AGENCIA LOGÍSTICA
FUERZAS MILITARES
La unión de nuestras Fuerzas

MANUAL POLÍTICAS SEGURIDAD DE LA INFORMACIÓN

ELABORÓ	FECHA	REVISÓ	FECHA	REVISÓ	FECHA
	29 09 2022		05 10 2022		05 10 2022
NOMBRE Deiby Leandro Alvarado Rodríguez		**NOMBRE** Daris Yaneth Padilla Díaz		**NOMBRE** Roberto Velásquez Arango	
CARGO Profesional Seguridad de la Información		**CARGO** Profesional Defensa – Grupo Informática		**CARGO** Coordinador Grupo Informática	
FIRMA		**FIRMA**		**FIRMA**	
REVISÓ	**FECHA**	**REVISÓ**	**FECHA**	**APROBÓ**	**FECHA**
	05 10 2022		05 10 2022		12 10 2022
NOMBRE César Adolfo González Peña		**NOMBRE** CR (RA) Sonia Dolly Gutiérrez Carrillo		**NOMBRE** CR. Carlos Augusto Mórales Hernández	
CARGO Coordinador Grupo de Redes e Infraestructura Tecnológica		**CARGO** Jefe Oficina Gestión TIC		**CARGO** Director General ALFM	
FIRMA		**FIRMA**		**FIRMA**	

TABLA DE CONTENIDO

1. INTRODUCCIÓN

La Agencia Logística de las Fuerzas Militares en adelante (ALFM) determina la información como un activo de alta importancia para la entidad que permite el desarrollo continuo con la misión y el cumplimiento del objetivo de la misma, lo cual genera la necesidad de implementar reglas y medidas que permitan proteger la confidencialidad, integridad y disponibilidad en todo el ciclo de vida de la información.

En el presente manual se establecen los lineamientos que integran el Sistema de Gestión de Seguridad de la Información – SGSI, los cuales deben ser adoptadas por los funcionarios, contratistas y terceros que presten sus servicios o tengan algún tipo de relación con la ALFM; estas se encuentran enfocadas al cumplimiento de la normatividad legal vigente y a las buenas prácticas de seguridad de la información, basadas en la NTC/ISO 27001:2013 y al Modelo de Seguridad y Privacidad de la Información – MSPI, del Ministerio de Tecnologías de la Información y las Comunicaciones - MinTIC.

La Seguridad de la Información es para la ALFM, una labor prioritaria que exhorta a todos a velar por el cumplimiento de las políticas establecidas en el presente manual.

2. OBJETIVOS DEL MANUAL

2.1. OBJETIVO GENERAL

Establecer los lineamientos y políticas que permitan proteger, asegurar y salvaguardar la confidencialidad, integridad y disponibilidad de los activos de información de la ALFM, teniendo en cuenta los procesos, la operación, objetivos de negocio y la normatividad legal vigente para la entidad.

2.2. OBJETIVOS ESPECÍFICOS

Identificar e implementar mecanismos para lograr el cumplimiento de la normatividad en materia de seguridad de la información, estableciendo, operando, manteniendo y dirigiendo de manera estandarizada, sistemática y organizada un sistema efectivo que permita el tratamiento seguro de la información en la entidad.

Desarrollar las actividades necesarias para garantizar la continuidad y disponibilidad de los sistemas de información de la ALFM.

Promover y mejorar la cultura de seguridad de la información en los funcionarios, contratistas y terceros de la ALFM, a través de la capacitación y sensibilización en el Sistema de Gestión de Seguridad de la Información (SGSI).

Realizar una adecuada gestión de riesgos de seguridad de la información implementando controles que contribuyan a mitigar su probabilidad de materialización.

Implementar mecanismos que fomenten la transparencia en el acceso a la información, mediante procesos de clasificación y control de acceso a la información.

Fortalecer y mantener los niveles de confianza de las personas en los procedimientos y servicios de seguridad de la información que presta la ALFM.

Velar por la protección y debido uso de los activos de información establecidos en la entidad para el cumplimiento de los objetivos institucionales (Herramientas tecnológicas)

Gestionar de manera adecuada los incidentes de seguridad de la información, generando, documentando y aplicando lecciones aprendidas con el fin de minimizar la posibilidad de ocurrencia y/o el impacto de incidentes futuros.

Mejorar continuamente el desempeño del SGSI, mediante la implementación de acciones correctivas y de mejora que se generen como resultado de las auditorías internas, externas y de las revisiones de seguridad de la información.

3. ALCANCE

La política de seguridad de la información aplica y es de obligatorio cumplimiento a todos los procesos, funcionarios, contratistas y terceros relacionados con la ALFM, que permiten el cumplimiento a los propósitos institucionales.

4. REFERENCIA NORMATIVA

Ley 527 (agosto 18) 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”.

Ley 594 (julio 14) de 2000 “Por la cual se dicta la Ley General de Archivos y se dictan otras disposiciones”.

Ley 599 (julio 14) de 2001 “Código Penal Colombiano”.

Ley 1952 (enero 28) de 2019 “Por medio de la cual se expide el código general disciplinario y deroga la ley 734 de 2002 y algunas disposiciones de la ley 1474 de 2011, relacionadas con el derecho disciplinario.

Ley 1221 (julio 16) de 2008 “Por la cual se establecen normas para promover y regular el Teletrabajo y se dictan otras disposiciones”.

Ley 1266 (diciembre 31) de 2008 “Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones”.

Ley 1273 (enero 05) de 2009 “Por medio del cual se modifica el código penal, se crea un nuevo bien jurídico tutelado-Denominado "De la protección de la información y de los datos" y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones”.

Ley 1581 (octubre 17) de 2012 “Disposiciones Generales para tratamiento de datos personales”.

Ley 1712 (marzo 06) de 2014 “Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública”.

Ley 1978 (julio 25) de 2019 “Por la cual se moderniza el sector de las tecnologías de la información y las comunicaciones – TIC, se distribuyen competencias, se crea un regulador único y se dictan otras disposiciones”.

NTC-ISO/IEC 27001 de 2013 “Tecnologías de la Información. Técnicas de Seguridad. Sistemas de Gestión de la Seguridad de la Información. Requisitos.”

Decreto 2364 (noviembre 22) de 2012 “Por medio del cual se reglamenta el artículo 7° de la Ley 527 de 1999, sobre la firma electrónica y se dictan otras disposiciones”.

Decreto 1377 (junio 27) de 2013 “Por el cual se reglamenta parcialmente la ley 1581 de 2012”.

Decreto 1078 (mayo 26) de 2015 “Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones”.

Decreto 728 (mayo 05) de 2017 “Por el cual se adiciona el capítulo 2 al título 9 de la parte 2 del libro 2 del decreto único reglamentario del sector tic, decreto 1078 de 2015, para fortalecer el modelo de Gobierno Digital en las entidades del orden nacional del estado colombiano, a través de la implementación de zonas de acceso público a internet inalámbrico”.

Decreto 1413 (agosto 25) de 2017 “Por el cual se adiciona el título 17 a la parte 2 del libro 2 del Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones, Decreto 1078 de 2015, para reglamentarse parcialmente el capítulo IV del título 111 de la Ley 1437 de 2011 y el artículo 45 de la Ley 1753 de 2015, estableciendo lineamientos generales en el uso y operación de los servicios ciudadanos digitales”.

Decreto 612 (abril 04) 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 (junio 14) de 2018 “Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones”.

Decreto 620 (mayo 02) de 2020 “Por el cual se subroga el título 17 de la parte 2 del libro 2 del decreto 1078 de 2015, para reglamentarse parcialmente los artículos 53, 54, 60, 61 y 64 de la ley 1437 de 2011, los literales e, j y literal a del parágrafo 2 del artículo 45 de la ley 1753 de 2015, el numeral 3 del artículo 147 de la ley 1955 de 2019, y el artículo 9 del decreto 2106 de 2019, estableciendo los lineamientos generales en el uso y operación de los servicios ciudadanos digitales.”

Decreto 45 (enero 15) de 2021 “Por el cual se derogan el decreto 704 de 2018 y el artículo 1.1.2.3. del decreto número 1078 de 2015, único reglamentario del sector de tecnologías de la información y las comunicaciones”.
Decreto 377 (abril 09) de 2021 “Por el cual se subroga el título 1 de la parte 2 del libro 2 del decreto 1078 de 2015, decreto único reglamentario del sector de tecnologías de la información y las comunicaciones, para reglamentar el registro único de tic y se dictan otras disposiciones”.

Decreto 934 (agosto 18) de 2021 “Por el cual se adiciona el capítulo 7 al título 2 de la parte 2 del libro 2 del decreto 1078 de 2015, decreto único reglamentario del sector de tecnologías de la información y las comunicaciones, para reglamentarse el parágrafo 2 del artículo 11 de la ley 1341 de 2009”.

Decreto 88 (enero 24) de 2022 “Por el cual se adiciona el título 20 a la parte 2 del libro 2 del decreto único reglamentario del sector de tecnologías de la información y las comunicaciones, decreto 1078 de 2015, para reglamentar los artículos 3, 5 y 6 de la ley 2052 de 2020, estableciendo los conceptos, lineamientos, plazos y condiciones para la digitalización y automatización de trámites y su realización en línea”.

Decreto 338 (marzo 08) de 2022 “Por el cual se adiciona el título 21 a la parte 2 del libro 2 del decreto único 1078 de 2015, reglamentario del sector de tecnologías de la información y las comunicaciones, con el fin de establecer los lineamientos generales para fortalecer la gobernanza de la seguridad digital, se crea el modelo y las instancias de gobernanza de seguridad digital y se dictan otras disposiciones”.

Decreto 767 (mayo 16) de 2022 “Por la cual se establecen los lineamientos generales de la Política de Gobierno Digital y se subroga el Capítulo 1 del Título 9 de la Parte 2 del Libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones”.

Decreto 1227 (junio 18) de 2022 “Por el cual se modifican los artículos 2.2.1.5.3, 2.2.1.5.5, 2.2.1.5.8 y 2.2.1.5.9 y se adicionan los artículos 2.2.1.5.15 al 2.2.1.5.25 al Decreto 1072 de 2015, único reglamentario del sector trabajo, relacionados con el teletrabajo.”

Decreto 1263 (julio 22) de 2022 “Por el cual se adiciona el titulo 22 a la parte 2 del libro 2 del Decreto 1078 de 2015, decreto único reglamentario del sector de tecnologías de la información y las comunicaciones, con el fin de definir lineamientos y estándares aplicables a la transformación digital pública.”

CONPES 3701 (julio 14) de 2011 “Lineamientos de política para ciberseguridad y ciberdefensa”.

CONPES 3854 (abril 11) de 2016 “Política Nacional de Seguridad Digital”.

CONPES 3920 (abril 17) de 2018 “Política nacional de explotación de datos (BIG DATA)”.

CONPES 3995 (julio 01) de 2020 “Nacional de confianza y seguridad Digital”.

Resolución 1519 (agosto 24) de 2020 “Por la cual se definen los estándares y directrices para publicar la información señalada en la ley 1712 del 2014 y se definen los requisitos materia de acceso a la información pública, accesibilidad web, seguridad digital, y datos abiertos”.

Resolución 413 (marzo 01) de 2021 “Por la cual define el uso de las tecnologías en la nube para el sector defensa y se dictan otras disposiciones”.

Resolución 500 (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.”

Resolución 0463 (febrero 09) de 2022 “Por el cual se define el uso de Tecnologías en la Nube para el Sector Defensa y se dictan otras disposiciones”.

Resolución 000460 (febrero 15) de 2022 “Por la cual se expide el plan nacional de infraestructura de datos y su hoja de ruta en el desarrollo de la política de gobierno digital, y se dictan los lineamientos generales para su implementación”.

Resolución 000746 (marzo 11) de 2022 “Por el cual se fortalece el modelo de seguridad y privacidad de la información y se definen lineamientos adicionales a los establecidos en la resolución no. 500 de 2021”.

Manual de Gobierno Digital (diciembre versión. 06) de 2018 “En este documento se desarrolla el proceso de implementación de la Política de Gobierno Digital a través de los siguientes cuatro (4) momentos: 1. Conocer la política; 2. Planear la política; 3. Ejecutar la política; y 4. Medir la política; cada uno de ellos incorpora las acciones que permitirán desarrollar la Política en las entidades públicas de nivel nacional y territorial”.

Manual integrado de gestión (septiembre 27) de 2019 “Manual integrado de gestión, código: GI-MA-02, versión No. 20”.

Directiva Permanente Ministerio Defensa No. 913 (abril 19) de 2013 “Guías y procedimientos en tecnología de información y comunicaciones para el Sector Defensa”.

Directiva Permanente Ministerio de Defensa No. 018 (junio 19) de 2014 “Políticas de seguridad de la información para el Sector Defensa”.

Directiva Presidencial No. 03 (marzo 15) de 2021 “Lineamientos para el uso de servicios en la nube, inteligencia artificial, seguridad digital y gestión de datos”.

Directiva Presidencial No. 02 (febrero 24) de 2022 “Por medio del cual se efectúa reiteración de la política pública en materia de seguridad digital”.

5. DEFINICIONES

ACTIVO: Se refiere a cualquier información o elemento relacionado con el tratamiento de esta (información, software, recurso humano, servicio, hardware, otro) que tiene un valor para la entidad.

ACTIVO CRITICO: Información, software, recurso humano, servicio, hardware u otro, los cuales, si son destruidos, su funcionamiento es degradado o que por cualquier otro motivo no se encuentra disponibles, pueden afectar el cumplimiento de la misionalidad de la ALFM.

ACTIVO DE INFORMACIÓN: Es el elemento de información que la ALFM recibe o produce en el ejercicio de sus funciones. Incluye la información que se encuentre presente en forma impresa, escrita, en papel, trasmitida por cualquier medio electrónico o almacenado en equipos de cómputo, incluyendo software, hardware, recurso humano, datos contenidos en registros, archivos, bases de datos, videos e imágenes.

ADMINISTRACIÓN DE RIESGOS: Se entiende por la administración de riesgos, el proceso de identificación, control, minimización o eliminación, a un costo aceptable, de los riesgos de seguridad que podrían afectar la información o impactar de manera considerable la operación. Dicho proceso es cíclico y deberá llevarse a cabo de forma periódica.

ALFM: Agencia Logística de las Fuerzas Militares.

AMENAZA: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la entidad en general.

ÁREAS SEGURAS: Son aquellas en donde se encuentran sistemas de procesamiento y almacenamiento de algún activo de información; en la ALFM se identifican las siguientes áreas seguras: Data Center, Archivos generales y de gestión, lugares que contengan información clasificada como Reservada (Oficinas de la entidad).

CIBERSEGURIDAD: Es el proceso de proteger los activos de información por medio del tratamiento de las amenazas de la información que es procesada, almacenada y/o transportada a través de sistemas de información interconectados.

