TICs, siguiendo los procedimientos y registros establecidos en los formatos de "Creación de Usuario".

c. El suministro de datos falsos con el fin de obtener una cuenta para ganar acceso no autorizado a los recursos de cómputo de la entidad, será informado a las autoridades competentes, con el fin que se inicien las investigaciones y se apliquen las sanciones aplicables.

d. El usuario (funcionario o contratista) deberá firmar el formato de "Creación de Usuario" en el cual queda por escrito el compromiso de aplicar y cumplir a cabalidad las políticas de seguridad de la entidad, que asume al recibir su nombre de usuario y contraseña.

e. La Oficina de TICs asignará los usuarios, contraseñas iniciales, roles y privilegios para acceso al software aplicativo, únicamente al personal cuyo ingreso a la entidad esté legalizado, y de acuerdo con los requerimientos del Jefe de la dependencia plasmados en el formato que la Oficina de TICs emplee para tal fin.

f. La Oficina de TICs efectuará la permanente actualización de los usuarios, roles y privilegios, acorde a las novedades de personal reportadas por las dependencias y la Dirección Administrativa y de Talento Humano.

g. De requerir habilitar acceso a algún servicio informático de la ALFM a un personal ajeno a la Entidad, el Jefe de la Dependencia donde estará operando el personal, debe solicitar, informar y sustentar de

manera coherente las razones de la solicitud a la Oficina de TICs y de manera concertada proceder a asignar los usuarios, roles y privilegios respectivos temporalmente. Una vez que ya no sea requerido el acceso a ese servicio, se debe informar de inmediato a la Oficina de TICs para suprimir las autorizaciones brindadas. La Oficina de TICs debe verificar permanentemente esas autorizaciones a personal ajeno a la entidad y efectuar los ajustes al respecto de manera controlada.

h. Es responsabilidad de la Dirección Administrativa y de Talento Humano, que, en el caso de vacaciones, licencia o retiro de algún funcionario de la Entidad, se informe inmediatamente a la Oficina de TICs la cancelación o inhabilitación de su cuenta de usuario de forma temporal o definitiva, evitando el uso de sus claves por cualquier otra persona, tanto en aplicativos como en las demás plataformas tecnológicas.

i. Al crear las cuentas de correo electrónico Institucional, la Oficina de TICs establecerá criterios de restricción, de acuerdo con las funciones o perfil del usuario, a efectos de racionalizar la capacidad del buzón, delimitar la posibilidad de enviar mensajes colectivos o a distintos grupos, orígenes o destinatarios, entre otras medidas.

j. Para el caso de usuarios (funcionarios o terceros) que deban deshabilitarse o modificar sus accesos, producto de desvinculación o reasignación de funciones, la Oficina de TICs no lo eliminará de las herramientas informáticas a las cuales tenga acceso, sino que lo bloqueará, desactivará o dejará inactivo, de tal forma que se pueda llegar a consultar de usuario inactivo las actividades o movimientos registrados en el sistema o herramienta tecnológica a la cual tenía acceso.

8.2. Suministro de cuentas de acceso a usuarios

a. Las cuentas y sus servicios informáticos asociados que no sean utilizados en un período superior a (2) el usuario en referencia y cesará el derecho de uso de su cuenta. De igual forma, se bloqueará el acceso al software aplicativo para aquellos funcionarios que deban ausentarse de la entidad por un largo periodo de tiempo (ejemplo: vacaciones, licencias).

b. La Oficina de TICs debe asignar privilegios de usuario para cada uno de los servicios informáticos, de acuerdo con lo solicitado por el jefe de la dependencia usuaria de la información, verificando la razonabilidad entre los privilegios solicitados y las funciones del solicitante, de acuerdo a los formatos de "creación de usuarios" y "excepciones de seguridad" definidos por la Oficina de TICs.

c. La Oficina de TICs debe efectuar la permanente actualización de los usuarios, roles y privilegios, según las novedades de personal reportadas por las dependencias y la Dirección Administrativa y de Talento Humano (tanto de la sede Principal como de las Regionales).

