

COPIA No. _____ DE _____ COPIAS
CIUDAD, Bogotá, D.C.
FECHA 12 JUL 2021

No 07 ALDG-ALOTIC-130

DIRECTIVA PERMANENTE

ASUNTO: Lineamientos de Seguridad Digital y de la Información, que abarcan la modalidad de Trabajo en Casa originado por la Emergencia Sanitaria por COVID-19.

AL: Señores Secretario General, Subdirectores Generales, Directores Nacionales, Jefes de Oficina, Directores Regionales y funcionarios de la Agencia Logística de las Fuerzas Militares.

1. OBJETIVO Y ALCANCE

a. Finalidad

1) Objetivos

- Objetivo general

Actualizar los lineamientos que orientarán a la Agencia Logística de las Fuerzas Militares (ALFM) en materia de Seguridad de la Información y Seguridad Digital de forma que todos los procesos orienten su funcionamiento con esta política, con la estrategia de Gobierno Digital del Estado Colombiano y con el Modelo de Seguridad y Privacidad de la Información (MSPI) de la ALFM, se establecen actividades que buscan implementar buenas prácticas para garantizar la seguridad de la información y derivado de la emergencia sanitaria por COVID-19 se autorizó el "Trabajo en Casa" de manera temporal para la entidad.

- Objetivos específicos

- Establecer y dar a conocer los 13 principios de seguridad que soportan el Sistema de Gestión de Seguridad de la Información (SGSI) de la ALFM.



07

- Integrar los lineamientos establecidos en este documento al funcionamiento de la ALFM, creando una cultura organizacional de seguridad de la información.
- Demostrar el liderazgo y compromiso de la Alta Dirección respecto al SGSI .
- Impartir lineamientos en materia de seguridad digital a los funcionarios de la entidad. Dada la emergencia sanitaria por el COVID-19, se incluyen acciones a la Política de Seguridad de la Información y Seguridad Digital, conforme a los lineamientos establecidos por Ministerio de Defensa y MINTIC.

2) Alcance

Esta directiva aplica a todos los procesos y funcionarios de la entidad, contratistas y terceros relacionados con la Agencia Logística de las Fuerzas Militares, y será revisada y actualizada por lo menos una vez al año o cuando amerite.

b. Referencias

- Ley 1273 de 2009, por medio de la 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.
- Documento CONPES 3701 de 2011, Lineamientos de Política para Ciberseguridad y Ciberdefensa.
- 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.
- Directiva Permanente Ministerio de Defensa No.018 de 2014, Políticas de Seguridad de la Información para el sector Defensa.
- Decreto 1078 de 2015, por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.

- 07
- Documento CONPES 3854 de 2016, Política Nacional de Seguridad Digital.
 - 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.
 - Decreto 1008 de 2018, por el cual se establecen los lineamientos generales de la política de Gobierno Digital.
 - Resolución No.5563 de 2018, por la cual se formula el Plan Estratégico de Tecnologías de la Información y las Comunicaciones del Sector Defensa y Seguridad 2018-2022.
 - Resolución No.27 del 17 de marzo de 2020, por la cual se adoptan medidas preventivas sanitarias, por causa del coronavirus - COVID-19 en la Agencia Logística de las Fuerzas Militares, y a través la cual establecen una serie de responsabilidades especiales.
 - 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.
 - Circular Externa N° 001 del AGN del 31 de marzo de 2020. Con asunto "LINEAMIENTOS PARA LA ADMINISTRACION DE EXPEDIENTES Y COMUNICACIONES OFICIALES".
 - Resolución No.408 del 20 de abril de 2020, por la cual se dictan medidas y acciones transitorias para administración de los expedientes y comunicaciones oficiales en medio de la emergencia sanitaria.
 - Documento CONPES 3995 de 1 de Julio de 2020, Política Nacional De Confianza y Seguridad Digital.
 - Resolución No.924 del 03 de noviembre del 2020, por la cual se dictan medidas y acciones transitorias para adopción de modalidades de trabajo para la prevención y cuidado colectivo frente al virus COVID-19.

- 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"
- LEY 2088 del 12 de mayo 2021 por la cual se regula el trabajo en casa y se dictan otras disposiciones.
- Resolución 506 de la ALFM, del 01 de junio 2021, por la cual se dictan medidas y acciones transitorias para adopción de modalidades de trabajo para la prevención y cuidado colectivo frente al virus COVID-19.

c. Vigencia

A partir de la fecha de su expedición. Deroga la directiva Permanente No.05 del 12 de marzo de 2019 y la directiva transitoria 03 de 14 de mayo de 2020 y las integra en este documento.