CLASIFICACIÓN DE LA INFORMACIÓN: Es el ejercicio por medio del cual se determina que la información pertenece a uno de los niveles de clasificación estipulados en la entidad. Tiene como objetivo asegurar que la información recibe el nivel de protección adecuado.

COLCERT: Por las siglas en inglés de Computer Emergency Response Team, es el Grupo de Respuesta a Emergencias Cibernéticas de Colombia, y tiene como responsabilidad central la coordinación de la Ciberseguridad y Ciberdefensa Nacional, la cual estará enmarcada dentro del Proceso Misional de Gestión de la Seguridad y Defensa del Ministerio de Defensa Nacional. Su propósito principal será la coordinación de las acciones necesarias para la protección de la infraestructura crítica del Estado colombiano frente a emergencias de Ciberseguridad que atenten o comprometan la seguridad y defensa nacional.

CONFIDENCIALIDAD: Entendida como la garantía del acceso a la información únicamente de los usuarios autorizados.

CONTROL: Medios para manejar el riesgo; incluyendo políticas, procedimientos, lineamientos, prácticas o estructuras organizacionales, las cuales pueden ser administrativas, técnicas, de gestión o de naturaleza legal.

CSIRT: Por las siglas en inglés de Computer Security Incident Response Team, es el equipo de Respuesta a Incidentes de Seguridad Informática de la Policía Nacional CSIRT-PONAL, creado para atender las necesidades de prevención, atención e investigación de los eventos e incidentes de seguridad informática, con el fin de proteger la infraestructura tecnológica, los activos de información y mitigar el impacto ocasionado por la materialización de los riesgos asociados con el uso de las tecnologías de la información y las telecomunicaciones

CUSTODIO: Es una parte designada de la entidad, un cargo, proceso, o grupo de trabajo encargado de administrar y hacer efectivos los controles de seguridad que el propietario de la información haya definido, tales como copias de seguridad, asignación privilegios de acceso, modificación y borrado.

DATA CENTER: Es el lugar donde se ubican los recursos de comunicaciones de Tecnologías de la Información, como Switch, patch, panel, UPS, Router, cableado de voz y de datos.

DATO PERSONAL: Es cualquier pieza de información vinculada a una o varias personas determinadas o determinables o que puedan asociarse con una persona natural o jurídica. Los datos impersonales (referencia que no se aplica o se refiere a ninguna persona en concreto.) no se sujetan al régimen de protección de datos de la presente ley. Cuando en la presente ley se haga referencia a un dato, se presume

que se trata de uso personal. Los datos personales pueden ser públicos, semiprivados o privados **(Ley 1266 de 2008 - artículo 3, literal e).**

DATO PÚBLICO: Es el dato calificado como tal según los mandatos de la ley o de la Constitución Política y todos aquellos que no sean semiprivados o privados, de conformidad con la presente ley. Son públicos, entre otros, los datos contenidos en documentos públicos, sentencias judiciales debidamente ejecutoriadas que no estén sometidos a reserva y los relativos al estado civil de las personas **(Ley 1266 de 2008 - artículo 3, literal f).**

DATO PRIVADO: Es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular (Únicamente puede accederse a ellos por orden de autoridad judicial competente y en ejercicio de sus funciones.) **(Ley 1266 de 2008 - artículo 3, literal h).**

DATO SEMIPRIVADO: Es semiprivado el dato que no tiene naturaleza íntima, reservada, ni pública y cuyo conocimiento o divulgación puede interesar no sólo a su titular sino a cierto sector o grupo de personas o a la sociedad en general, como el dato financiero y crediticio de actividad comercial o de servicios **(Ley 1266 de 2008 - artículo 3, literal g).**

DATO SENSIBLE: Es el dato que afecta la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición así como los datos relativos a la salud, a la vida sexual y los datos biométricos **(Ley 1581 de 2012 - artículo 5°).**

DISPONIBILIDAD: Entendida como la garantía del acceso a la información en el instante en que el usuario la necesita.

DOCUMENTO EN CONSTRUCCIÓN: No será considerada información pública aquella información preliminar y no definitiva, propia del proceso deliberatorio (discusión o reflexión sobre un asunto - documento) de un sujeto obligado en su calidad de tal. **(Es importante tener en cuenta este concepto que aplica respecto de todos los activos cuando se estén en construcción) (Ley 1712 de 2014 - artículo 6, literal k).**

INCIDENTE DE SEGURIDAD: Evento o serie de eventos de seguridad de la información no deseados o inesperados, que tienen probabilidad significativa comprometer las operaciones del negocio y amenazar la seguridad de la información.

INFORMACIÓN: Datos relacionados que tienen significado para la entidad. La información es un activo que, como otros activos importantes del negocio, es esencial para las actividades de la entidad y, en consecuencia, necesita una protección adecuada.

La información dada por la Ley 1712 de 2014, se refiere a un conjunto organizado de datos contenido en cualquier documento que los sujetos obligados generen, obtengan, adquieran, transformen o controlen.

INFORMACIÓN PÚBLICA: Es toda la información que un sujeto obligado genere, obtenga, adquiera, con controle en su calidad de tal.

INFORMACIÓN PÚBLICA CLASIFICADA: Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado de manera motivada y por escrito, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados. **(Ley 1712 de 2014 - Artículo 18).**

INFORMACIÓN PÚBLICA RESERVADA: Es aquella información "que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada, de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados **(Ley 1712 de 2014).**

IDENTIFICACIÓN DE ACTIVOS DE INFORMACIÓN: Es un código para ordenar y localizar los activos de información dentro de la Agencia.

INTEGRIDAD: Entendida como la preservación de la información de forma completa y exacta.

PROPIETARIO DE LA INFORMACIÓN: Es un área designada de la entidad, un cargo, proceso, o grupo de trabajo que tiene la responsabilidad de garantizar que la información y los activos asociados con los servicios de procesamiento de información se clasifican adecuadamente, y de definir y revisar periódicamente las restricciones y clasificaciones del acceso, teniendo en cuenta las políticas aplicables sobre el control del acceso.

RIESGO: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información.

SISTEMA DE INFORMACIÓN: Se refiere a un conjunto independiente de recursos de información organizados para la recopilación, procesamiento, mantenimiento, transmisión y difusión de información según determinados procedimientos, tanto automatizados como manuales. Conjunto de aplicaciones que interactúan entre sí para apoyar un área o proceso de la ALFM.

USUARIO: Cualquier persona que genere, obtenga, transforme, conserve o utilice información de la Agencia en papel o en medio digital, físicamente o a través de las redes de datos y los sistemas de información de la ALFM. Son las personas que utilizan la información para propósitos propios de su labor y que tendrán el derecho manifiesto de uso dentro del inventario de información.

VPN: Red virtual privada por sus siglas en ingles Virtual Private Network.

6. PRINCIPIOS DE SEGURIDAD

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

Las 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 y terceros.

La ALFM protegerá la información generada, procesada o resguardada por los procesos de negocio, su infraestructura tecnológica y activos (de información) del riesgo que se genera de los accesos otorgados a terceros, o como resultado de un servicio interno en outsourcing.

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 parte de los funcionarios y/o personal 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 control 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 activos de información.

La ALFM garantizará a través de una adecuada gestión de los eventos de seguridad y las debilidades asociadas con los activos 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 los diferentes eventos.

La ALFM garantizará el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas.

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.

7. POLÍTICAS DE LA SEGURIDAD DE LA INFORMACIÓN – *(Dominio 5).*

7.1. DIRECTRICES ESTABLECIDAS POR LA DIRECCIÓN PARA LA SEGURIDAD DE LA INFORMACIÓN – *(Categoría 5.1).*

Objetivo: Brindar orientación y apoyo por parte de la ALFM, para la seguridad de los activos de información de acuerdo con los lineamientos establecidos por la normatividad vigente mediante el presente manual.

7.1.1. Políticas para la seguridad de la información – *(Control 5.1.1).*

La ALFM en cumplimiento al compromiso del SGSI, crea un esquema de seguridad de la información, definiendo y estableciendo roles y responsabilidades que involucren las actividades de operación, gestión y administración de la seguridad de la información, así como la existencia de funciones relacionadas al Comité Institucional de Gestión y Desempeño (absorbe el comité del SGSI).

La Oficina TIC debe establecer los roles y responsabilidades de operación y administración de los sistemas de información de la ALFM; a los funcionarios, contratistas y terceros relacionados con la entidad, los cuales deberán estar debidamente documentados.

La Oficina TIC debe establecer un plan de capacitación interno que permita el fomento continúo de la creación de cultura y conciencia de seguridad en los funcionarios, contratistas y terceros relacionados con la ALFM.

Todos los funcionarios, contratistas y terceros relacionados con la ALFM, tienen la responsabilidad y obligación de cumplir con las políticas, normas, procedimientos y buenas prácticas de seguridad de la información establecidas en el presente manual y los demás lineamientos establecidos por la entidad.

Los Directores, Subdirectores y Jefes de Oficina de la ALFM deben asegurarse de que todos los procedimientos de seguridad de la información dentro de su área de responsabilidad se ejecuten correctamente para lograr el cumplimiento de las políticas y estándares de seguridad de la información de la entidad.

7.1.2. Revisión de las políticas para la seguridad de la información – *(Control 5.1.2).*

Las políticas establecidas en el presente manual serán revisadas y/o actualizadas por lo menos una vez al año o si ocurren cambios significativos, asegurando la conveniencia, adecuación y mejoramiento continuo.

8. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN – *(Dominio 6).*

8.1. ORGANIZACIÓN INTERNA – *(Categoría 6.1).*

Objetivo: Establecer un marco de referencia de gestión para el inicio y control de la implementación y operación de la seguridad de la información en la ALFM.

8.1.1. Roles y responsabilidades para la seguridad de la información – *(Control 6.1.1).*

La ALFM en cumplimiento al compromiso del Sistema de Gestión de Seguridad de la Información – SGSI, cuenta con un esquema de seguridad de la información definiendo y estableciendo roles y responsabilidades que involucren las actividades de operación, gestión y administración de la seguridad de la información, el cual se encuentra estructurado de forma transversal para el cumplimiento obligatorio de todos los funcionarios, contratistas y terceros relacionados con la entidad; estos roles y responsabilidades se encuentran descritos en la **Documentación General Matriz de Roles y Responsabilidades Sistema de Gestión de la Seguridad de la Información – SGSI – GTI-DG-02.**

8.1.2. Separación de deberes – *(Control 6.1.2).*

Todos los funcionarios, contratistas o terceros que tengan acceso a la información de la ALFM, deben tener claramente definidos sus deberes frente a la gestión de la Seguridad de la Información, con el fin de minimizar el uso no autorizado, indebido o accidental de los activos de información.

El acceso a la información de la ALFM, es otorgado solo a usuarios que se encuentren previamente autorizados por la Oficina TIC con el consentimiento de cada uno de los jefes de área o dependencias, teniendo en cuenta lo requerido para la realización de sus labores relacionadas con su responsabilidad o tipo de servicio con los privilegios requeridos.

La Oficina TIC debe recepcionar el **Formato Solicitud Creación o Actualización de Usuarios - GTI-FO-04,** frente a la creación de usuarios en todos los sistemas de información de la entidad garantizando los controles de acceso, de tal forma que haya segregación de funciones entre quien administre, opere, mantenga, audite y en general, tenga la posibilidad de acceder a los sistemas de información, así como quien otorga el privilegio y quien lo utiliza.

8.1.3. Contacto con las autoridades – *(Control 6.1.3).*

La Oficina TIC deberá mantener contacto con las autoridades nacionales en materia de seguridad de la información con el fin de intercambiar experiencias y obtener asesoramiento para el mejoramiento de las prácticas y controles de seguridad, por lo tanto, se debe mantener contacto con las siguientes entidades especializadas en temas relativos a la seguridad de la información.

A. Ministerio de las Tecnologías de la Información y las Comunicaciones – MinTIC.

B. Grupo de respuesta a emergencias cibernéticas de Colombia – ColCERT

C. Equipo de respuesta a Incidentes de Seguridad Informática Colombia – CSIRT Gobierno

8.1.4. Seguridad de la información en la gestión de proyectos – *(Control 6.1.5).*

La seguridad de la información se debe integrar a la gestión de proyectos de la ALFM, para asegurar que los riesgos de seguridad de la información se identifiquen y traten como parte del proyecto. Esto debe aplicar a cualquier proyecto, independientemente de su naturaleza. Por lo tanto, es responsabilidad de los lideres de proyectos, de los dueños de proceso, de los funcionarios y contratistas de la entidad, asegurar que se sigan las siguientes directrices:

A. Todos los proyectos que se desarrollen en el marco del cumplimiento de los objetivos de los Procesos de la ALFM, deberán tener un componente de seguridad en la información, el cual debe ser acompañado y asesorado por la Subdirección General de Contratación, la Oficina Asesora de Planeación e Innovación institucional (Direccionamiento estratégico) y la Oficina TIC, de acuerdo a la especificidad técnica, teniendo en cuenta las obligaciones que están estipuladas en el **Manual de contratación - CT-MA-01**.

B. Los objetivos del proyecto no deben ir en contravía de la Política de seguridad de la información, por lo tanto, los objetivos establecidos en el presente manual deben ser incluidos en el proyecto.

C. Realizar valoración de los riesgos de seguridad de la información en la fase de estudios previos del proyecto, para identificar los controles necesarios.

D. Hacer seguimiento a los riesgos y controles aplicados, tratándolos durante todas las fases del proyecto.

E. Se debe diligenciar el **Formato Acuerdo de confidencialidad y no divulgación contratistas - GTI-FO-01,** a todos los contratistas o terceros que participen en un proceso de contratación, donde se suministre información perteneciente a la entidad, protegiendo de este modo la Confidencialidad, integridad y disponibilidad de la información.

8.2. DISPOSITIVOS MÓVILES Y TELETRABAJO – *(Categoría 6.2).*

Objetivo: Definir los lineamientos para el uso, administración, consulta y operación de los servicios en los dispositivos móviles de la ALFM y a su vez controlar el acceso a los mismos, en las instalaciones de la entidad y en las áreas de teletrabajo.

8.2.1. Política para dispositivos móviles – *(Control 6.2.1).*

Los dispositivos móviles institucionales (teléfonos móviles, teléfonos inteligentes (Smartphone), portátiles, entre otros), son una herramienta de trabajo que se deben utilizar únicamente para facilitar las comunicaciones de los usuarios de la entidad.

Los usuarios de dispositivos móviles institucionales deben tener instaladas únicamente las aplicaciones distribuidas, autorizadas y configuradas por la administración de la entidad.

Los funcionarios no están autorizados a cambiar la configuración, a desinstalar software, formatear o restaurar de fábrica los equipos móviles institucionales asignados, únicamente se deben aceptar y aplicar las actualizaciones.

Los dispositivos móviles institucionales deben tener únicamente la tarjeta SIM asignada por la entidad, de igual forma, la tarjeta SIM únicamente debe instalarse en los equipos asignados.