d. El Grupo de Seguridad y el personal de Tecnología deberán comunicar a todos los usuarios, contratistas y terceros, la obligatoriedad de informar y reportar los diferentes tipos de incidentes y vulnerabilidades que evidencien o sospechen en los servicios que se presten a través de la red de datos y servicios informáticos de la entidad y que podrían tener un impacto en la seguridad de los activos tecnológicos de la ALFM, de esa manera se procederá a alertar también a entidades de seguridad del estado para de esa manera prevenir la afectación a otras entidades y a la población en general.

e. No deben existir usuarios (funcionarios o contratistas) con acceso privilegiado total a las herramientas tecnológicas, y ante la eventualidad de que sea estrictamente necesario, se debe registrar la justificación en el formato de "Creación de Usuario" con el aval del director/jefe de la dependencia a la cual pertenece

el usuario, y este tipo de usuarios serán objeto de monitoreo especial permanente.

8.3. Administración de los derechos de acceso de usuarios

a. Los administradores de la plataforma tecnológica y Agentes de Soporte Técnico, junto con los directores nacionales, Jefes de Oficina y Directores Regionales, deben controlar los privilegios asignados a los usuarios de las aplicaciones a su cargo, verificando que estén definidos de acuerdo a sus funciones asignadas en cada proceso. Esta actividad se deberá efectuar mínimo una vez cada trimestre y reportar por escrito a la Oficina de TICs, cualquier novedad y/o ajuste que se deba efectuar al respecto producto de un traslado o reasignación de funciones, entre otros.

b. La Oficina de TICs asignará el uso de Internet a los usuarios que lo requieran de acuerdo a las responsabilidades de su trabajo y funciones asignadas, tan solo por motivos de interés institucional y con previa autorización del jefe inmediato del usuario, quien debe verificar mínimo una vez cada trimestre esas autorizaciones y reportar por escrito a la Oficina de TICs, cualquier novedad y/o ajuste que se deba efectuar al respecto.

c. La Oficina de TICs deberá revisar periódicamente los privilegios asignados a los usuarios e implementar mecanismos de control que restrinjan posibles brechas en la seguridad de la plataforma tecnológica de la Entidad, producto de malas prácticas por parte de los usuarios internos, bien sea desde los equipos de cómputo asignados o desde sus equipos personales.

d. Está prohibido que los funcionarios de la ALFM utilicen sus equipos personales en las instalaciones de la entidad para cumplir sus funciones, excepto en los casos en los cuales dadas las condiciones así se requiera y sea autorizado por el Director o Jefe del área, caso en el cual se informará a la Oficina de TIC para que proceda a habilitar el respectivo acceso.

e. Toda la información generada producto del desempeño de las actividades de un usuario de TIC en la ALFM, es propiedad de la entidad, por lo tanto, se debe salvaguardar y velar por su correcta utilización. Cualquier uso diferente deberá ser solicitado mediante autorización a los directores y Jefes de Oficina acorde al caso. El usuario no podrá eliminar la información contenida en el equipo asignado como activo bajo su responsabilidad. Esto ocasionará investigaciones y sanciones disciplinarias.

f. De la información referente a la ALFM que se manipule en equipos personales debe entregarse una copia a la Dependencia a la cual pertenece el usuario, para salvaguarda y posterior consulta.

g. De requerir habilitar acceso a algún servicio informático de la ALFM a un personal ajeno o terceros a la Entidad, el jefe de la dependencia donde estará operando el personal, debe informar a la Oficina de TICs, y de manera concertada proceder a asignar los usuarios, roles y privilegios respectivos y temporales. Una vez ya no sea requerido el acceso a ese servicio, se debe informar de inmediato a la Oficina de TICs para suprimir o deshabilitar las autorizaciones brindadas. La Oficina de TICs debe verificar permanentemente esas autorizaciones brindadas al personal ajeno o terceros a la entidad y efectuar los ajustes al respecto de manera controlada.

h. Se deberán mantener activos los archivos log en los diferentes servicios informáticos y sistemas de información autorizados a los usuarios, de forma que permitan contar con un historial de eventos efectivo de los accesos y movimientos realizados en la plataforma tecnológica de la ALFM.

i. Es responsabilidad de cada usuario (funcionario o contratista) tener actualizado en el inventario del Almacén General la relación de las herramientas tecnológicas asignadas; y al terminar su empleo, contrato o acuerdo, deberá efectuar la entrega controlada de esos inventarios al Almacén General, verificando previamente y en conjunto con el Coordinador o Jefe Directo, que se haya realizado el backup respectivo y se haya eliminado de los equipos la información sensible, especialmente si los equipos van a ser reasignados a otras dependencias o al Almacén General en caso de que ocurra una devolución.