2. INFORMACIÓN – POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL

La Dirección General de la Agencia Logística de las Fuerzas Militares, entendiéndola importancia de una adecuada gestión de la información, se ha comprometido en liderar la implementación del Modelo de Seguridad y Privacidad de la Información (MSPI) en la entidad, buscando establecer un marco de confianza en el ejercicio de sus deberes con el Estado y los ciudadanos, dando cumplimiento a las leyes y normas vigentes y aplicables, en concordancia con la misión y visión de la entidad, y asignando los recursos necesarios para que esta implementación se pueda llevar a cabo.

Para la Agencia Logística de las Fuerzas Militares, la protección de la información busca la disminución del impacto generado sobre sus activos, por los riesgos identificados de manera sistemática, con el objeto de mantener un nivel de exposición que permita responder por la integridad, la confidencialidad y la disponibilidad de ésta, acorde con las necesidades de los diferentes grupos de interés identificados.

Para alinear la dirección estratégica de la Entidad, la Agencia Logística de las Fuerzas Militares establece la compatibilidad de los lineamientos de seguridad de la



07

información de la ALFM y los objetivos de seguridad de la información, estos últimos correspondientes a:

- Minimizar el riesgo asociado a la afectación de procesos misionales y en general de las funciones de la entidad para reducir impactos negativos.
- Cumplir con los principios de seguridad de la información.
- Cumplir con los principios de la función administrativa.
- Mantener la confianza de sus clientes, contratistas y empleados.
- Apoyar la innovación tecnológica.
- Proteger los activos tecnológicos.
- Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información y seguridad digital.
- Promover el uso de las mejores prácticas de seguridad de la información, como base de aplicación para el concepto de Seguridad Digital.
- Fortalecer la cultura y habilidades de seguridad de la información y seguridad digital en los funcionarios, terceros, practicantes, personal en comisión y usuarios de la ALFM.
- Apoyar a las entidades de orden nacional encargadas de velar por la seguridad digital del estado, y de la población en general, para generar alertas tempranas para prevenir la materialización de riesgos cibernéticos.
- Garantizar la continuidad de la operación del negocio frente a incidentes.

A continuación, se establecen los principios de seguridad que soportan el Sistema de Gestión de Seguridad de la Información y Seguridad Digital de la Agencia Logística de las Fuerzas Militares:

- La ALFM ha decidido definir, implementar, mantener y mejorar de forma continua un Sistema de Gestión de Seguridad de la Información, soportado en directrices claras alineadas a las necesidades de la misión institucional, y a los requerimientos normativos que le aplican a su naturaleza.



07

- Los roles y responsabilidades frente a la seguridad de la información serán definidas, compartidas, publicadas y aceptadas por cada uno de los funcionarios, contratistas, grupos de valor, partes interesadas o terceros.
- La ALFM protegerá la información generada, procesada o resguardada por los procesos de la Entidad, su infraestructura tecnológica y activos del riesgo que se genera de los accesos otorgados a terceros (ejemplo: proveedores, contratistas o clientes), o como resultado de un servicio interno tercerizado.
- La ALFM protegerá la información creada, procesada, transmitida o resguardada por sus procesos de negocio y del SIG, con el fin de minimizar impactos financieros, operativos o legales debido a un uso incorrecto de esta. Para ello es fundamental la aplicación de controles de acuerdo con la clasificación de la información de su propiedad o en custodia.
- La ALFM protegerá su información de las amenazas originadas por el personal interno o externo.
- La ALFM protegerá las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos.
- La ALFM controlará la operación de sus procesos de negocio y del SIG garantizando la seguridad de los recursos tecnológicos y las redes de datos.
- La ALFM implementará controles de acceso a la información, sistemas y recursos de red.
- La ALFM garantizará que la seguridad sea parte integral del ciclo de vida de los sistemas de información.
- La ALFM garantizará a través de una adecuada gestión de los eventos de seguridad y las debilidades asociadas con los sistemas de información, una mejora efectiva de su modelo de seguridad.
- La ALFM garantizará la disponibilidad de sus procesos de negocio, del SIG y la continuidad de su operación; basada en el impacto que pueden generar diferentes situaciones a causa de la Emergencia Sanitaria por COVID – 19.
- La ALFM garantizará el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas.