Los dispositivos móviles deben contar con una contraseña de ingreso segura, también deben tener configurado el bloqueo de manera automática y manual.

Ante el daño, pérdida o hurto del equipo, el funcionario deberá informar de manera inmediata a la Oficina TIC y a la Dirección Administrativa, para continuar con el procedimiento administrativo que dé lugar.

Los teléfonos móviles y/o teléfonos inteligentes institucionales, debe permanecer encendidos y cargados durante las horas laborales o de acuerdo con la responsabilidad y requerimientos propios del cargo.

Es responsabilidad del funcionario hacer buen uso del dispositivo suministrado por la ALFM con el fin de realizar actividades propias de su cargo o funciones asignadas en la entidad y así mismo salvaguardar la información de la entidad.

Los funcionarios de dispositivos móviles institucionales deben mantener desactivados las funciones de redes inalámbricas Wifi, puertos infrarrojos, puerto Bluetooth, previniendo de este modo la fuga de la información.

Los funcionarios que tengan asignados dispositivos móviles institucionales NO deben hacer uso de redes inalámbricas públicas.

En caso de requerirse instalación de aplicaciones adicionales en el dispositivo móvil institucional, debe ser solicitado y autorizado por la Oficina TIC.

8.2.2. Teletrabajo – *(Control 6.2.2).*

La Oficina TIC en caso de requerirse pondrá al servicio de los funcionarios las herramientas y brindará la capacidad de conexiones de acceso remoto a través de VPN, para la habilitación de Teletrabajo en modalidad “Trabajo en casa”, sobre las cuales se crearán usuarios con acceso externo vía VPN (red privada virtual sobre software de seguridad perimetral), contemplando dos (02) tipos de conexiones o accesos externos:

A. VPN Tipo 1: Acceso a aplicativos específicos como ORFEO, Suite Visión, entre otros.

B. VPN Tipo 2: Acceso total al equipo del funcionario. Este acceso normalmente aplica para Directivos y administradores de plataformas informáticas (Oficina TIC), con el cumplimiento de los criterios establecidos en el presente manual.

La habilitación de este tipo de conexión y acceso “VPN” se efectuará en los casos en que sea absolutamente necesario, por lo tanto, cada solicitud debe ser individual.

Se autorizarán estos accesos “VPN”, 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.

La solicitud deberá realizarse y gestionarse mediante caso en la “mesa de ayuda”, anexando el **Formato Solicitud de Excepciones de Seguridad Informática - GTI-FO-05,** debidamente diligenciado, en donde se incluirá justificación acorde y clara a la solicitud, el cual deberá firmarse por los Directores, Subdirectores y Jefes de Oficina y el funcionario a quien se le habilitará el servicio solicitado.

La solicitud del documento será validada por la Oficina TIC de acuerdo con el requerimiento, con el Director General y/o la Secretaría General y/o el Grupo SST y/o la Dirección Administrativa, para la respectiva aprobación de este.

La Oficina TIC creará y soportará las VPN gestionadas, mediante las plataformas de seguridad perimetral con las que cuenta la ALFM.

La Oficina TIC garantizará las capacitaciones e instrucciones necesarias, frente al manejo y uso de las conexiones VPN, con el fin de que NO se generen limitaciones en el desempeño de sus funciones.

La Oficina TIC aplicará medidas de seguridad física a los dispositivos de la entidad como:

A. Generación, entrega, monitoreo y cierre 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 el tráfico de la red inicia a través de las redes públicas.

B. Se aplicará el cierre de sesión por inactividad en la conexión VPN.

C. Aplicación de los lineamientos de contraseña segura establecidos.

9. SEGURIDAD DE LOS RECURSOS HUMANOS – *(Dominio 7).*

9.1. ANTES DE ASUMIR EL EMPLEO – *(Categoría 7.1).*

Objetivo: Asegurar que los funcionarios y contratistas comprenden sus responsabilidades y son idóneos en los roles paras los cuales serán contratados.

9.1.1. Selección – *(Control 7.1.1).*

La Dirección Administrativa y talento Humano debe contar con un procedimiento de selección de personal que se encuentre ajustado con las leyes y reglamentos de ética pertinentes, el cual debe incluir:

A. Verificación de referencias
B. Verificación de la hoja de vida completa
C. Verificación de la identidad del aspirante
D. Verificación de competencia
E. Pruebas psicotécnicas
F. Verificar en términos generales que sea una persona confiable para desempeñar el rol a contratar, especialmente si es un cargo crítico para la ALFM

La Dirección Administrativa y talento Humano deberá definir los mecanismos de autorización para el tratamiento de los datos personales de los funcionarios y contratistas de acuerdo con lo establecido en la Ley 1581 de 2012 “Por la cual se dictan disposiciones generales para la protección de datos personales.” y sus decretos reglamentarios.

La Dirección Administrativa y talento Humano deberá aplicar los lineamientos y políticas establecidos en el **Manual para la Publicación de Vacantes Postulación, Reclutamiento, Selección y Vinculación de Personal - GTH-MA-04.**

Por intermedio de la Dirección Administrativa y talento Humano, se debe realizar un estudio de seguridad detallado a los candidatos, aspirantes y contratistas, de acuerdo a lo estipulado en el **Formato Estudio de Seguridad Personal** y generar el concepto de confidencialidad.

La Dirección Administrativa y talento Humano debe notificar las novedades de vinculación a la Oficina TIC mediante el mecanismo definido y así mismo realizar una adecuada gestión de acceso físico por parte de los funcionarios nuevos a la ALFM.

Los Directores, Subdirectores y Jefes de Oficina deben enviar novedades de vinculación de funcionarios o contratistas a través de la “mesa de ayuda” a la Oficina TIC, con el fin que se

realice una adecuada gestión de acceso a los servicios TIC (gestión de usuarios) previo diligenciamiento del **Formato Solicitud Creación o Actualización de Usuarios - GTI-FO-04.**

9.1.2. Términos y condiciones de empleo – *(Control 7.1.2).*

La Dirección Administrativa y talento Humano deberá aplicar el **Formato acuerdo de Confidencialidad Servidores Públicos - GTH-FO-119**, a todos los funcionarios que sean contratados o presten sus servicios de manera directa, teniendo en cuenta que accederán a los activos de información con los que cuenta la ALFM.

La Subdirección General de Contratación deberá aplicar el **Formato acuerdo de confidencialidad y no divulgación contratistas - GTI-FO-01,** a todos los contratistas que accedan a prestar sus servicios a la entidad, luego de llevar a cabo el proceso de contratación.

Sera responsabilidad de los funcionarios y contratistas velar por los activos de información asignados para la ejecución de sus funciones, en razón a que mediante la clasificación de estos empiezan a ejercer la función de custodios.

La Subdirección General de Contratación y la Dirección Administrativa y talento Humano, deberán asegurar que los funcionarios y contratistas acepten los términos y condiciones relativos a la seguridad de la información, referente a la naturaleza y al alcance del acceso que tendrán a los activos de la información de la entidad.

Los funcionarios y terceros que tienen cuenta de usuario para el acceso a los sistemas de información, pueden realizar el cambio de su fotografía en las plataformas que lo permitan, de tal forma que al realizar la inclusión y/o cambio de fotografía, al ser considerado un dato sensible, “una foto contiene la imagen de una persona, lo que corresponde a un dato biométrico”, el titular está dando su aprobación, en cuanto al tratamiento de sus datos personales de acuerdo a la ley 1581 de 2012.

9.2. DURANTE LA EJECUCIÓN DEL EMPLEO – *(Categoría 7.2).*

Objetivo: Asegurar que los funcionarios y contratistas asuman y cumplan sus responsabilidades frente a la seguridad de la información de la ALFM

9.2.1. Responsabilidades de la Dirección – *(Control 7.2.1).*

La Alta Dirección en apoyo de la Oficina TIC, deberán exigir la aplicación de la seguridad de la información a todos los funcionarios y contratistas que laboren en la ALFM, de acuerdo con las políticas y lineamientos establecidos por la entidad.

Los Directores, Subdirectores y Jefes de Oficina deben asegurarse de que los funcionarios y contratistas conozcan las responsabilidades para la clasificación de la información y la gestión de activos institucionales asociados con información, instalaciones de procesamiento de información y servicios de información que deben ser manejados por el funcionario o contratista.

Los Directores, Subdirectores y Jefes de Oficina debe informar los roles y responsabilidades que tienen los funcionarios y contratistas relacionados con la seguridad de la información, antes de brindar los accesos a los activos de la información.

Los Directores, Subdirectores y Jefes de Oficina, velarán por que los funcionarios y contratistas participen de manera activa en las sensibilizaciones dadas por la Oficina TIC con relación a temas de seguridad de la información.

Los Directores, Subdirectores y Jefes de Oficina velarán porque los funcionarios y contratistas den cumplimiento a los ítems establecidos en los acuerdos de confidencialidad y no divulgación.

La Dirección Administrativa - talento Humano y la Subdirección General de Contratación deben asegurar que los funcionarios y contratistas respectivamente conozcan y acepten la Política de seguridad de la información, para esto deben informar a la Oficina TIC, para que les indique las medidas a seguir para la consulta y aplicación de esta política.

La Dirección Administrativa y talento Humano deben comunicar a la Oficina TIC, los cambios de cargo de personal, indicando los cambios en los recursos tecnológicos asignados; especialmente actualizaciones sobre accesos a carpetas compartidas y sistemas de información.

9.2.2. Toma de conciencia, educación y formación en la seguridad de la información – *(Control 7.2.2).*

Incluir en los programas de Inducción y de reinducción el tema seguridad de la información asegurando que los funcionarios conozcan sus responsabilidades, así como las implicaciones por el uso indebido de activos de información y recursos informáticos, haciendo énfasis en las consecuencias jurídicas que puede acarrear como servidor público.

Los Directores, Subdirectores y Jefes de Oficina, establecerán los mecanismos para asegurar que los funcionarios asistan a las charlas de sensibilización y capacitación en seguridad de la información brindadas por la Oficina TIC.

Todos los funcionarios y contratistas deben recibir información y procedimientos pertinentes para su cargo; durante el proceso de vinculación, inducción o cuando dichas políticas sean actualizadas y/o modificadas con el fin de mantener la concientización sobre la importancia de la seguridad de la información.

La Oficina TIC debe mantener un programa anual de concientización y capacitación para todos los funcionarios, así como para los contratistas y terceros que interactúen con la información institucional y desarrollen actividades en la entidad.

La concientización de seguridad implica el conocimiento, por parte de todo el personal que accede a información de la ALFM, de las obligaciones básicas y del deber de reserva que adquieren, derivadas del acceso a este tipo de información, así como de las responsabilidades penales y disciplinarias que son aplicables en caso de incumplimiento.

9.2.3. Proceso Disciplinario – *(Control 7.2.3).*

Dentro de la estrategia de seguridad de la información de la ALFM, está establecido un Procedimiento Gestión de Talento Humano - Investigaciones Administrativas para los funcionarios que hayan cometido alguna violación de la Política de Seguridad de la Información. El proceso disciplinario también ayuda como medida disuasiva para evitar que los funcionarios, contratistas y terceros de la entidad violen las políticas y los procedimientos de seguridad de la

información, así como para cualquier otra violación de la seguridad. Las investigaciones disciplinarias corresponden a actividades pertenecientes a la Oficina de Control Interno Disciplinario de la ALFM, de acuerdo a los procedimientos establecidos para tal fin.

Actuaciones que conllevan a la violación de la seguridad de la información establecida en la ALFM:

A. No firmar los acuerdos de confidencialidad y no divulgación, documentos de entrega de información o de activos de información.
B. Ingresar a carpetas de otros procesos o áreas, sin autorización, con intención de consultar, manipular, borrar o adulterar la información.
C. No reportar los incidentes de seguridad o las violaciones a las políticas de seguridad, cuando se tenga conocimiento de ello.
D. No guardar de forma segura la información cuando se ausenta de su puesto de trabajo o al terminar la jornada laboral, documentos impresos que contengan información pública reservada o clasificada.
E. No guardar la información digital, producto del procesamiento de la información perteneciente a su proceso en las carpetas oficiales o bajo una protección restringida.
F. Dejar los computadores encendidos en horas no laborables, sin la debida autorización para ello.
G. Permitir que personas ajenas a la ALFM, deambulen sin acompañamiento, al interior de las instalaciones, en áreas no destinadas al público.
H. Almacenar en dispositivos extraíbles personales la información de la entidad, sin la debida autorización.
I. Solicitar cambio de contraseña de otro usuario, sin la debida autorización del titular o su jefe inmediato.
J. Hacer uso de la red de datos para obtener, mantener o difundir en los equipos de sistemas, material pornográfico (penalizado por la ley) u ofensivo, cadenas de correos y correos masivos no autorizados.
K. Utilización de software no relacionado con la actividad laboral y que pueda degradar el desempeño de la plataforma tecnológica institucional.
L. Recibir o enviar información institucional a través de correos electrónicos personales, diferentes a los asignados por la institución.
M. Utilizar equipos electrónicos o tecnológicos desatendidos o que, a través de sistemas de interconexión inalámbrica, sirvan para transmitir, recibir y almacenar datos.
N. Usar dispositivos de almacenamiento externo en los computadores, cuya autorización no haya sido otorgada por la Oficina TIC.
O. Negligencia en el cuidado de los equipos, dispositivos portátiles o móviles entregados para actividades propias de la entidad.
P. No cumplir con las actividades designadas para la protección de los activos de información de la entidad.
Q. El que impida u obstaculice el funcionamiento o el acceso normal al sistema informático, los datos informáticos o las redes de telecomunicaciones de la ALFM, sin estar autorizado.
R. El que destruya, dañe, borre, deteriore o suprima datos informáticos o un sistema de tratamiento de información de la ALFM
S. El que distribuya, envíe, introduzca software malicioso u otros programas de computación de efectos dañinos en la plataforma tecnológica de la ALFM

T. El que superando las medidas de seguridad informática suplante un usuario ante los sistemas de autenticación y autorización establecidos por la ALFM
U. No mantener la confidencialidad de las contraseñas de acceso a la red de datos, los recursos tecnológicos o los sistemas de información de la entidad o permitir que otras personas accedan con el usuario y clave del titular a estos.
V. Permitir el acceso u otorgar privilegios de acceso a las redes de datos de la ALFM a personas no autorizadas.
W. Llevar a cabo actividades fraudulentas, ilegales o intentar acceso no autorizado a cualquier recurso tecnológico de la ALFM.
X. Retirar de las instalaciones de la entidad, estaciones de trabajo o computadores portátiles que contengan información institucional sin la autorización pertinente.
Y. Sustraer de las instalaciones de la ALFM, documentos con información institucional calificada como información pública reservada o clasificada, o abandonarlos en lugares públicos o de fácil acceso.
Z. Entregar, enseñar y divulgar información institucional, calificada como información pública reservada y clasificada a personas o entidades no autorizadas.
AA. No realizar el borrado seguro de la información en equipos o dispositivos de almacenamiento de la ALFM, para traslado, reasignación o para disposición final.
BB. Utilizar los activos de la ALFM para ejecutar cualquier acción que pretenda difamar, abusar, afectar la reputación o presentar una mala imagen de la ALFM o de alguno de sus funcionarios.
CC. Realizar cambios no autorizados en la plataforma tecnológica de la ALFM.
DD. Instalar programas o software no autorizados en las estaciones de trabajo o equipos portátiles institucionales, cuyo uso no esté autorizado por la Oficina TIC.
EE. Copiar sin autorización los programas de la ALFM, violar los derechos de autor o acuerdos de licenciamiento.