9. POLÍTICAS DE CONTROL DE ACCESO A SISTEMAS Y APLICACIONES

Brindar a los usuarios los parámetros para acceder a los sistemas de información y aplicaciones y para el uso adecuado de estas herramientas sin vulnerar la seguridad de la información de la entidad.

9.1. Procedimiento de ingreso seguro

a. Todos los usuarios de los sistemas informáticos de la ALFM deben diligenciar el formato de "Creación de Usuario" establecido por la Oficina de TICs, para que se determinen los perfiles o privilegios de acceso a las aplicaciones de acuerdo a su cargo y funciones a desempeñar en la Entidad.
f. dos meses, serán bloqueadas e inactivadas del sistema.

g. La Oficina de TICs, acorde al presupuesto disponible, podrá establecer medidas de seguridad para restringir el acceso a los recursos informáticos, como pueden ser: tarjetas magnéticas, firmas digitales, medios de identificación biométrica o cualquier otro similar, que garanticen la identidad y autenticación correcta del usuario.

h. El usuario (funcionario o tercero) deberá firmar un formato en el cual queda por escrito el compromiso de aplicar las políticas de seguridad de la entidad, que asume al recibir su nombre de usuario y contraseña.

i. Al crear los usuarios, roles y privilegios de acceso al software aplicativo institucional, la Oficina de TICs establecerá criterios de restricción, de acuerdo con las funciones o perfil del usuario, a efectos de restringir y/o delimitar el uso de transacciones no autorizadas, siempre soportándose en los criterios que se establezcan en el formato diligenciado y enviado por las Jefaturas y Direcciones.

j. Cuando un funcionario o contratista que tenga asignado un acceso a un software aplicativo, sea desvinculado de la entidad, o se ordene la restricción de acceso por uso indebido, previa notificación por la Dirección Administrativa y de Talento Humano, la Oficina de TICs bloqueará de forma inmediata
b. Administración de accesos de usuarios: La Oficina de TICs establece los procedimientos para controlar la asignación de derechos de acceso a los sistemas, datos y servicios de información avalados por la Coordinación de cada proceso y el director de la dependencia, justificada a través del formato "Creación de Usuario" debidamente diligenciado, el cual debe reposar en la Oficina de TICs.

c. Creación de Usuarios

- La Oficina de TICs, deberá mantener los registros donde cada uno de los líderes responsables de los procesos haya autorizado a los servidores públicos o terceros el acceso a los diferentes sistemas de información de la entidad.
- Los datos de acceso a los sistemas de información deberán estar compuestos por un ID o nombre de usuario y contraseña que debe ser único por cada servidor público o tercero.

• Cuando se retire o cambie de contrato cualquier servidor público o tercero, se deberá aplicar la deshabilitación y cambios de privilegios en los sistemas de información a los que el usuario estaba autorizado.

9.2. Sistema de gestión de contraseñas

a. Los funcionarios de la ALFM deben establecer sus contraseñas de acceso a los equipos de cómputo y aplicaciones cumpliendo con un mínimo de 8 caracteres y la combinación de números, letras mayúsculas y minúsculas, y al menos un carácter especial.

b. Todos los funcionarios de la ALFM deberán cambiar su contraseña de acceso a los diferentes sistemas de información con una frecuencia de mínimo una (1) vez cada quince días.

c. Por políticas y lineamientos de seguridad de acceso a los sistemas de información, los usuarios de acceso a la red se deben bloquear automáticamente luego de 3 intentos fallidos de autenticación.

d. En caso que un funcionario de la ALFM sea trasladado o removido de las funciones en la operación de los diferentes sistemas de información o herramientas informáticas, el líder del proceso debe solicitar a la Oficina de Tecnología mediante correo electrónico o medio escrito, la deshabilitación o modificación del perfil según corresponda.

9.3. Control de acceso a códigos fuente de programas

a. La pérdida de información en el software aplicativo (y sus bases de datos), puede ser generada en un alto porcentaje por diversas fallas ajenas al software mismo, para lo cual los funcionarios de la ALFM deberán:

• Minimizar la ocurrencia de fallas físicas del hardware, velando por un adecuado ambiente de operación del mismo (temperatura, humedad, polvo) y reportando a la Oficina de TICs, con la debida pertinencia, las fallas u operación irregular que se observe en el hardware (equipo) y/o software debidamente instalado en este.