307

- La ALFM promoverá jornadas de sensibilización y capacitación referentes a la seguridad digital y de la información, para todos los funcionarios y personal externo que realice actividades que comprometan el manejo de información de la entidad.
- La ALFM establece con carácter temporal y extraordinario la modalidad del “Trabajo en casa”, a causa de la Emergencia Sanitaria por COVID – 19.
- La Dirección General de la ALFM se compromete con el desarrollo del Sistema de gestión de Seguridad de la Información (SGSI), brindando los recursos (económicos, logísticos, administrativos y de talento humano) necesarios para su implementación, mantenimiento y certificación.

3. EJECUCIÓN.

a. Misión General

A partir de la fecha, la Secretaría General, las Subdirecciones Generales, las Direcciones Nacionales, las Oficinas Nacionales y las Direcciones Regionales velarán por el pleno cumplimiento de las directrices establecidas en la presente Directiva, y la socializarán tanto a los funcionarios de la ALFM como a los contratistas y/o terceros relacionados con la ALFM.

b. Misiones Particulares

- Director General
 - a) Aprueba los lineamientos y los planes de seguridad de la información y seguridad Digital.
 - b) Aprueba las estrategias y mecanismos de control para el tratamiento de riesgos que se generen como resultado de los reportes o propuestas del Comité Institucional de Gestión y Desempeño.
 - c) Facilita los recursos requeridos para la implementación de los lineamientos y ejecución de los planes de seguridad de la información y seguridad digital.



- Secretaría General

Supervisa el cumplimiento de la presente Directiva que establece los lineamientos en materia de Seguridad y Privacidad de la Información de la ALFM.
- Comité Institucional de Gestión y Desempeño que absorbe el Comité de Seguridad de la Información
 - a) Revisa y propone a la alta dirección, los lineamientos de Seguridad de la Información y Seguridad Digital, con el fin de someterlos a aprobación
 - b) Realiza seguimiento a la implementación de los procedimientos relacionados con los lineamientos de Seguridad de la Información y Seguridad Digital.
 - c) Propone estrategias para la implantación de los controles necesarios para el adecuado cumplimiento y apropiación de los lineamientos de seguridad y la debida mitigación de las situaciones de riesgo detectadas.
- Subdirecciones Generales, Direcciones Nacionales, Jefes de Oficina y Direcciones Regionales
 - a) Clasifican los activos de información de acuerdo con el grado de sensibilidad y criticidad de estos, y mantienen esta información documentada y actualizada y apoyan la actualización de la "matriz de activos de información", con el acompañamiento y/o asesoría de la Oficina TIC (profesional de Seguridad Tecnológica y de la Información)
 - b) Solicitan a la Oficina TIC los permisos, roles y privilegios de acceso a la información para cada uno de sus colaboradores de acuerdo con sus funciones y competencia; en cumplimiento de los lineamientos establecidos al interior de la entidad
 - c) Ejercen el liderazgo y compromiso en la aplicación de los lineamientos de seguridad de la información al interior de su dependencia.

- 07
- d) Verifican el cumplimiento por parte del personal de los lineamientos establecidos en la presente directiva.
 - e) Socializan el contenido de la presente directiva con los funcionarios, contratistas y demás terceros que participan dentro de sus procesos.
 - f) Solicitan a la Oficina TIC los servicios de VPN para acceso a las aplicaciones o trabajo remoto a los funcionarios bajo su responsabilidad, para aplicar la modalidad de TRABAJO EN CASA; dicha solicitud deberá realizarse a través de caso en la “mesa de ayuda” anexando el formato GTI-FO-04 “Solicitud Creación o Actualización de Usuarios” debidamente diligenciado, en donde se incluirá justificación acorde y clara a la solicitud, y el cual deberá firmarse por el Coordinador de grupo, Director o jefe de la dependencia y el funcionario a quien se le habilitará el servicio solicitado, los cuales pueden ser:
 - Acceso remoto a equipos de cómputo por la VPN, el cual aplica a nivel Directivo y con el cumplimiento de los criterios establecidos en “Instrucciones Generales de Coordinación” de esta Directiva.
 - Acceso a Aplicativos por VPN.
 - Acceso a SAP a través del Router.
- Dirección Administrativa y de Talento Humano
 - a) Cumple con los lineamientos de seguridad de la información del Talento Humano.
 - b) Notifica a todo el personal que se incorpora a la ALFM, sus obligaciones respecto al cumplimiento de los lineamientos de seguridad de la información, incluidos en la presente directiva. y de todas las normas, procedimientos y prácticas que de ella surjan.
 - c) Incluye dentro del plan anual de capacitación temas referentes a la seguridad de la información y tecnologías de la 4 revolución, así como socializa las diferentes convocatorias promovidas por MINTIC y otras entidades para gestionar la participación de los funcionarios de la ALFM.
 - d) Emite los lineamientos respecto a la clasificación, disposición y aseguramiento de la información al interior de la entidad, conforme a las directrices emitidas por el Archivo General de la Nación.