9.3. TERMINACIÓN O CAMBIO DE EMPLEO – *(Categoría 7.3).*

Objetivo: Establecer lineamientos para las responsabilidades y deberes de seguridad de la información que permanezcan validos después de la terminación de contratos o cambio de empleo.

9.3.1. Terminación o cambio de responsabilidades de empleo – *(Control 7.3.1).*

Los Directores, Subdirectores y Jefes de Oficina o a quienes se deleguen deberán recoger y custodiar la información de la ALFM en el caso de retiro, investigación, inhabilidades o cambio de funciones.

El supervisor del contrato o a quien se delegue deberá recoger y custodiar la información de la ALFM bajo la responsabilidad de los contratistas en caso de terminación anticipada, definitiva, temporal o cesión del contrato.

La Dirección Administrativa - talento Humano y la Subdirección General de Contratación o a quienes se deleguen deberán informar a la Oficina TIC, mediante caso generado en la plataforma de mesa de ayuda o vía correo electrónico, la desvinculación administrativa, laboral o contractual del funcionario o contratista; una vez notificada la novedad se deberá proceder a la inactivación de accesos a las plataformas tecnológicas, teniendo en cuenta los siguientes parámetros:

A. Si el buzón pertenece a una cuenta de correo genérica (ejemplo: seguridadti@agencialogistica.gov.co), a este se le deberá cambiar la contraseña inmediatamente y asignar un nuevo responsable para evitar accesos no autorizados.
B. En caso de que el buzón de correo electrónico sea objeto de investigación por parte de las autoridades competentes se les entregara en cadena de custodia una copia del buzón garantizando su integridad; se deben inactivar los accesos biométricos de los sistemas de control de acceso.
C. Emitir comunicado a los proveedores y demás personal con el que el funcionario o contratista tenga contacto, indicándole que esa persona ya no labora en la ALFM e indicando quien asumirá sus funciones o responsabilidades.
D. Adicionalmente en proceso de desvinculación se deberá tener en cuenta los siguientes parámetros:

1) Para el buzón de correo electrónico se creará una copia de respaldo una vez se dé por terminada la vinculación con la ALFM.
2) Bajo ningún parámetro se podrán restablecer los accesos a estas cuentas; solo se podrán restablecer buzones en ambientes offline y no se podrán emitir correos ni notificaciones desde estos buzones de correo electrónico.
3) Se deben inactivar todos los accesos a los sistemas de información.
4) Se debe solicitar la devolución del carnet o cualquier otro distintivo de autenticación o prenda de vestir, que lo acredite como funcionario de la ALFM.

Los Directores, Subdirectores y Jefes de Oficina deben asegurar que el retiro los funcionarios y contratistas se realice de una manera ordenada, por lo cual deberá supervisar la entrega de los equipos asignados y el retiro de los accesos a sistemas de información, se cumplan correctamente; previo diligenciamiento del **Formato Paz y Salvo por Retiro de la Institución** - **GTH-FO-61**; las responsabilidades y los deberes de seguridad de la información permanecerán validos después de la terminación o cambio de empleo por lo que se deben definir, comunicar al empleado o contratista y se deben hacer cumplir.

10. GESTIÓN DE ACTIVOS – *(Dominio 8).*

10.1. RESPONSABILIDAD POR LOS ACTIVOS – *(Categoría 8.1).*

Objetivo: Identificar los activos organizacionales y definir las responsabilidades de protección apropiadas.

10.1.1. Inventario de activos – *(Control 8.1.1).*

Se deben identificar los activos de información, sus respectivos propietarios, custodios y su ubicación, a fin de elaborar y mantener un inventario actualizado mínimo cada año, de acuerdo a la **Guía para la gestión y clasificación de activos de información - GTI-GU-02,** mediante formato Registro de Activos de Información alineado con la Ley 1712 de 2014 Ley de Transparencia.

Cada proceso de la ALFM debe ser responsable de mantener actualizado el inventario de activos de información con el acompañamiento de la Oficina TIC, de acuerdo con las directrices establecidas para la gestión de activos.

La entidad implementa las directrices para lograr y mantener la protección adecuada y uso de los activos de información mediante la asignación a los usuarios finales que deban administrarlos de acuerdo a sus roles y funciones.

10.1.2. Propiedad de los activos – *(Control 8.1.2).*

Cada proceso de la ALFM tiene la custodia sobre todo activo generado y procesado, contenido por sus sistemas de cómputo, así como también de todo aquel trasmitido a través de su red de telecomunicaciones o cualquier otro medio de comunicación físico o electrónico y se reserva el derecho de conceder el acceso a la información.

La ALFM es la propietaria de los activos de información y los administradores de estos activos (custodios) son los funcionarios y contratistas que estén autorizados y sean responsables por la información de los procesos a su cargo, de los sistemas de información o aplicaciones informáticas, hardware o infraestructura Tecnológica (TIC).

La Entidad debe realizar el tratamiento de información documental de acuerdo a lo establecido en el **Manual de gestión documental - GA-MA-03.**

Una parte de los activos de TIC, se debe mantener en una base de datos bajo la responsabilidad de la Oficina TIC. (CMDB - Base de datos de gestión de configuraciones / Configuration Management Database).

10.1.3. Uso aceptable de los activos – *(Control 8.1.3).*

El empleó de los activos de información debe ser exclusivamente con propósitos laborales, los usuarios (todo aquel que se le otorgue un nombre de usuario y una clave de acceso) deberán utilizar únicamente los programas y equipos autorizados por la Oficina TIC.

Los recursos informáticos de la ALFM no podrán ser utilizados, salvo previa autorización escrita, para divulgar, propagar o almacenar contenido personal o comercial de publicidad, promociones, ofertas, programas informáticos, propaganda, material religioso o cualquier otro uso que no esté autorizado.

Los funcionarios no deben realizar intencionalmente actos que impliquen un mal uso de los recursos tecnológicos o que vayan en contravía de las políticas de seguridad de la información, entre ellos, envíos o reenvíos masivos de correos electrónicos o spam, práctica de juegos en línea, uso de redes sociales personales, conexión de periféricos o equipos no autorizados que atenten contra la seguridad de la información y ambientes de trabajo seguros, etc.

La instalación de cualquier tipo de software en los equipos de cómputo de la ALFM, es responsabilidad exclusiva de la Oficina TIC o los agentes de Soporte para Regionales, son ellos los únicos autorizados para realizar esta labor.

Los funcionarios no podrán efectuar ninguna de las siguientes labores sin previa autorización de la Oficina TIC:

A. Bajar, descargar e instalar software de Internet u otro servicio en línea en cualquier estación de trabajo o servidor de la ALFM.

B. Modificar, revisar, transformar o adaptar cualquier software propiedad de la ALFM.
C. Descompilar o realizar ingeniería inversa en cualquier software de propiedad de la ALFM.
D. Copiar o distribuir cualquier software de propiedad de la ALFM.
E. Cambiar la configuración de hardware de propiedad de la ALFM.

Ningún activo informático adquirido y que sea configurable, debe ser instalado con la configuración por defecto del fabricante o proveedor, incluyendo cuentas y claves de administrador; se debe realizar la configuración adecuada de seguridad a través de la Oficina TIC.

Los funcionarios a través del correo electrónico deberán informar a la Oficina TIC de cualquier violación de las políticas de seguridad, uso indebido y debilidades de seguridad de la información de la ALFM.

Los funcionarios serán responsables de todas las transacciones o acciones efectuadas con su "cuenta de usuario", así mismo ningún funcionario deberá acceder a la red o servicios TIC de la ALFM, utilizando una cuenta de usuario o clave de otro funcionario.

Los funcionarios salvo autorización expresa no podrán hacer uso de redes externas a través de dispositivos institucionales de la ALFM (modem USB, Router, wifi público, internet compartido de dispositivos móviles etc.); esto compromete la seguridad de los recursos informáticos de la ALFM.

La información de la ALFM debe ser respaldada de forma frecuente, debe ser almacenada en lugares apropiados en los cuales se pueda garantizar que la información está segura y podrá ser recuperada en caso de un desastre o de incidentes con los equipos de procesamiento.

Está prohibido que personal ajeno a los delegados por la Oficina TIC (agentes de soporte), destapen o retiren partes de los equipos de cómputo propiedad de la ALFM.

Los funcionarios o contratistas no deben realizar cambios en las estaciones de trabajo relacionados con la configuración de equipo, tales como conexiones de red, usuarios locales de la máquina, papel tapiz y protector de pantalla no definido. Estos cambios deben ser realizados únicamente por la Oficina TIC o el personal autorizado.

Los funcionarios o contratistas de los activos informáticos no deben realizar cambios físicos en las estaciones de trabajo, tales como: Cambio de ubicación, mantenimientos, repotenciación, modificaciones en su configuración física. Estas actividades solo podrán ser efectuadas por la Oficina TIC o el personal autorizado.

Toda actividad informática no autorizada (escaneos de seguridad, ataques de autenticación o de negación del servicio, entre otros) que afecte tanto las redes corporativas como los sistemas de información de la ALFM, están prohibidas dando lugar a los procesos disciplinarios y/o legales correspondientes.

Todas las estaciones de trabajo deben apagarse o hibernarse al término de la jornada laboral, exceptuando a los funcionarios que por cumplimiento de sus funciones se haga necesario que la estación de trabajo permanezca activa.

Los equipos de cómputo, servidores, teléfonos IP y equipos de comunicaciones, deben conectarse a los puntos de corriente eléctrica identificados como regulados, con el fin de evitar que por picos altos de energía se pueda dañar el componente tecnológico. Estos puntos de corriente regulada están soportados por las UPS en dado caso de cortes de energía, de tal forma que no se apague abruptamente el dispositivo, entre tanto entra en operación de la planta eléctrica.

10.1.4. Devolución de activos – *(Control 8.1.4).*

Los funcionarios o contratistas deberán realizar la devolución de todos los activos de información asignados por la ALFM en el proceso de desvinculación o cambio de función, de igual manera deberán documentar y entregar a la entidad los conocimientos importantes que posee de la labor que ejecutan, mediante el **Formato Acta Entrega Oficina y/o Cargo - GA-FO-27.**

10.2. CLASIFICACIÓN DE LA INFORMACIÓN – *(Categoría 8.2).*

Objetivo: Asegurar que la información recibe un nivel apropiado de protección, acorde a su importancia en la ALFM.

10.2.1. Clasificación de la información – *(Control 8.2.1).*

Los responsables de la información deben realizar la clasificación y control de activos de información con apoyo de la Oficina TIC; con el objetivo de garantizar que reciban un nivel apropiado de protección, clasificación de la información e identificación de su sensibilidad, criticidad, definiendo los niveles de protección y medidas de tratamiento conforme a lo estipulado en la **Guía para la gestión y clasificación de activos de información - GTI-GU-02.**

La ALFM aplica los criterios contenidos en la Ley 1712 de 2014 “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.” Artículos 6 y 19; en consecuencia, la información que deba gozar de reserva será denominada como “Documentación Pública Reservada”.

La clasificación debe realizarse evaluando las características en las cuales se basa la seguridad de la información: Confidencialidad, Integridad y Disponibilidad.

La clasificación de los activos debe revisarse mínimo cada año y ajustarse en caso de requerirse, cuando sea identificado algún riesgo o cuando haya cambios en la estructura del proceso.

10.2.2. Etiquetado de la información – *(Control 8.2.2).*

El procedimiento para el etiquetado de la información será aplicado de acuerdo a lo estipulado en la **Guía para la gestión y clasificación de activos de información - GTI-GU-02,** siendo este el documento rector que imparte los lineamientos para la debida gestión.

10.2.3. Manejo de activos – *(Control 8.2.3).*

Se aplicará la **Guía para la gestión y clasificación de activos de información - GTI-GU-02,** para el manejo de activos de conformidad con el esquema de clasificación de la información aprobado por la ALFM.

10.3. MANEJO DE MEDIOS – *(Categoría 8.3).*

Objetivo: Prevenir la divulgación, la modificación, el retiro o la destrucción de información almacenada en medios de soporte.

10.3.1. Gestión de medios removibles – *(Control 8.3.1).*

Se encuentra restringida la conexión a la infraestructura tecnológica (servidores, computadores, scanner y demás equipos de tecnologías de la información) de la ALFM de cualquier almacenamiento como dispositivos personales USB, discos duros externos, CDs, DVDs, cámaras fotográficas, cámaras de video, teléfonos celulares, smartphone, tabletas, módems, memorias SD o de almacenamiento, entre otros dispositivos no institucionales. Las excepciones especiales serán autorizadas por la Oficina TIC previo diligenciamiento del **Formato Solicitud de Excepciones de Seguridad Informática - GTI-FO-05.**

Los medios de almacenamiento removibles como cintas, discos duros, CDs, DVDs, dispositivos USB, entre otros, así como los medios impresos que contengan información institucional, deben ser controlados y físicamente protegidos mediante algún mecanismo (cifrado, resguardo en gavetas de seguridad, cajas fuertes, control de accesos, etc.), que garantice su integridad y confidencialidad.

Los Directores, Subdirectores y Jefes de Oficina definirán los medios removibles de almacenamiento que podrán ser utilizados por las personas autorizadas en los sistemas de información y en la plataforma tecnológica, en caso de ser requerido para el cumplimiento de sus funciones mediante el **Formato Solicitud de Excepciones de Seguridad Informática - GTI-FO-05.**

La Oficina TIC debe proveer el uso de carpetas compartidas minimizando el uso de medios removibles, con el propósito de que el intercambio de información al interior de la entidad sea controlado y seguro.

Los medios removibles utilizados al interior de la entidad no deben ser utilizados en sitios públicos, así mismo, debe tratarse bajo cuidado alejado de daños externos como agua, polvo o fuego.

10.3.2. Disposición de los medios – *(Control 8.3.2).*

En la ALFM se debe disponer (reintegrar) en forma segura de los medios cuando ya no se requieran, empleando procedimientos formales y el uso del **Formato Traslado de Bienes - GA-FO-04.**

Los medios que contienen información confidencial de acuerdo a su nivel de criticidad, identificados en la matriz de activos de información de la ALFM, se deben disponer de forma

segura, mediante incineración, destrucción o el borrado de datos antes de ser reutilizados o dados de baja.