• Verificar constantemente el entorno de funcionamiento del equipo de cómputo sobre el cual opera el sistema, constatando permanentemente que no existan aspectos que puedan afectar su funcionalidad y con ello la correcta operación de los aplicativos: temperatura excesiva. humedad, polvo, fallos de corriente, cables de red defectuosos, entre otros, e informando inmediatamente a la Oficina de TICs estas anomalías para concertar su solución.

• Minimizar la ocurrencia de fallas en los sistemas aplicativos, originados por intervención humana, debido a configuraciones inapropiadas, manipulación indebida, mala ejecución de los procedimientos establecidos y errores en el ingreso de la información al sistema. El usuario del software aplicativo deberá sujetarse permanentemente a las políticas establecidas en los manuales de operación del software aplicativo (manuales de uso).

• Los usuarios y terceros de la ALFM deben cumplir, acatar y aplicar estrictamente las directivas permanentes y transitorias emitidas por la Oficina de TICs para la debida operación de las plataformas de TI.

• Los funcionarios de la ALFM tienen la obligación de asistir a las capacitaciones que se programen respecto del software que utilizan para su labor. En caso de duda al ejecutar un procedimiento en el software, deben

consultar con el funcionario especialista del área, con la Oficina de TICs o en los manuales de usuario del software respectivo.

b. Ante un error en el funcionamiento del software aplicativo, los funcionarios de la ALFM deberán sujetarse a los procedimientos establecidos en los manuales y directrices de la Oficina de TICs y no intentar de forma alguna, por sus propios medios, acceder a los programas (fuentes y ejecutables) del aplicativo ni a las bases de datos en donde reposa la información.

c. Para la atención de irregularidades o errores en el software aplicativo, la Oficina de TICs tiene trazado el siguiente mecanismo de atención:

- El usuario del software reporta el error a la Oficina de TICs mediante Ticket (caso de mesa de ayuda).
- La Oficina de TICs le asignará el requerimiento a un funcionario especialista en el tema.
- El funcionario de la Oficina de TICs entrará en contacto con el usuario final del caso, estableciendo plenamente el requerimiento, determinando su causa probable y proyectará la solución al mismo (bien sea de forma remota o definitivamente mediante desplazamiento al sitio).
- El caso atendido se documenta y se informa vía al usuario final y al Jefe de la dependencia respectiva, con la trazabilidad de la solución en la herramienta de "mesa de ayuda" y entrega a satisfacción al funcionario.
- Se archiva toda la información del caso como soporte y como elemento de consulta de lecciones aprendidas para futuros requerimientos similares.

10. POLÍTICAS PARA COPIAS DE RESPALDO

La Oficina de TICs define el tipo de copias y la periodicidad de las mismas, así como los soportes en las que se deben realizar y las ubicaciones de los centros de respaldo, conformando un documento denominado "Guía de Backup de Aplicativos".

10.1. Respaldo de la información

a. Al realizar copias de seguridad en CD o DVD y proceder a su etiquetado, la etiqueta correcta debe incluir la siguiente información:

- Identificador de copia. Mediante esta cadena alfanumérica se identifica de manera uniforme cada una de las copias de seguridad realizadas. Este debe incluir la dependencia o regional que genera la copia.
- Tipo de copia. Se debe indicar si la copia es incremental, diferencial o completa.
- Fecha en la que se realizó la copia.
- Contenido. Siempre se incluirá el contenido en clave que almacena la copia de seguridad. Esto permitirá recuperar un determinado archivo sin necesidad de estar cargando cada una de las copias en el equipo.
- Responsable. Debe indicar el nombre del funcionario que realizó la copia de seguridad para que facilite las consultas o las peticiones de actualización y restauración de la misma en caso de ser necesario.

b. La Oficina de TICs, al etiquetar correctamente las copias de seguridad, llevará un registro exhaustivo de las mismas y de las restauraciones realizadas.

c. El personal responsable de ejecutar las tareas de backups y recuperación deberá regirse por los procedimientos y actividades establecidas en la Guía de Backups de Software Aplicativo y Herramientas Informáticas y en el Plan de Contingencia, con el fin de que la Entidad cuente con información de copias segura, confiable y disponible, que le permita cumplir con las metas y asegurar la correcta operación de los sistemas y aplicativos.