07

- Oficina Asesora Jurídica
 - a) Define, documenta y actualiza los requerimientos estatutarios, regulatorios y contractuales en materia de seguridad de la información, y establece los lineamientos de la entidad para satisfacer esos requerimientos.
 - b) Asesora a la entidad en materia legal, en lo relacionado a la seguridad de la información, y establece las pautas legales que permitan cumplir con los requerimientos legales en esta materia.
- Subdirección General de Contratación
 - a) Asegura la incorporación de las cláusulas en materia de seguridad de la información en los contratos, acuerdos u otra documentación que la entidad establezca con terceros.
- Oficina TIC
 - a) Lidera, gestiona y hace seguimiento a la implementación del Sistema de Gestión de Seguridad de la Información (SGSI) al interior de la entidad.
 - b) Gestiona los requerimientos de seguridad informática establecidos para la operación, administración y comunicación de los sistemas y recursos tecnológicos de la entidad.
 - c) Gestiona el mantenimiento y disponibilidad de la plataforma tecnológica (hardware, software y comunicaciones), con el cumplimiento de las medidas de seguridad establecidas en la entidad.
 - d) Gestiona y controla los sistemas de protección de la información necesarios para controlar los riesgos en un nivel que permita su adecuado manejo y seguimiento.
 - e) Gestiona, actualiza y socializa periódicamente los lineamientos de seguridad de la información, los procedimientos y formatos de aplicación de los mismos al interior de la entidad.
 - f) La ALFM ha autorizado frente a la Emergencia Sanitaria por COVID -19 el mecanismo de "TRABAJO EN CASA" y en cumplimiento a la regulación de la ley N° 2088 del 12 de mayo de 2021 mediante la cual se rige el Trabajo en Casa, la Oficina TIC pondrá al servicio de los funcionarios las



07

herramientas y brindará la capacidad de conexiones de acceso remoto a través de VPN, para la habilitación de trabajo en casa previa autorización del Jefe y Coordinador inmediato de cada funcionario; soportará técnicamente a la ALFM mediante la plataforma tecnológica en la Entidad, sobre la cuales se crearán usuarios con acceso externo vía plataformas directas y/o VPN (red privada virtual sobre software de seguridad perimetral), contemplando 3 tipos de conexiones o accesos externos:

- **VPN Tipo1:** Acceso a aplicativos específicos como Orfeo, Suite visión, entre otros.
 - **VPN Tipo2:** Acceso Total al equipo del usuario. Este acceso normalmente aplica para Directivos y con el cumplimiento de los criterios establecidos en “Instrucciones Generales de Coordinación” de esta Directiva.
 - **Acceso sin VPN:** Acceso a aplicativos para ser operados desde un sitio externo (Zimbra, SAP, SISCOM, etc.).
- g) Las VPN serán creadas y soportadas en las plataformas de seguridad perimetral que la ALFM ya posee (desde antes de la Emergencia Sanitaria por COVID-19) y por tanto no se debe requerir inversión adicional en TIC para afrontar esta época de crisis.
- h) Garantizará las capacitaciones e instructivos necesarios con el fin que NO se generen limitaciones en las conexiones remotas y/o desempeño de las funciones desde el Trabajo en Casa.
- i) Notificará mediante el caso registrado en la “mesa de ayuda”, la habilitación del servicio de VPN.
- j) Soportará técnicamente videoconferencias y reuniones virtuales que se programen en la Entidad.
- k) Aplica medidas Seguridad física a los dispositivos de la entidad como:
- Entrega usuarios de VPN para conectar a los funcionarios en trabajo remoto a la red interna de la Entidad, con el fin de evitar ataques, teniendo presente que, por la implementación de TRABAJO EN CASA, el tráfico de la red inicia a través de las redes públicas, desde los hogares de los funcionarios.
 - Seguirá aplicando el cierre de sesión cuando el usuario no esté usando la computadora en TRABAJO EN CASA.