Cuando el funcionario o contratista responsable de un activo de información finalice su vinculación con la ALFM, los equipos de cómputo asignados, deberán ser reintegrados mediante el **Formato Traslado de Bienes - GA-FO-04,** a la respectiva dependencia o al almacén general.

Los equipos de contratistas que hayan sido autorizados para acceder a las instalaciones de la entidad, al finalizar el contrato o labores para las cuales estaban definidos, se les efectuará una revista de sanitización que incluirá entre otras tareas el borrado seguro de la información a través de la verificación realizada a los equipos. La Oficina TIC, emitirá constancia (informe de supervisión) del proceso realizado al momento del retiro del equipo de las instalaciones físicas correspondientes.

La información contenida en la generación de Backup debe estar protegida en un lugar seguro y bajo llave, de acuerdo a disposición de la Oficina TIC.

Se debe guardar varias copias de datos valiosos para la ALFM en medios separados, con el fin de evitar la pérdida de información por daño o robo de los medios removibles.

Las copias de Backups se deben guardar en una ubicación alterna a la localización de los datos o aplicaciones, para aumentar la seguridad ante posibles impactos de desastres naturales, accidentes, incendios, entre otros.

Se debe realizar pruebas periódicas a las copias de datos para validar la integridad de la información.

10.3.3. Transferencia de medios físicos – *(Control 8.3.3).*

Los medios que contienen información se deberán proteger contra accesos no autorizados, uso indebido o alteración durante su transporte.

Para la transferencia de medios físicos (Transferencias Documentales), se deberá tener en cuenta el **Plan de transferencias documentales - GA-DG-04** y sus documentos relacionados.

El embalaje de la información debe ser apropiado que mitigue los daños físicos que se puedan presentar en el transporte de la misma, protegiendo la exposición al calor, humedad o campos electromagnéticos.

Se debe llevar un registro que identifique el contenido de los medios, la protección aplicada, al igual que los tiempos de transferencia a los responsables durante el transporte, y el recibido en su destino de acuerdo a lo estipulado en el **Procedimiento Gestión Administrativa - Control de Registros - GA-PR-01.**

11. CONTROL DE ACCESO – *(Dominio 9).*

11.1. REQUISITOS DEL NEGOCIO PARA CONTROL DE ACCESO – *(Categoría 9.1).*

Objetivo: Limitar el acceso no autorizado a la información y/o a las instalaciones de procesamiento de información de la ALFM.

11.1.1. Política de control de acceso – *(Control 9.1.1).*

La entidad define las reglas para asegurar un acceso controlado, físico o lógico, a la información y plataforma informática de la ALFM, considerándolas como importantes para el SGSI.

El control de acceso a la Información se realiza aplicando el principio de mínimo privilegio necesario autorizado para la realización de las actividades asignadas.

El acceso a la información se realiza de acuerdo con los niveles de calificación de la información y perfil asignado al usuario.

Los funcionarios o contratistas que tengan bajo su responsabilidad la custodia de la información física almacenada en los archivadores que se encuentra en las oficinas, deben mantener el control de acceso a esta información; por lo tanto, debe estar bajo llave. Se recomienda que las llaves se guarden en un sitio seguro, bajo la custodia de las personas que la dependencia estime conveniente.

La Oficina TIC suministrará a los funcionarios los usuarios y claves respectivas para el acceso a los servicios de red y sistemas de información a los que hayan sido autorizados, los usuarios y claves son de uso personal e intransferible. Es responsabilidad del usuario el manejo apropiado de los usuarios y claves que se le asignen, previo diligenciamiento del **Formato Solicitud Creación o Actualización de Usuarios - GTI-FO-04.**

La Oficina TIC debe suministrar a los usuarios una autenticación secreta temporal segura, que se obligue a cambiar, al usarla por primera vez.

El acceso a los activos de información institucionales estará permitido únicamente a los usuarios autorizados por el propietario de cada activo, de acuerdo a lo estipulado en la **Guía para la gestión y clasificación de activos de información - GTI-GU-02.**

Los administradores de red de la Oficina TIC, deben identificar y eliminar o deshabilitar periódicamente las identificaciones de usuarios redundantes, con el fin de que no sean asignados a otros usuarios.

La Oficina TIC debe realizar la parametrización para proteger los sistemas de información contra intentos de ingreso mediante fuerza bruta.

La Oficina TIC debe parametrizar los sistemas de información, restringiendo los tiempos de conexión con el fin de brindar seguridad adicional en aplicaciones de alto riesgo y para reducir la ventana de oportunidad para acceso no autorizado.

Está prohibido el acceso no autorizado a los códigos fuentes de los programas y elementos asociados como (diseños, especificaciones, librerías de fuentes de programas, planes de verificación y planes de validación), y sobre todo de aquellas aplicaciones, que están protegidas por derechos de autor.

La conexión remota a la red de área local de la ALFM debe ser realizada, a través, de una conexión VPN segura suministrada por la entidad, la cual debe ser aprobada, registrada y auditada por la Oficina TIC, previo diligenciamiento y autorización del **Formato Solicitud de Excepciones de Seguridad Informática - GTI-FO-05.**

El Data Center 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 Data Center es un área restringida y por lo tanto solo se puede ingresar a ella con autorización del jefe de la Oficina TIC o de los funcionarios designados por esa Jefatura a través de las Coordinaciones.
B. La operación de cualquiera de los dispositivos que se encuentren en el Data Center, solo podrá realizarse por los funcionarios autorizados por la Jefatura de la Oficina TIC.

Las personas que ingresen al Data Center, deberán seguir las normas de seguridad que para el efecto se dispongan desde la Oficina TIC, tales como:

A. Diligenciar previamente el **Formato Planilla de Control de Acceso Data Center** - **GTI-FO-10**, 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.
B. No ingresar ningún tipo de bebidas o alimentos.
C. No accionar ninguno de los dispositivos de alarmas sin razón ni autorización.
D. No encender objetos que puedan ocasionar que las alarmas y sistemas de seguridad se activen tales como: cigarrillos, fósforos, encendedores, etc.
E. No conectar equipos de soldadura, aspiradora, brilladora u otro electrodoméstico o herramienta industrial.
F. No operar ninguno de los diferentes equipos que en él se encuentran instalados sin autorización del jefe de la Oficina TIC o de alguno de los profesionales autorizados de la misma área.
G. Se debe brindar acompañamiento permanente de un funcionario de la ALFM al personal externo cuando realice procesos de mantenimiento y diligenciar el **Formato Planilla de Control de Acceso Data Center** - **GTI-FO-10**, establecido para tal fin.

11.1.2. Acceso a redes y a servicios en red – *(Control 9.1.2).*

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.

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 TIC, caso en el cual se deberá remitir la solicitud en el **Formato Solicitud de Excepciones de Seguridad Informática - GTI-FO-05.**

La Oficina TIC 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.

El servicio de Internet no debe ser utilizado para:

A. 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.
B. 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.
C. Descargar, instalar o ejecutar archivos o software no autorizado por la Oficina TIC y que comprometa la seguridad y el normal funcionamiento de los equipos, servicios y plataformas de la Entidad.
D. 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.
E. Utilizar los recursos de la ALFM para ganar acceso no autorizado a redes y sistemas remotos a través de puertas traseras de sistemas (backdoor).
F. 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.
G. 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 por los canales de comunicación institucional.
H. 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.
I. Violar o intentar violar los sistemas de seguridad de los equipos a los cuales se tenga acceso, tanto a nivel local como externo.
J. 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.
K. Violar o intentar violar los sistemas de seguridad para realizar labores propias de los administradores de la plataforma tecnológica.
L. 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 como 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.

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.

La Oficina TIC 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:

A. 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).
B. 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.
C. 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, CGR, entre otros.) 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.
D. Perfil de navegación Tecnología: Perfil configurado con características de navegación similar al perfil Medio, pero orientado para el personal de la Oficina de TIC 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.

La Oficina TIC 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 o el uso indebido del servicio, con el fin de que se inicien las acciones disciplinarias a que haya lugar.

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.

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

Cualquier instalación de software, utilitarios, antivirus, etc., previamente deben ser probados en entornos controlados y debidamente autorizados por la Oficina TIC.

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 TIC.

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 TIC.

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, YouTube, Instagram 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.

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.

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.

Los usuarios de las redes inalámbricas deben ser sometidos a las mismas condiciones de seguridad y reserva de las redes cableadas, en lo que respecta a identificación, autenticación, control de contenido de internet y cifrado, entre otros.

11.2. GESTIÓN DE ACCESO A USUARIOS – *(Categoría 9.2).*

Objetivo: Asegurar el acceso a los usuarios autorizados y evitar el acceso no autorizado a sistemas y servicios.

11.2.1. Registro y cancelación del registro de usuarios – *(Control 9.2.1).*

El registro de usuarios se realiza aplicando el principio de mínimo privilegio necesario autorizado para la realización de las actividades asignadas. Estos privilegios deben revisarse a intervalos regulares y ser modificados o reasignados, cuando se presenten cambios en el perfil del usuario, ya sea por promociones, ascensos, traslados, cambios de cargo o terminación de la relación laboral, de acuerdo a lo estipulado en el **Procedimiento Gestión de TICs - Gestión Mesa de Ayuda Tecnológica - GTI-PR-02.**

La Dirección Administrativa y de Talento Humano debe informar inmediatamente a la Oficina TIC, 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 TIC para la suspensión transitoria de sus cuentas de usuario (red, aplicativos y demás servicios informáticos).

La creación de las cuentas de usuario, cambios de perfil o cargo (red, aplicativos y demás herramientas informáticas) y su acceso correspondiente, solo puede ser otorgado por la Oficina TIC, siguiendo los procedimientos y registros establecidos en el **Formato Solicitud Creación o Actualización de Usuarios - GTI-FO-04.**

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.

El usuario (funcionario o contratista) deberá firmar el **Formato Solicitud Creación o Actualización de Usuarios - GTI-FO-04,** 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.

La Oficina TIC 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 TIC emplee para tal fin.

La Oficina TIC 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 de la sede principal y las regionales.

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 TIC 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 TIC para suprimir las autorizaciones brindadas. La Oficina TIC debe verificar permanentemente esas autorizaciones a personal ajeno a la entidad y efectuar los ajustes al respecto de manera controlada.

Es responsabilidad de la Dirección Administrativa y de Talento Humano de la sede principal y las regionales, que, en el caso de vacaciones, licencia o retiro de algún funcionario de la Entidad, se informe inmediatamente a la Oficina TIC 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.

Caso similar aplica para los contratistas que finalicen sus actividades para lo cual el supervisor del contrato deberá informar inmediatamente a la Oficina TIC la cancelación o inhabilitación de su cuenta de usuario de forma temporal o definitiva.

Al crear las cuentas de correo electrónico Institucional, la Oficina TIC 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.

Para el caso de usuarios (funcionarios o terceros) que deban deshabilitarse o modificar sus accesos, producto de desvinculación o reasignación de funciones, la Oficina TIC no lo eliminará de las herramientas informáticas a las cuales tenga acceso, sino que lo bloqueará, desactivará o dejará inactivo, por determinado tiempo, 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.

11.2.2. Suministro de acceso a usuarios – *(Control 9.2.2).*

Las cuentas y los servicios informáticos asociados que no sean utilizados en un período superior a (2) meses, el usuario en referencia 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, incapacidades, sanciones, etc.).

La Oficina TIC debe asignar privilegios de usuario para cada uno de los servicios informáticos, de acuerdo con lo solicitado por el jefe de la dependencia que requiera el servicio, verificando la razonabilidad entre los privilegios solicitados y las funciones del solicitante, de acuerdo a los **Formatos Solicitud Creación o Actualización de Usuarios - GTI-FO-04** y **Formato Solicitud de Excepciones de Seguridad Informática - GTI-FO-05**.

La Oficina TIC 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).

La Oficina TIC deberá 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 prevenir la afectación a otras entidades y a la población en general.

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 Solicitud Creación o Actualización de Usuarios - GTI-FO-04** 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.

11.2.3. Gestión de derechos de acceso privilegiado – *(Control 9.2.3).*

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 TIC, cualquier novedad y/o ajuste que se deba efectuar al respecto producto de un traslado o reasignación de funciones, entre otros.

La Oficina TIC 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 TIC, cualquier novedad y/o ajuste que se deba efectuar al respecto.

La Oficina TIC 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 desde los equipos de cómputo asignados.

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 TIC para que proceda a habilitar el respectivo acceso.

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.

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 TIC 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 TIC para suprimir o deshabilitar las autorizaciones brindadas. La Oficina TIC debe verificar permanentemente esas autorizaciones brindadas al personal ajeno o terceros a la entidad y efectuar los ajustes al respecto de manera controlada.

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.

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 a la dependencia o 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.

Los privilegios de administrador de cualquier equipo de cómputo, deben ser asignados exclusivamente al administrador del sistema. En ningún caso se deben asignar estos privilegios de acceso al usuario del equipo.

Los privilegios de acceso privilegiado a los sistemas de información deben ser otorgados exclusivamente a quienes tengan el control del mismo, previo diligenciamiento del **Formato Solicitud Creación o Actualización de Usuarios - GTI-FO-04,** el cual debe ser independiente al formato creado para la asignación de usuario de dominio.

11.2.4. Gestión de información de autenticación secreta de usuarios – *(Control 9.2.4).*

La Oficina TIC debe suministrar la información de usuario de forma secreta para la autenticación temporal, siendo esta única para cada usuario, así mismo, se debe solicitar a cada usuario el acuse de recibido de la misma, haciendo el respectivo uso del **Formato Solicitud Creación o Actualización de Usuarios - GTI-FO-04**, en el campo NÚMERO MÓVIL Y TELÉFONO FIJO / EXTENSIÓN.

Para el caso de los sistemas de información donde el usuario no se encuentra enlazado con el Directorio Activo (usuario de dominio), los usuarios que se generen serán notificados mediante el caso generado en mesa de ayuda o vía correo electrónico del funcionario que está realizando la solicitud.

11.2.5. Revisión de los derechos de acceso de usuarios – *(Control 9.2.5).*

Los propietarios o custodios de los activos de información deben realizar revisiones periódicas a los derechos de acceso de los usuarios a intervalos regulares y notificar cualquier novedad vía correo electrónico a la Oficina TIC.

La Oficina TIC debe contar con un registro de las modificaciones realizadas a las cuentas privilegiadas, esto de acuerdo a los formatos recepcionados de las actualizaciones a usuarios.

11.2.6. Retiro o ajuste de los derechos de acceso – *(Control 9.2.6).*

Los derechos de acceso de todos los funcionarios y contratistas a la información y a las instalaciones de procesamiento de información de la ALFM se deben retirar al terminar su empleo, contrato o acuerdo, previo diligenciamiento del **Formato Paz y Salvo por Retiro de la Institución** - **GTH-FO-61** o se deben ajustar cuando se hagan cambios de funciones previo diligenciamiento del **Formato Solicitud Creación o Actualización de Usuarios - GTI-FO-04.**

11.3. RESPONSABILIDADES DE LOS USUARIOS – *(Categoría 9.3).*

Objetivo: Todos los usuarios de la ALFM responderán por las acciones u omisiones efectuadas con sus cuentas que puedan atentar con la información de autenticación.