d. El responsable del uso de un bien informático, mantendrá una copia de seguridad de sus archivos de ofimática (Word, Excel, PowerPoint, AutoCAD, etc.) correspondientes a su estación de trabajo, en otro medio de almacenamiento, como CD o DVD, USB, disco externo, probando a su vez el mecanismo de recuperación, para lo cual la Oficina de TICs deberá orientar y capacitar a todos los funcionarios que lo requieran para realizar backups de los archivos en uso e identificar a cuáles se debe hacer copia periódica de acuerdo al aplicativo (o software de ofimática) que maneje, teniendo en cuenta los parámetros establecidos en la Guía de Backups de Software Aplicativo y Herramientas Informáticas.

e. El Coordinador de Grupo del área cuyo usuario deba tomar copia de la información, verificará la existencia de la copia de seguridad actualizada, de toda la información relevante, que resida en los equipos de cómputo asignados a su dependencia.

f. La Oficina de TICs debe registrar las restauraciones realizadas y los motivos que han ocasionado dicha recuperación y llevará un registro, con mínimo los siguientes campos:

- **Fecha de restauración** en la que se realizó la recuperación de la copia.
- **Incidencia que ha motivado la restauración**. Decir la causa que ocasionó la restauración de la información.
- **Ubicación**. Decir el equipo en el que se realiza la restauración de la información perdida.
- **Técnico**. El funcionario responsable que lleva a cabo la restauración.

10.2. Restauración de backups

Esta actividad se realizará ante la ocurrencia de un siniestro con la información o ante una solicitud de restauración esporádica a archivos de usuarios y bases de datos, y finaliza con el backup restaurado y los archivos con información institucional y bases de datos de aplicaciones informáticas y sistemas de información de la ALFM instaladas y en plena producción.

a. Verificar el último backup existente y confiable (almacenado, verificado, etiquetado), de acuerdo a las políticas, procedimientos y guías establecidos para tal fin.

b. Ejecutar la restauración del Backup bajo la directriz del administrador de la Plataforma tecnológica y de coordinador del Grupo y de acuerdo a los instructivos de instalación según el software o herramienta a restaurar, teniendo presente las configuraciones requeridas de hardware, software, bases de datos, esquemas de comunicación y demás configuraciones necesarias (tanto en servidores como en máquinas cliente).

c. Verificar y probar la integridad y funcionalidad del software y de la información del backup restaurado.

d. Notificar a los usuarios finales sobre la herramienta restaurada, para su verificación y aval, y para la entrada en operación formal de la base de datos, de los archivos, de software o herramienta informática requerida.

11. POLÍTICAS PARA EL REGISTRO DE EVENTOS Y SEGUIMIENTO

Mediante el registro de eventos en los diversos recursos informáticos de la plataforma tecnológica se efectuará un seguimiento a los accesos realizados por los usuarios a la información de la Entidad, con el objeto de minimizar el riesgo de pérdida de integridad de la información. Cuando se presenten eventos que pongan en riesgo la integridad, veracidad y consistencia de la información se deberán documentar y realizar las acciones tendientes a su solución.

11.1. Registro de eventos

a. En caso de que se presenten problemas o se produzcan errores o se quiera conocer exactamente qué acciones ejecutan los sistemas operativos o los diferentes programas o servicios de la entidad, se puede acceder a los llamados archivos log, o ficheros de registro de eventos. Estos "logs" los cuales son gestionados y estarán debidamente configurados en todas las aplicaciones, servidores, bases de datos y sistemas de manera automática y permitirán controlar (de forma centralizada) todos los procesos relevantes.

b. Control: Generar una política de operación donde los administradores por medio de los backup guarden los logs de los registros de los sistemas de operación para detectar:

- Novedad o incidencia que más se presenta. (repetitiva)
- Tipo de error
- Causa del error
- Corrección
- Definición «software o hardware.»
- Fecha y hora incidencia

11.2. Registros del administrador y del operador

a. El responsable de la Oficina de TICs (administrador de la plataforma de TI) desarrollará y verificará el cumplimiento de los procedimientos para comunicar las fallas en el procesamiento de la información o los sistemas de comunicaciones, que permitan tomar las medidas correctivas necesarias.

b. Se registrarán las fallas comunicadas en la "mesa de ayuda", debiendo existir reglas claras para el manejo de las mismas, con inclusión de:

- Revisión de registros de fallas para garantizar que las mismas fueron resueltas satisfactoriamente.
- Revisión de medidas correctivas para garantizar que los controles no fueron comprometidos, y que las medidas tomadas fueron autorizadas.
- Documentación de la falla con el objeto.