07

- Seguirá aplicando los lineamientos de contraseña segura establecidos.
 - Continuará proporcionando herramientas colaborativas como videoconferencias, que permitan a los funcionarios comunicarse entre sí, efectuar reuniones y capacitaciones virtuales.
- l) Promoverá permanentemente estrategias de sensibilización en temas relacionados a seguridad digital, apropiación de buenas prácticas y comportamientos en entornos digitales, para prevenir la materialización de riesgos asociados a las tecnologías corporativas y en el hogar por la proliferación de ataques cibernéticos derivados de la emergencia sanitaria por COVID - 19, actividad que se realizará a través de boletines informativos y alertas de seguridad emitidos por correo electrónico institucional.
- Grupo de Marketing y Comunicaciones
 - a) Elabora los elementos audiovisuales necesarios para la sensibilización en temas de seguridad de la información al interior de la entidad, en coordinación con el profesional encargado de la Seguridad de la Información en la ALFM.

c. Instrucciones Generales de Coordinación

- ✓ Todo el personal es responsable cumplir los lineamientos en seguridad de la información que maneja en desarrollo de sus funciones en la Agencia Logística de las Fuerzas Militares, y de todos los recursos informáticos que se encuentren bajo su responsabilidad y operación.
- ✓ Todo el personal sin excepción alguna, deberá participar activamente de las actividades relacionadas con la prevención y mitigación de riesgos cibernéticos, en el marco de dar cumplimiento a la responsabilidad de todo el personal conocer y aplicar los lineamientos específicos contenidos en el Manual de "Políticas de Uso, Operación y Seguridad para las Tecnologías de la Información y las Comunicaciones", el cual se encuentra publicado en la Suite Visión Empresarial y es de obligatorio cumplimiento.
- ✓ El acceso VPN Tipo 2 (acceso al PC) es restringido únicamente para los Directivos y para casos muy excepcionales, en cuyo caso se deben cumplir los siguientes criterios:



02.03

- a. La habilitación de este tipo de conexión y acceso "VPN Tipo 2" se efectuará en los casos en que sea absolutamente necesario, por lo tanto, cada solicitud debe ser individual y contar con el aval respectivo del Jefe/Director de la Dependencia de la cual es orgánico el "funcionario solicitante". Cada Jefe/Director de la Dependencia debe sustentar a la Oficina TIC dicha necesidad y responde por lo que haga el subalterno a través de dicha conexión.
- b. Se deberá diligenciar el formato GTI-FO-04 "Solicitud Creación o Actualización de Usuarios", firmar (funcionario, Coordinador y jefe de la dependencia) y allegar la solicitud vía "caso" en la "mesa de ayuda".
- c. La Oficina TIC evaluará por cada funcionario, el cargo, el volumen y tipo de información, aplicativos y servicios tecnológicos que utiliza, y plasmará el resultado para justificar si se requiere acceso total al equipo.
- d. Se autorizarán estos accesos VPN Tipo 2, manejando lineamientos estrictos que permitan mitigar los riesgos potenciales para la ALFM, como lo es la posible afectación a la infraestructura por propagación de Malware, Virus, Ransomware (virus secuestrador de información), fuga y extracción no autorizada de información.
- e. Previa autorización y supervisión del propietario de la información (Jefe/Director de la Dependencia), se verificará de forma remota las condiciones de seguridad del equipo personal desde el que se va a hacer uso de este servicio, con el fin de constatar que cuente especialmente con un antivirus licenciado y actualizado que permita prevenir riesgos de infección por virus informáticos.
- f. Los funcionarios a quienes se les otorgue este acceso, responden por las actividades que se hagan con su usuario y en sus máquinas (de la Entidad y personal), reconfirmará la aceptación y cumplimiento de los lineamientos de Seguridad, entre las que se destaca, que el usuario y la contraseña asignado es "personal e intransferible".
- g. La Oficina TIC realizará monitoreo a la existencia de conexiones fuera de los horarios laborales establecidos (diferentes a: Lunes a Sábado de 6:30 a 19:00 horas) y se reportarán a cada Jefe/Director de dependencia para su seguimiento y control.