11.3.1. Uso de información de autenticación secreta – *(Control 9.3.1).*

Los usuarios con acceso a los sistemas de información deben proteger los recursos asignados por la entidad, guardar el secreto de su contraseña, no prestar su clave de usuario bajo ninguna circunstancia, cambiar su contraseña periódicamente y notificar a la Oficina TIC, cualquier novedad o incidente informático, que observe en el funcionamiento de su cuenta y en la aplicación de las Políticas de Seguridad de la Información.

Cada administrador de los sistemas de información debe asegurar que la información de autenticación secreta, configurada por defecto desde fábrica, se modifica después de la instalación de los sistemas o software.

Los usuarios deben propender por una administración responsable de sus contraseñas personales, evitando que sean almacenadas en formatos no protegidos.

La administración, así como la asignación y entrega de las contraseñas iniciales a los usuarios deberá ser gestionada por la Oficina TIC, resguardando la confidencialidad de los datos a entregar.

Los usuarios deberán aplicar las siguientes recomendaciones para el uso y selección de las contraseñas de acceso y por lo tanto se responsabilizan de cualquier acción que se realice utilizando el nombre y contraseña de usuario que le sean asignados:

A. Las contraseñas son de uso personal y por ningún motivo se deben prestar a otros usuarios.
A. Las contraseñas no deberán ser reveladas por ningún motivo.
B. Las contraseñas no se deberán escribir en ningún medio, excepto para los casos de administradores, cuando son entregadas en custodia y el archivo se debe encontrar cifrado resguardando su confidencialidad, integridad y disponibilidad.
C. Es deber de cualquier funcionario y contratista reportar cualquier sospecha que una persona esté empleando un usuario y contraseña que no le pertenece, con el propósito de gestionar el incidente de seguridad.
D. La longitud mínima de las contraseñas debe ser de 8 dígitos y contener mínimo una mayúscula, una minúscula, un número y un carácter especial.
E. Las contraseñas no deben estar basadas en temas que puedan adivinarse fácilmente u obtener usando información relacionada con la persona, (nombres, números de teléfono, fechas de nacimiento, etc.).
F. Las contraseñas deben estar libres de caracteres completamente numéricos o alfabéticos idénticos, consecutivos.

11.4. CONTROL DE ACCESO A SISTEMAS Y APLICACIONES – *(Categoría 9.4).*

Objetivo: Evitar el acceso no autorizado a sistemas y aplicaciones.

11.4.1. Restricción de acceso a la información – *(Control 9.4.1).*

El acceso de los usuarios a la información y las funciones del sistema de la aplicación debe limitarse de acuerdo con la política de control de acceso definida.

Las restricciones para el acceso a las aplicaciones se deben basar en el rol que el usuario desempeñará, para ello se debe cumplir con los siguientes aspectos:

A. Generar menús para controlar el acceso a las funciones del sistema de aplicación.
B. Controlar los permisos de acceso de los usuarios: lectura, escritura, modificación y eliminación.
C. Controlar y definir la interacción e intercambio de datos entre sistemas (internos y externos).

La Oficina TIC debe asegurar que las salidas de información de los sistemas, aplicaciones o plataformas que manejan información confidencial sólo contengan la información requerida para el cumplimiento de las labores y solamente el personal autorizado tenga acceso a esta.

Dentro de los aspectos para tener en cuenta por parte de los usuarios, para un buen uso de los sistemas operativos están:

A. El administrador de la plataforma es el responsable de otorgar los accesos a los recursos del sistema operativo.
B. Las autorizaciones a las rutinas del sistema operativo no deben permitir modificaciones, en caso de requerirse, éstas deben ser autorizadas y documentadas.
C. El uso de herramientas o utilitarios propios de los sistemas operativos deben ser limitado a personal autorizado y su uso está restringido a casos específicos, debe disponerse de la trazabilidad de las operaciones realizadas en los casos que son autorizados.
D. Está prohibido el uso de herramientas intrusivas con fines de vulnerar la seguridad del sistema operativo, bases de datos, redes etc.; solamente la Oficina TIC podrá utilizarlas en la realización de pruebas de vulnerabilidad.
E. Las sesiones que no han presentado ningún tipo de actividad por un período de tiempo determinado deben finalizar automáticamente de acuerdo con la configuración definida; esto mismo aplica para los accesos remotos (VPN).
F. Todas las estaciones de trabajo deben estar plenamente identificadas para garantizar la conexión de equipos confiables, esto debe venir acompañado de correctas configuraciones de red que restrinjan la conexión a los servidores permitiendo solamente las conexiones necesarias.
G. Se deben registrar los intentos exitosos y fallidos de autenticación del sistema, mediante los Logs.

11.4.2. Sistema de gestión de contraseñas – *(Control 9.4.3).*

El funcionario debe recibir un usuario y una contraseña para acceder a los recursos informáticos de la entidad, ésta contraseña es de cambio obligatorio en el primer uso, garantizando así su responsabilidad y único conocimiento sobre la misma. Dicha contraseña debe tener una longitud mínima de 8 (ocho) caracteres alfanuméricos, diferentes a nombres propios o cualquier otra palabra de fácil identificación.

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.

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.

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 TIC mediante generación de caso de mesa de ayuda, correo electrónico o medio escrito, la deshabilitación o modificación del perfil según corresponda, previo diligenciamiento del **Formato Solicitud Creación o Actualización de Usuarios - GTI-FO-04.**

11.4.3. Uso de programas utilitarios privilegiados – *(Control 9.4.4).*

Se restringe y controla estrictamente el uso de programas utilitarios que pudieran tener capacidad de anular el sistema y los controles de las aplicaciones los cuales serán únicamente autorizados por la Oficina TIC.

La Oficina TIC mediante la estructuración de las Directivas de Grupo como políticas de seguridad en el Directorio Activo, restringe el acceso no autorizado a los programas utilitarios de los sistemas operativos y demás.

11.4.4. Control de acceso a códigos fuente de programa – *(Control 9.4.5).*

El acceso a código fuente de los programas es limitado, únicamente los funcionarios designados por la Oficina TIC podrán contar con acceso a esta información y harán uso de la misma.

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:

A. 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 TIC, con la debida pertinencia, las fallas u operación irregular que se observe en el hardware (equipo) y/o software debidamente instalado en este.
B. Velar por que se encuentren conectados a los puntos de corriente eléctrica identificados como regulados (tomas naranjas o rojos) únicamente los servidores y estaciones de trabajo.
C. 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 TIC estas anomalías para concertar su solución.
D. 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).

E. Los usuarios y terceros de la ALFM deben cumplir, acatar y aplicar estrictamente las directivas permanentes y transitorias emitidas por la Oficina TIC para la debida operación de las plataformas de TI.
F. 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 TIC o en los manuales de usuario del software respectivo.

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 TIC 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.

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

A. El usuario del software reporta el error a la Oficina TIC mediante caso de mesa de ayuda.
B. La Oficina TIC le asignará el requerimiento a un funcionario especialista en el tema.
C. El funcionario de la Oficina TIC 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).
D. 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.
E. Se archiva toda la información del caso como soporte y como elemento de consulta de lecciones aprendidas para futuros requerimientos similares.
F. Una vez finalizado el caso en la plataforma de mesa de ayuda, el funcionario deberá diligenciar la encuesta de satisfacción, dando de esta forma el cierre definitivo en la plataforma.

12. CRIPTOGRAFÍA – *(Dominio 10)*

12.1. CONTROLES CRIPTOGRÁFICOS – *(Categoría 10.1).*

Objetivo: Asegurar el uso apropiado y eficaz de la criptografía para proteger la confidencialidad, autenticidad y/o integridad de la información.

12.1.1. Políticas sobre el uso de controles criptográficos – *(Control 10.1.1).*

La Oficina TIC debe verificar los sistemas o aplicaciones que realicen y/o permitan la transmisión de información Pública Reservada y Clasificada, lo realicen mediante herramientas de cifrado de datos.

Asegurar que la información Pública Reservada y Clasificada, sea protegida por el usuario final generador de la información, con el uso de la herramienta de encriptación para transferencias de archivos con esta clasificación, por medio de los sistemas de información y comunicaciones.

Los usuarios de la ALFM que usen las herramientas criptográficas, deben dar cumplimiento a los acuerdos y legislación existente Nacional y/o Internacional.

La Oficina TIC debe definir e implementar mecanismos y controles criptográficos para garantizar el cumplimiento de los objetivos de seguridad definidos, en términos de protección de la confidencialidad de la información en medio electrónico, tanto cuando se encuentra almacenada como cuando es transmitida o procesada la información, teniendo en cuenta la clasificación y sensibilidad de la misma.

No se permite el uso de herramientas o mecanismos de cifrado de información diferentes a las autorizadas por la ALFM, los cuales deben estar documentados en una lista de software autorizado que sea divulgada a todos los funcionarios y contratistas autorizados.

13. SEGURIDAD FÍSICA Y DEL ENTORNO – *(Dominio 11).*

13.1. ÁREAS SEGURAS – *(Categoría 11.1).*

Objetivo: Prevenir el acceso físico no autorizado, el daño y la interferencia a la información y a las instalaciones de procesamiento de la información de la ALFM.

13.1.1. Perímetro de seguridad física – *(Control 11.1.1).*

Todas las áreas que se hayan definido como restringidas y activos de información que la componen, son considerados áreas seguras; por lo tanto, deben ser protegidos los accesos no autorizados mediante controles y tecnologías de autenticación.

Se consideran áreas restringidas los centros de datos y todos aquellos que manejen o contengan información sensible; además se prohíbe:

A. Uso de redes inalámbricas.
B. Ingreso de teléfonos celulares, dispositivos de almacenamiento, smartphone, tabletas, equipos de cómputo personal, cámaras fotográficas o cualquier equipo tecnológico no autorizado.

En las áreas seguras donde se encuentren activos informáticos, se debe cumplir como mínimo con los siguientes lineamientos:

A. No consumir alimentos ni bebidas.
B. No ingresar elementos inflamables.
C. No permitir el acceso de personal ajeno, sin que esté acompañado por un funcionario durante el tiempo que dure su visita.
D. No almacenar elementos ajenos a la funcionalidad de la respectiva zona segura.
E. No permitir la toma de fotos o grabaciones de las áreas seguras sin la previa autorización del área responsable de cada una de ellas.
F. No permitir el ingreso de equipos electrónicos, así como maletas o contenedores, a menos que haya una justificación para esto. En ese caso, deberán ser registradas al ingreso y salida, para minimizar la posibilidad de ingreso de elementos no autorizados o la extracción de elementos.

Las áreas protegidas deben contar con las condiciones ambientales que garanticen la correcta operación de los equipos (aire acondicionado de alta precisión) y el estado de los medios que contienen información, así como un sistema de detección y control de incendios.

13.1.2. Controles físicos de entrada – *(Control 11.1.2).*

Todas las puertas que utilicen sistema de control de acceso, deberán permanecer cerradas y es responsabilidad de todos los funcionarios y contratistas autorizados evitar que las puertas se dejen abiertas.

Se debe exigir a todo el personal, sin excepción, el porte en un lugar visible del mecanismo de identificación adoptado para ello por cada una de las oficinas, mientras permanezcan dentro de las instalaciones de la ALFM.

Los visitantes deben permanecer acompañados de un funcionario cuando se encuentren dentro de alguna de las áreas seguras.

Es responsabilidad de todos los funcionarios y contratistas acatar las normas de seguridad y mecanismos de control de acceso a las oficinas de la ALFM.

Los funcionarios y contratistas, así como los visitantes, deben tener acceso físico restringido a los sitios que requieran y les sean autorizados para el cumplimiento de sus funciones, tareas o misión dentro de las instalaciones.

Los servicios de procesamiento de información sensible o crítica deben estar ubicados en áreas restringidas, protegidas por perímetros de seguridad definidos, con barreras y controles de ingreso adecuados. Dichas áreas deben estar protegidas físicamente contra accesos no autorizados, daño e interferencia. La protección suministrada debe estar acorde con los riesgos identificados.

Las áreas protegidas se resguardan mediante el empleo de controles de acceso físico y registro, los cuales se encuentran definidos en el **Protocolo de bioseguridad ingreso y permanencia instalaciones ALFM** - **GTH-DG-06,** para el caso de los visitantes se debe diligenciar el **Formato Autorización Ingreso y Permanencia de Visitantes - GA-FO-36** a fin de permitir el acceso sólo a personal autorizado.

Para incrementar la seguridad en estas áreas se establecerán controles y lineamientos adicionales, así como para las actividades de terceros que tengan lugar allí.

13.1.3. Seguridad de oficinas, recintos e instalaciones – *(Control 11.1.3).*

Las instalaciones claves deben estar ubicadas estratégicamente en zonas con acceso restringido al público.

Debe definirse donde sea aplicable, que las edificaciones sean discretas y den un indicio mínimo de su propósito, sin señales obvias externas o internas, que identifiquen la presencia de actividades de procesamiento de información.

Es necesario establecer que las instalaciones estén configuradas para evitar que las actividades o información confidenciales, sean visibles y/o audibles desde el exterior. El blindaje electromagnético también debe ser el apropiado.

Los directorios y guías telefónicas internas, que identifican los lugares de las instalaciones de procesamiento de información confidencial deben ser accesibles solo a personal autorizado.

13.1.4. Protección contra amenazas externas y ambientales – *(Control 11.1.4).*

Para la selección de las áreas protegidas se tendrá en cuenta la posibilidad de daño producido por incendio, inundación, explosión, agitación civil y otras formas de desastres naturales o provocados por el hombre. También se tomarán en cuenta las disposiciones y normas establecidas (estándares) en materia de sanidad y seguridad.

Las plataformas tecnológicas y los activos de información serán ubicadas y protegidas de tal manera que reduzcan los riesgos ocasionados por amenazas y peligros ambientales y las oportunidades de acceso no autorizado.

Las dependencias de la Oficina Principal y cada una de las Regionales deben acoger los lineamientos a que haya lugar de acuerdo a la normatividad ambiental vigente para el Manejo de Residuos de Aparatos Eléctricos y Electrónicos (RAEE), de forma que se prevenga y reduzca el impacto ambiental.

Se debe garantizar la seguridad física del Centro de Datos, incluyendo entre otros los siguientes subsistemas:

A. Sistema Alarma
B. Sistema Eléctrico
C. Sistema de protección contra incendios
D. Control de temperatura
E. Planilla de ingreso de personal ajeno.