11.3. Sincronización de relojes

La sincronización de la hora deberá realizarse a través de las políticas establecidas en el Directorio Activo, tanto para equipos de cómputo como para servidores, y la hora será la establecida por el Instituto Nacional de Metrología, lo cual permitirá mantener la configuración conforme a la hora legal colombiana.

12. POLÍTICAS PARA TRATAMIENTO DE DATOS PERSONALES

La ALFM, a través de sus funcionarios y demás personas que intervengan en el "Tratamiento de Datos de Carácter Personal", tienen la obligación profesional de guardar y mantener la reserva de tales datos, salvo las excepciones legales, para lo cual se seguirán los respectivos conductos de control.

12.1. Protección de datos personales

a. La ALFM, en los procesos y aplicativos que requieran datos personales de usuarios, informará a los titulares de los datos personales el régimen de protección de datos adoptado por la Entidad, así como la finalidad y demás principios que regulan el tratamiento de estos datos. Así mismo, informará a los usuarios sobre la existencia de las Bases de Datos de carácter personal que custodie los derechos que le asisten a los titulares.

b. La ALFM facilitará al titular del dato el obtener toda la información respecto de sus propios datos personales, sean parciales o completos, del tratamiento aplicado a los mismos y su finalidad, la ubicación de las bases de datos que contienen sus datos personales y sobre las comunicaciones y/o cesiones realizadas respecto de ellos. De igual manera, de así requerirlo, la ALFM brindará los medios de comunicación para que estos sean actualizados, borrados o eliminados según el caso que los asista.

c. En desarrollo del principio del consentimiento informado, el titular del dato tiene derecho a otorgar su autorización, por cualquier medio que pueda ser objeto de consulta posterior, para tratar sus datos personales en la ALFM.

d. De manera excepcional, esta autorización no será requerida en los siguientes casos:

- Cuando la información sea requerida o deba ser entregada a una entidad pública o administrativa en cumplimiento de sus funciones legales, o por orden judicial.
- Cuando se trate de datos de naturaleza pública.
- En casos de emergencia médica o sanitaria.

e. La ALFM contempla dentro de los deberes a los encargados de la información de la Oficina de TICs (sede Principal y Regionales), lo siguiente:

- Garantizar al titular de los datos, en todo tiempo, el ejercicio pleno y efectivo de los derechos que le asisten como titular de los datos.
- Mantener las condiciones de seguridad necesarias para impedir la adulteración, manipulación pérdida, consulta, uso o acceso no autorizado o fraudulento de los datos personales.
- Realizar oportunamente la actualización, rectificación o supresión de los datos en los términos señalados en la Ley 1581 de 2012.
- Tramitar las consultas y reclamos formulados por los titulares en los términos señalados en la Ley 1581 de 2012.

f. La información de las Bases de Datos de la ALFM seguirá siendo tratada mientras se mantenga una relación legal o contractual con el titular de la información. En todo caso, de manera general, la información no será objeto de tratamiento por un período superior de veinte (20) años contados a partir de su recolección de acuerdo con las circunstancias legales o contractuales que hacen necesario el manejo de la misma, sin perjuicio de que, en cualquier caso, se mantenga para cumplir con gestiones de carácter estadístico, histórico o cualquier obligación de carácter legal.

CONTROL DE CAMBIOS

VERSIÓN	DESCRIPCIÓN DE CAMBIOS
01	Versión inicial.
02	Adición de normatividad aplicable Adición y eliminación de definiciones del glosario. Ordenamiento alfabético de las definiciones. Eliminación de políticas que se encontraban duplicadas en diferentes sitios del manual. Actualización de los nombres de las dependencias conforme al organigrama actual.
03	Adición de normatividad aplicable Adición y eliminación de definiciones del glosario. Ordenamiento alfabético de las definiciones. Revisión de redacción a las políticas que aplique.