07

- h. Para los usuarios que se les habilite el acceso VPN Tipo 2, por criterios de seguridad y para mitigar riesgos, el sistema les solicitará cambio de contraseña con frecuencia de cada 15 días.
- i. La Oficina TIC generará reportes de tráfico mensual de los equipos y usuarios de los funcionarios VPN Tipo 2 y reportará a la Dirección General cualquier anomalía que al respecto sea detectada, para generar los seguimientos y correctivos del caso.
- ✓ Con ocasión de las medidas y acciones transitorias adoptadas por la ALFM debido a la emergencia sanitaria por COVID-19, todos los funcionarios quienes en ejercicio de sus funciones requieran manejar comunicaciones oficiales y requieran retirar documentos de manera temporal de las instalaciones de la ALFM, deberán dar estricto cumplimiento a las instrucciones emitidas mediante el relacionado acto administrativo No. 408 del 20 de abril de 2020.
- ✓ Afrontar las circunstancias actuales producto de la emergencia sanitaria por COVID-19, sin dejar de cumplir la misión institucional y los procesos de abastecimientos, pero a la vez evitando la exposición innecesaria de los funcionarios al virus y preservando los criterios de seguridad de la información y de la seguridad digital.
- ✓ Para el trámite de las **comunicaciones internas**, se debe tener en cuenta lo siguiente:
- Se utilizará la firma digital en PDF, evitando imprimir innecesariamente estos documentos al ser viables el trámite de forma digital y dando cumplimiento a la Estrategia de Cero Papel.
 - La documentación de carácter interno de la ALFM (excepto carácter legal) será firmada digitalmente a través del Acrobat.
 - Se tramitarán los memorandos por el Sistema de Información ORFEO, únicamente podrán imprimirse los documentos que tengan anexos originales tales como (Facturas, Contratos, Actas de liquidación, pagos, etc.).
- ✓ Para el trámite de las **comunicaciones oficiales externas**, se debe tener en cuenta lo siguiente:



- Todos los funcionarios de la ALFM deberán cumplir con los requisitos de seguridad de la entidad y con la Ley de Protección de Datos Personales.
 - La documentación firmada digitalmente en Acrobat será válida siempre y cuando se tramite a través del Sistema de Información Orfeo y/o por el correo institucional, donde se pueda evidenciar la trazabilidad y la participación de los usuarios firmantes del documento, para así soportar su legalidad al tramitarla fuera de la Entidad.
 - Remitir los oficios por los canales oficiales y/o correos electrónicos de las entidades externas, con el fin de no tener que imprimir la documentación a menos que sea estrictamente necesario.
 - Inmediatamente sea posible, incorporar en los respectivos expedientes, los documentos originados, recibidos, tramitados y firmados digitalmente durante la contingencia, donde cada productor de la información debe validar si es necesario imprimir y tomar firmas manuscritas. Los documentos se deben incluir en los expedientes de acuerdo con su clasificación en la Tabla de Retención Documental de cada dependencia, actualizando la lista de chequeo y diligenciando el Formato Único de Inventario Documental- FUID.
 - Los Subdirectores, Directores y Jefes de Oficina, deben garantizar el valor probatorio de los Oficios (Externos) firmados digitalmente y surgidos de sus respectivas dependencias.
- ✓ Es responsabilidad de todo el personal (funcionario o externo) dar cumplimiento a las siguientes recomendaciones de Seguridad Digital, para mitigar los riesgos en las funciones de Trabajo en Casa:
- Mantener actualizado el sistema operativo de su equipo personal.
 - Realizar cambio periódico de claves de acceso a las redes WIFI de su hogar.
 - No instalar aplicaciones de exijan permisos de acceso a su computadora personal.
 - Instalar y mantener actualizado el software antivirus de su computadora personal.