13.1.5. Trabajo en áreas seguras – *(Control 11.1.5).*

El Data Center o centro de cableado debe contar con mecanismos que cumplan los requisitos ambientales (temperatura, humedad, voltaje, entre otros) especificados por los fabricantes de los servidores y equipos de comunicaciones que alberga, igualmente debe contar con sistemas mecánicos para control de incendios, impedir el acceso a personal no autorizado, consumo de alimentos, bebidas o cigarrillo.

La ALFM cuenta con un Sistema de Seguridad CCTV, para otorgar la mayor seguridad posible tanto a los visitantes como a los funcionarios que ingresan a sus instalaciones. El Sistema de Seguridad CCTV opera bajo las siguientes directrices:

A. Profesional seguridad física y del patrimonio es el responsable de operar el sistema CCTV

B. Profesional seguridad física y del patrimonio debe garantizar el funcionamiento del sistema CCTV las 24 horas del día de los 365 días del año. La Dirección Administrativa y de Talento Humano. garantizara la operación y monitoreo.
C. El acceso al centro de monitoreo es de carácter restringido. Las únicas personas que tienen permiso de acceder son el Profesional seguridad física y del patrimonio y aquellos funcionarios que autorice la Dirección Administrativa y de Talento Humano.
D. El personal asignado para la administración de los medios tecnológicos del CCTV debe notificar vía telefónica o electrónica a la profesional seguridad física y del patrimonio acerca de las fallas o ausencias de video que se presenten en las cámaras del sistema CCTV (Circuito Cerrado de Televisión) de la ALFM. Lo anterior con el fin de restablecer dicho servicio y mantener su correcto funcionamiento.
E. Cuando el personal asignado detecte que alguna cámara ha sido girada sin autorización, debe informar a la Dirección Administrativa y de Talento Humano, para que se genere la evidencia y se autorice devolverla a su posición original.
F. Cuando el personal asignado para la administración de los medios tecnológicos del CCTV detecte anomalías o incidentes en las zonas de monitoreo, éstas deben ser reportadas inmediatamente al Supervisor de contrato de Vigilancia y Seguridad Privada.
G. Toda solicitud de copias de video debe hacerse por escrito a la Dirección Administrativa y de Talento Humano.
H. Todas las grabaciones tienen una duración mínima de 30 días y después se reescribe.
I. Está prohibido dar información de especificaciones técnicas y ubicaciones de cámaras.
J. Toda copia de video generada debe ser entregada mediante oficio o mediante cadena de custodia.

La ALFM debe contar con un plan de emergencias definido por la Dirección Administrativa y de Talento Humano., el cual debe estar basado en la **Guía para el diseño del plan de emergencias - GTH-GU-11**, que debe ser probado anualmente, con el fin de brindar protección contra amenazas externas.

13.1.6. Áreas de despacho y cargas – *(Control 11.1.6).*

Se debe controlar los puntos de acceso tales como áreas de despacho y de carga, y otros puntos en donde pueden entrar personas no autorizadas, y si es posible, aislarlos de las instalaciones de procesamiento de información para evitar el acceso no autorizado, adicionalmente se debe cumplir con los siguientes parámetros:

A. Deben existir registros que dejen evidencia del transporte donde se identifique el contenido de los medios, la protección aplicada, al igual que los tiempos de transferencia a los responsables durante el transporte, y el recibo en su destino.
B. Establecer que el acceso al área de despacho y de carga desde el exterior de la edificación se debería restringir al personal identificado y autorizado.
C. Definir que el área de despacho y carga se debe diseñar de manera que los suministros se puedan cargar y descargar sin que el personal de despacho tenga acceso a otras partes de la edificación.
D. Establecer que las puertas externas de un área de despacho y carga se aseguran cuando las puertas internas están abiertas.

E. Definir que el material que ingresa se inspecciona y examina para determinar la presencia de explosivos, químicos u otros materiales peligrosos, antes de que se retiren del área de despacho y carga.
F. Establecer que el material que ingresa se registra de acuerdo con los procedimientos establecidos al entrar al sitio.
G. Definir que los despachos entrantes y salientes están separados físicamente, en donde sea posible.
H. Establecer que el material entrante se inspecciona para determinar evidencia de manipulación durante el viaje. Si se descubre esta manipulación, se debería reportar de inmediato.

13.2. EQUIPOS – *(Categoría 11.2).*

Objetivo: Prevenir la pérdida, daño, robo o compromiso de activos y la interrupción de las operaciones de la ALFM.

13.2.1. Ubicación y protección de los equipos – *(Control 11.2.1).*

Los equipos que hacen parte de la infraestructura tecnológica de las ALFM, deben ser ubicados y protegidos adecuadamente para prevenir la pérdida, daño, robo o acceso no autorizado de los mismos.

La ALFM adoptará los controles necesarios para mantener los equipos alejados de sitios que puedan tener riesgo de amenazas potenciales como fuego, explosivos, agua, polvo, vibración, interferencia electromagnética y vandalismo, entre otros.

Los equipos tales como máquinas de copiado, impresoras y máquinas de fax deben estar ubicados en zonas de acceso restringido únicamente al personal de la dependencia, debe estar con su respectiva configuración (usuarios autorizados) y el control para su uso.

13.2.2. Servicios de suministro – *(Control 11.2.2).*

La ALFM cuenta con aire acondicionado, UPS (sistema de alimentación ininterrumpida, en inglés (Uninterruptible Power Supply). que asegura el tiempo necesario de autonomía para que la planta eléctrica entre a soportar la carga o mientras regresa la energía eléctrica, ante una falla en el suministro de energía, un enlace de red redundante y un sistema de monitoreo de las condiciones (temperatura, humedad, voltaje, apertura y cierre de puertas) del Datacenter.

13.2.3. Seguridad del cableado – *(Control 11.2.3).*

El cableado de energía eléctrica y comunicaciones que transportan datos o brinda apoyo a los servicios de información estarán protegidos contra intercepción o daños.

En las unidades de la ALFM todo el sistema de cableado estructurado deberá contemplar la normatividad vigente, que proporciona una guía para la ejecución de la administración de un buen sistema de cableado.

13.2.4. Mantenimiento de equipos – *(Control 11.2.4).*

Únicamente el personal autorizado por la Oficina TIC (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 TIC.

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.

Se debe asegurar que, en la infraestructura utilizada para el procesamiento de la información, las comunicaciones y la seguridad informática, se realicen mantenimientos periódicos de acuerdo al **Procedimiento Gestión de TICs - Mantenimiento TICs** - **GTI-PR-04,** con el fin de que dichas actividades no se vean afectadas por obsolescencia. Por lo tanto, se revisará constantemente la vida útil de cada uno de los recursos que componen dicha infraestructura de acuerdo con la descripción y recomendaciones de sus fabricantes, contemplando dentro de estos mantenimientos correctivos/preventivos aquellos equipos cuya garantía de fábrica expiró.

Los usuarios son responsables por la custodia y las acciones que se realicen a través de los activos informáticos asignados, por lo tanto, deben estar presentes en el sitio de trabajo cuando se realice cualquier mantenimiento o actualización de dichos activos e inspeccionar para asegurarse que no ha sido alterado y que su funcionamiento es adecuado.

La Oficina TIC debe llevar un registro mediante el **Formato Mantenimiento Preventivo Efectuado a Hardware** - **GTI-FO-02** de todas las fallas reales o sospechadas, y de todo el mantenimiento preventivo que se realice sobre los activos informáticos de la entidad.

13.2.5. Retiro de activos – *(Control 11.2.5).*

Todo el personal que por cumplimiento de sus funciones institucionales necesite retirar un activo de información de las instalaciones de la ALFM, deben ser debidamente identificados y registrados antes de conceder la autorización respectiva.

El retiro de cualquier activo de información de la entidad, debe ser autorizado por el propietario del activo previa solicitud del funcionario interesado de acuerdo al diligenciamiento del **Formato Ingreso y Salida de Elementos - GA-FO-35**.

La ALFM proporcionará los mecanismos y recursos necesarios para que en cada punto de acceso a las instalaciones exista un control de revisión, donde se inspeccione y se lleve el control de los equipos que son ingresados y retirados de la entidad de acuerdo al diligenciamiento de la **Formato Planilla de Control Ingreso y Salida** - **GA-FO-34**.

13.2.6. Seguridad de equipos y activos fuera de la instalación – *(Control 11.2.6).*

Si por razones de trabajo los funcionarios que tengan a su cargo un equipo de cómputo necesitan llevarlo a sitios fuera de las instalaciones deben estar previamente autorizados por el jefe de la dependencia, la información sensible o clasificada que contengan debe estar cifrada en el disco duro o borrada en forma segura.

Los usuarios que requieran manipular los equipos o medios fuera de las instalaciones de la ALFM, deben velar por la protección de los mismos sin dejarlos desatendidos.

El propietario del activo, con el apoyo de la Oficina TIC, identificará mediante una metodología de análisis de riesgos que cada dependencia, establezca los riesgos potenciales que puede generar el retiro de equipos o medios de las instalaciones; así mismo, adoptará los controles necesarios para la mitigación de dichos riesgos.

En caso de pérdida o robo de un equipo portátil o cualquier medio que contenga información clasificada y que esté además relacionada con la defensa y la seguridad nacional, el responsable del equipo deberá ponerlo en conocimiento de la Oficina TIC y debe realizar inmediatamente el respectivo reporte de incidente de seguridad, así como realizar la correspondiente denuncia ante la autoridad competente, si el caso lo amerita.

Los equipos de cómputo o activos de información que por razones del servicio se retiren de las instalaciones de la ALFM, deberán contener únicamente la información estricta y necesaria para el cumplimiento de su misión, así mismo, se deshabilitarán los recursos que no se requieren o puedan poner en riesgo la información que contiene, adicionalmente la información debe estar cifrada.

13.2.7. Disposición segura o reutilización de equipos – *(Control 11.2.7).*

Para los procesos de baja, de reutilización, enajenación o de garantía de los dispositivos que contengan medios de almacenamiento, se debe cumplir según sea el caso, con la destrucción física del mismo o borrado seguro, teniendo muy presente los temas de licenciamiento de software para cada una de las situaciones enunciadas.

Cuando el activo de información sea dado de baja se retira el disco duro y se realiza el borrado seguro a la información para prevenir la pérdida de confidencialidad en la ALFM. Posteriormente se realizará la destrucción segura y se documentará mediante acta, registro fílmico y/o fotográfico.

Para la reasignación de los equipos de cómputo se entregarán a la Oficina TIC para realizar el borrado seguro de la información y configuración de los mismos.

Para la garantía en equipos de cómputo se realiza el backup de la información y el borrado seguro, se procede a la entrega del disco duro a la empresa encargada de realizar el soporte y respectiva garantía cuando aplique.

Para la renovación de equipos de cómputo se realiza el particionamiento y configuración respectiva del disco duro con posterior entrega a la dependencia.

13.2.8. Equipos de usuarios desatendidos – *(Control 11.2.8).*

En horas no hábiles, o cuando los sitios de trabajo se encuentren desatendidos, los usuarios deberán dejar los medios que contengan información crítica protegida bajo llave.

Los usuarios deberán bloquear su estación cada vez que se ausenten de su puesto de trabajo y sólo se podrá desbloquear con la contraseña del mismo usuario que la bloqueó.

13.2.9. Política de escritorio y pantalla limpios – *(Control 11.2.9).*

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.

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.

Toda vez que un funcionario, personal en comisión o contratista se ausenta de su lugar de trabajo, debe bloquear su equipo de cómputo asignado, para de esta forma proteger la información alojada en aplicaciones, servicios y plataformas de la ALFM, deberá guardar en lugar seguro cualquier documento, medio magnético u óptico removible que contenga información confidencial y sensible.

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.

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 TIC.

La autenticación o ingreso a las estaciones de trabajo de la institución debe requerir como mínimo la identificación de un usuario y una clave asignada.

Los funcionarios, contratistas, personas en comisión, pasantes y terceros que tienen algún vínculo con la ALFM deben conservar su escritorio libre de información, propia de la entidad, que pueda ser alcanzada, copiada o utilizada por terceros o por personal que no tenga autorización para su uso o conocimiento.

14. SEGURIDAD DE LAS OPERACIONES – *(Dominio 12).*

14.1. PROCEDIMIENTOS OPERACIONALES Y RESPONSABILIDADES – *(Categoría 12.1).*

Objetivo: Asegurar las operaciones correctas y seguras de las instalaciones de procesamiento de la información.

14.1.1. Procedimientos de operación documentados – *(Control 12.1.1).*

Los procedimientos de operación se deben documentar y poner a disposición de todos los usuarios que los necesiten.

La ejecución de cualquier actividad asociada con la infraestructura tecnológica para el procesamiento de información, comunicaciones y seguridad informática debe estar soportada por instrucciones o procedimientos operativos documentados, los formatos siempre deben estar a disposición de todos los usuarios que los necesiten para el desarrollo de sus labores.

Los procedimientos operativos deben quedar debidamente documentados, teniendo en cuenta el procesamiento y manejo de la información, contactos de soporte en caso de dificultades técnicas u operativas, así como instrucciones para el manejo de medios y exposición de resultados especiales y de carácter confidencial.

Los procedimientos operativos deben contener instrucciones para el manejo de los errores que se puedan presentar en la ejecución de las actividades, contactos de soporte, procedimientos de reinicio y recuperación de sistemas y aplicaciones, forma de procesamiento y manejo de la información, copia de respaldo de la información y los demás a los que hubiera lugar.

14.1.2. Gestión de cambios – *(Control 12.1.2).*

Todo cambio que se realice sobre cualquier activo de información debe ser controlado, gestionado y autorizado adecuadamente por parte de la Oficina TIC, conforme al **Formato Gestión del Cambio** - **GI-FO-17**; debe cumplir con una planificación y ejecución de pruebas que identifiquen riesgos e impactos potenciales asociados que puedan afectar su operación.

14.1.3. Gestión de capacidad – *(Control 12.1.3).*

La Oficina TIC, como área responsable de la administración de la plataforma tecnológica, debe implementar los mecanismos, controles y herramientas necesarias para asegurar que los recursos que componen dicha plataforma sean periódicamente monitoreados, afinados y proyectados para futuros requerimientos de capacidad de procesamiento y comunicación.

El responsable de cada componente de la plataforma tecnológica deberá realizar el monitoreo permanente sobre este.

14.1.4. Separación de los ambientes de desarrollo, pruebas y operación – *(Control 12.1.4).*

La Oficina TIC proveerá los mecanismos, controles y recursos necesarios para contar con niveles adecuados de separación lógica o física entre los ambientes de desarrollo, pruebas y producción para toda su plataforma tecnológica y sistemas de información, con el fin de reducir el acceso no autorizado y evitar cambios que pudieran afectar su operación.

Los usuarios deberán utilizar diferentes perfiles para el ambiente de desarrollo, de pruebas y de producción; así mismo, se deberá asegurar que cada usuario cuente únicamente con los privilegios necesarios en cada ambiente para el desarrollo de sus funciones.