- 07
- ✓ Ningún funcionario está autorizado a enviar información de la ALFM por medios NO Oficiales (WhatsApp, Gogle Drive, etc.).
 - ✓ Todos los funcionarios de la ALFM, deberán cumplir con los requisitos de seguridad de la entidad y la ley de protección de datos personales; acorde a lo que estipula la Ley 1581 de 2012 en Colombia, la cual contempla todo el manejo de la información de una persona (Permite a los ciudadanos conocer, actualizar y rectificar toda la información que tengan las diferentes entidades y bases de datos del país) y el Decreto 1377 de 2013 que reglamenta parcialmente la Ley 1581 de 2012, mediante el cual se decretan unas disposiciones generales sobre el tratamiento de datos en el ámbito personal, que comprende aquellas actividades que se inscriben en el marco de la vida privada o familiar, las autorizaciones y el consentimiento que se obtiene a la entidad al momento de recolectar los datos que los usuarios y todo lo que dicta la ley en materia de políticas de tratamiento, ejercicio de los derechos de los titulares, transferencias y transmisiones internacionales de datos personales y responsabilidad demostrada frente al tratamiento de datos personales.
 - ✓ Durante el período de aislamiento preventivo obligatorio de acuerdo con lo establecido mediante Decreto 491 del 28 marzo de 2020, se autoriza que cuando no se cuenten con firma manuscrita, podrán adoptar firma digital a través Acrobat DC. Cada funcionario, sus coordinadores y Directores o Jefes, serán responsables de adoptar las medidas necesarias para garantizar la seguridad de los documentos que se firmen por este medio.
 - ✓ Se dispone del uso de las herramientas tecnológicas para comunicarse, el trabajo colaborativo y telepresencial mediante videoconferencias, para lo cual los funcionarios deberán aplicar y respetar los lineamientos de seguridad establecidos en el "Manual de Políticas de Uso, Operación y Seguridad para las Tecnologías de la Información y las Comunicaciones".

4. DISPOSICIONES ADMINISTRATIVAS

El incumplimiento de las disposiciones señaladas en este documento estará sujeto a las respectivas investigaciones y sanciones disciplinarias que amerite.

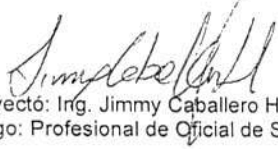
07

FIRMADO.




Coronel JUAN CARLOS RIVEROS PINEDA
Secretario General


Encargado de las funciones del Director General de la Agencia Logística de las Fuerzas Militares




Proyectó: Irg. Jimmy Caballero Herrera
Cargo: Profesional de Oficial de Seguridad




Revisó: Ing. Yuri Daianny Ruiz
Cargo: Coordinadora de Informática



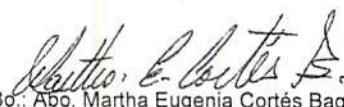
Revisó: Ing. César Adolfo González
Cargo: Coordinador redes e Infraest.



Aprobó: Cr. (RA) Sonia Dolly Gutiérrez
Cargo: Jefe Oficina de TICs



Vo. Bo.: Rommel Daniel Gutiérrez Gómez
Cargo: Jefe Oficina de Planeación e Innovación Institucional



Vo.Bo.: Abo. Martha Eugenia Cortés Baquero
Cargo: Jefe Oficina Asesora Jurídica



Vo.Bo.: Adm. Emp. Sandra Liliana Vargas
Cargo: Directora Administrativa y de Talento Humano

DISTRIBUCIÓN:

Original: Dirección General



Copias Digitales:

Copia 1:	Secretaría General
Copia 2:	Oficina de Control Interno
Copia 3:	Oficina de Control Interno Disciplinario
Copia 4:	Oficina de Planeación e Innovación Institucional
Copia 5:	Oficina de TICs
Copia 6:	Oficina Jurídica
Copia 7:	Subdirección General Abastecimientos y Servicios
Copia 8:	Subdirección General Contratación
Copia 9:	Subdirección General Operación Logística
Copia 10:	Dirección Administrativa y Talento Humano
Copia 11:	Dirección Financiera
Copia 12:	Dirección Abastecimientos Clase I
Copia 13:	Dirección Otros Abastecimientos y Servicios
Copia 14:	Dirección Infraestructura
Copia 15:	Dirección Producción
Copia 16:	Regional Amazonía
Copia 17:	Regional Antioquia-Chocó
Copia 18:	Regional Caribe
Copia 19:	Regional Centro
Copia 20:	Regional Llanos Orientales
Copia 21:	Regional Nororiente
Copia 22:	Regional Norte
Copia 23:	Regional Pacífico
Copia 24:	Regional Sur
Copia 25:	Regional Suroccidente
Copia 26:	Regional Tolima Grande