No deberán realizarse pruebas, instalaciones o desarrollos de hardware o software directamente sobre el entorno de producción con el fin de evitar problemas de disponibilidad, confidencialidad e integridad de la información.

El ambiente del sistema de prueba debe emular el ambiente de producción lo más similar posible.

No se permite la copia de información pública clasificada y reservada desde el ambiente de producción al ambiente de desarrollo y/o calidad. En caso que sea estrictamente necesario, la copia debe contar con las respectivas autorizaciones y se deben implementar controles que garanticen que la confidencialidad de la información sea protegida mediante el uso de usuarios, roles y privilegios definidos y controlados, para determinados lapsos de tiempos en que se efectuaran las pruebas.

Se restringe el acceso a los compiladores, editores, utilidades de los sistemas y otras herramientas de desarrollo desde los sistemas del ambiente de producción a cualquier usuario que no lo requiera para el desarrollo de su labor.

Periódicamente se podrán verificar las versiones instaladas tanto en ambiente de pruebas como en producción y se confrontará esta información con revisiones previas y con las versiones de programas fuentes almacenadas en los repositorios de la ALFM.

14.2. PROTECCIÓN CONTRA CÓDIGOS MALICIOSOS – *(Categoría 12.2).*

Objetivo: Asegurar que la información y las instalaciones de procesamiento de información estén protegidas contra códigos maliciosos.

14.2.1. Controles contra códigos maliciosos – *(Control 12.2.1).*

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 TIC.

Los usuarios de la entidad son responsables de verificar que la información y los medios de almacenamiento (USB, CD, DVD, Discos Duros, 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 la Oficina TIC programará los escaneos automáticos de antivirus que se realizan de manera controlada.

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.

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.

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.

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 TIC para la detección y erradicación del virus.

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.

Las herramientas y demás mecanismos de seguridad implementados no deberán ser deshabilitados o desinstalados sin la correspondiente autorización de la Oficina TIC y deberá ser actualizadas en forma permanentemente.

Todos los medios de almacenamiento que se conecten a equipos de la infraestructura de la ALFM, deberán ser escaneados en búsqueda de código malicioso o cualquier elemento que pudiera afectar la seguridad de la información corporativa.

Los sistemas, equipos e información institucionales deberán ser revisados periódicamente para verificar que no haya presencia de código malicioso.

14.3. COPIAS DE RESPALDO – *(Categoría 12.3).*

Objetivo: Proteger la información contra la pérdida de datos.

14.3.1. Respaldo de la Información – *(Control 12.3.1).*

Al realizar copias de seguridad en CD, DVD o cualquier otro medio de almacenamiento, debe proceder a su etiquetado, la etiqueta correcta debe incluir la siguiente información:

A. 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.
B. Tipo de copia. Se debe indicar si la copia es incremental, diferencial o completa.
C. Fecha en la que se realizó la copia.
D. 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.
E. 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.

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

El personal responsable de ejecutar las tareas de Backups y recuperación deberá regirse por los procedimientos y actividades establecidas en la **Guía Realización de BACKUPS de Usuarios - GTI-GU-01** 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.

Cada usuario responsable de activos de información crítica y oficial para la entidad que no se encuentre respaldada mediante algún sistema de información debe propender por resguardar una copia de seguridad de sus archivos de ofimática (Word, Excel, PowerPoint, etc.) que se generen en su estación de trabajo, o bien solicitar a la Oficina TIC el resguardo en una carpeta compartida, probando a su vez el mecanismo de recuperación, para lo cual la Oficina TIC 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 Realización de BACKUPS de Usuarios - GTI-GU-01**

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.

La Oficina TIC debe registrar las restauraciones realizadas y los motivos que han ocasionado dicha recuperación y llevará un registro mediante la plataforma de mesa de ayuda, con mínimo los siguientes campos:

A. Fecha de restauración en la que se realizó la recuperación de la copia.
B. Incidencia que ha motivado la restauración; decir la causa que ocasionó la restauración de la información.
C. Ubicación. Decir el equipo en el que se realiza la restauración de la información perdida.
D. Técnico. El funcionario responsable que lleva a cabo la restauración.

Si el jefe de la dependencia de la cual se retira el usuario requiere copia de esta información, debe enviar una comunicación oficial a la Oficina TIC, para evaluar la pertinencia de la toma de backup, restauración y entrega de la copia.

El uso de dispositivos de almacenamiento externo se encuentra restringido (dispositivos móviles, DVD, CD, memorias USB, agendas electrónicas, celulares, etc.), ya que son susceptibles de transmisión de virus informáticos o pueden ser utilizados para la extracción de información no autorizada. Para utilizar dispositivos de almacenamiento externo se debe obtener aprobación formal e individual de la Oficina TIC previo diligenciamiento y aprobación del **Formato Solicitud de Excepciones de Seguridad Informática - GTI-FO-05.**

La Oficina TIC proporcionará medios de respaldo adecuados para asegurar que toda la información esencial y el software, se pueda recuperar después de una falla, garantizando que la información y la infraestructura de software crítica de la entidad, sean respaldadas y puedan ser restauradas en caso de una falla y/o desastre.

La restauración de copias de respaldo debe estar debidamente aprobada por el propietario de la información y solicitada a través de la herramienta de “mesa de ayuda” establecida por la entidad.

Los administradores de las plataformas de información, generarán copias de respaldo (Backup) mensualmente; con el fin de garantizar la continuidad de las actividades realizadas en la entidad, y efectuará las restauraciones en caso de requerirse.

La Oficina TIC debe mantener un inventario actualizado de las copias de respaldo de la información y los aplicativos o sistemas de la ALFM, **Formato Almacenamiento Periódico de Backups - GTI-FO-03.**

Se debe hacer copias de respaldo de la información, software e imágenes de los sistemas, y ponerlas a prueba regularmente con el fin de mantener su integridad.

14.4. REGISTRO Y SEGUIMIENTO – *(Categoría 12.4).*

Objetivo: Registrar eventos y generar evidencia.

14.4.1. Registro de eventos – *(Control 12.4.1).*

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” 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.

Tanto los sistemas de información que manejan información crítica, como los dispositivos de procesamiento, de red y de seguridad informática deben generar registros de eventos que serán verificados periódicamente con el fin de detectar actividades no autorizadas sobre la información.

El tiempo de retención de los “logs” estará dado por las condiciones específicas de cada sistema de información, recurso informático o dispositivo de red y por las leyes, normativas o regulaciones que rigen a la ALFM.

El lugar de retención de los registros estará definido por el nivel de clasificación de información que posean dichos registros.

Todo evento que se identifique por medio del monitoreo y revisión de los registros y que ponga en riesgo la integridad, disponibilidad o confidencialidad de la infraestructura tecnológica deberá ser reportado a la Oficina TIC.

Se debe elaborar, conservar y revisar regularmente los registros acerca de actividades del usuario, excepciones, fallas y eventos de seguridad de la información.

14.4.2. Protección de la información de registro – *(Control 12.4.2).*

El usuario deberá reportar de forma inmediata a la Oficina TIC y a la Dirección Administrativa y talento Humano, 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.

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

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

14.4.3. Registro del administrador y del operador – *(Control 12.4.3).*

La Oficina TIC (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.

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

A. Revisión de registros de fallas para garantizar que las mismas fueron resueltas satisfactoriamente.
B. Revisión de medidas correctivas para garantizar que los controles de seguridad no fueron comprometidos, y que las medidas tomadas fueron autorizadas.
C. Documentación de la falla y las acciones adelantadas para subsanarla.

14.4.4. Sincronización de relojes – *(Control 12.4.4).*

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

14.5. CONTROL DE SOFTWARE OPERACIONAL – *(Categoría 12.5).*

Objetivo: Asegurar la integridad de los sistemas operacionales.

14.5.1. Instalación de software en sistemas operativos – *(Control 12.5.1).*

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), debe ser expresamente autorizado e instalado por personal de la Oficina TIC.

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

Mantener en todos los equipos de la ALFM solamente software licenciado y autorizado por la Oficina TIC, 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”.

Está estrictamente prohibido para los funcionarios (excluyendo de esta prohibición al personal debidamente autorizado de la Oficina TIC, 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:

A. 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 TIC con el único propósito de administrar la funcionalidad y la seguridad de los recursos informáticos institucionales.
B. Rastreen vulnerabilidades en sistemas de cómputo (hardware o software). Se excluye de esta prohibición las herramientas que utilice la Oficina TIC con el único propósito de constatar los niveles de la seguridad de los recursos informáticos institucionales.
C. Tengan un carácter de juegos y/o contenidos pornográficos.

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.

Se considera una falta grave que instalen o intenten instalar cualquier tipo de programa (software) no autorizado 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 TIC y estar relacionado en el inventario de software que la entidad reporta a la Dirección Nacional de Derechos de Autor.

14.6. GESTIÓN DE LA VULNERABILIDAD TÉCNICA – *(Categoría 12.6).*

Objetivo: Prevenir el aprovechamiento de las vulnerabilidades técnicas.

14.6.1. Gestión de las vulnerabilidades técnicas – *(Control 12.6.1).*

La información sobre las vulnerabilidades técnicas de los sistemas de información que se utilizan en la ALFM, se obtendrá en el momento oportuno; se evalúa la exposición de la entidad a estas vulnerabilidades, y se toman las medidas requeridas para tratar el riesgo asociado.

La Oficina TIC, se encargará de identificar las vulnerabilidades técnicas de las diferentes plataformas tecnológicas y definirá las herramientas o servicios necesarios para gestionar las vulnerabilidades.

La Oficina TIC, será el responsable de proponer y ejecutar un programa de evaluación y gestión de vulnerabilidades que debe ser utilizado para la plataforma tecnológica de la entidad.

No se permite a los usuarios de los activos informáticos, sin previa autorización de la Oficina TIC, realizar o participar por iniciativa propia o de terceros, en pruebas de acceso o ataques (activos o pasivos) a los activos informáticos de la ALFM, o a la utilización de los mismos para efectuar pruebas de vulnerabilidad, ataques a otros equipos o sistemas externos.

Los administradores de las plataformas y sistemas de información serán responsables de mantener protegida la infraestructura a su cargo de los riesgos derivados de las vulnerabilidades técnicas identificadas.

Se realizará, por parte de la Oficina TIC, el seguimiento y verificación para las correcciones de las vulnerabilidades identificadas.

La Oficina TIC, realizará las revisiones de las alertas de seguridad, definiendo en caso de ser necesario, un plan de acción para mitigar el impacto de las mismas en la infraestructura tecnológica de la entidad.

14.6.2. Restricciones sobre la instalación de software – *(Control 12.6.2).*

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), debe ser expresamente autorizado e instalado por personal de la Oficina TIC.

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

Mantener en todos los equipos de la ALFM solamente software licenciado y autorizado por la Oficina TIC, 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”.

Está estrictamente prohibido para los funcionarios (excluyendo de esta prohibición al personal debidamente autorizado de la Oficina TIC, 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:

A. 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 TIC con el único propósito de administrar la funcionalidad y la seguridad de los recursos informáticos institucionales.
B. Rastreen vulnerabilidades en sistemas de cómputo (hardware o software). Se excluye de esta prohibición las herramientas que utilice la Oficina TIC con el único propósito de constatar los niveles de la seguridad de los recursos informáticos institucionales.
C. Tengan un carácter de juegos y/o contenidos pornográficos.

El software 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.

Se considera una falta grave que instalen o intenten instalar cualquier tipo de programa (software) no autorizado 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 TIC y estar relacionado en el inventario de software que la entidad reporta a la Dirección Nacional de Derechos de Autor.

Los funcionarios de la ALFM, son responsables de dar aviso a la Oficina TIC, por medio de la mesa de ayuda institucional, de cualquier anomalía detectada en relación al funcionamiento del software.

Con el fin de mitigar las vulnerabilidades, la Oficina TIC debe contar con conexiones que provean de forma segura actualizaciones automáticas de seguridad ara los sistemas operativos y aplicaciones que corresponda.

La Oficina TIC, será la encargada de la actualización de software, así como de las actualizaciones y parches de seguridad requeridas por las estaciones de trabajo.

14.7. CONSIDERACIONES SOBRE AUDITORIAS DE SISTEMAS DE INFORMACIÓN – *(Categoría 12.7).*

Objetivo: Minimizar el impacto de las actividades de auditoría sobre los sistemas operacionales.

14.7.1. Controles sobre auditorias de sistemas de información – *(Control 12.7.1).*

La ALFM apoyada en la Oficina de Control Interno y la Oficina Asesora de Planeación y Gestión Institucional, a través del **Procedimiento Gestión de Seguimiento y Evaluación - Auditorías Internas - GSE-PR-02** verificará el cumplimiento de los requisitos de la normatividad legal vigente, los requisitos internos del proceso y procedimientos. Estás deberán ser acordadas y planificadas para reducir al mínimo las interrupciones en los procesos.

Se deben establecer a través de la Oficina de Control Interno y la Oficina Asesora de Planeación y Gestión Institucional, controles que permitan realizar auditorías, supervisión de las actividades por los técnicos responsables de la infraestructura de red y sus sistemas de información.

El alcance de las pruebas técnicas de auditoría se debe acordar y controlar, las pruebas de auditoría que puedan afectar la disponibilidad del sistema se deben realizar fuera de horas laborales.

15. SEGURIDAD DE LAS COMUNICACIONES – *(Dominio 13).*

15.1. GESTIÓN DE LA SEGURIDAD DE LAS REDES – *(Categoría 13.1).*

Objetivo: Asegurar la protección de la información en las redes, y sus instalaciones de procesamiento de información de soporte.

15.1.1. Controles de red – *(Control 13.1.1).*

La Oficina TIC, administra y gestiona la red de la ALFM.

La Oficina TIC, establece los controles lógicos para el acceso a los diferentes recursos informáticos, con el fin de mantener los niveles de seguridad apropiados.

La Oficina TIC, proporciona todos los recursos tecnológicos de conectividad necesarios para que se puedan desempeñar las funciones y actividades asignadas a cada uno de los funcionarios y contratistas de la entidad.

La Oficina TIC, monitorea la funcionalidad de las redes a través del uso de analizadores de red.

Los funcionarios, contratistas y terceros; no tienen permitido conectar a las estaciones de trabajo o a los puntos de acceso de la red institucional, elementos de red (tales como switches, enrutadores, módems, etc.), que no sean autorizados por la Oficina TIC.

15.1.2. Seguridad de los servicios de red – *(Control 13.1.2).*

La Oficina TIC realiza control de seguridad en la consulta de servicios en las redes internas a través de la habilitación de puertos de escucha de las aplicaciones.

15.1.3. Separación en las redes – *(Control 13.1.3).*

En los equipos de administración de red de la ALFM, se crean la separación de las redes a través de VLAN's y en los equipos de administración perimetral se realiza la segmentación.

La plataforma tecnológica crítica de la ALFM, que soporta los sistemas de información, debe estar separada en segmentos de red físicos y lógicos e independientes de los segmentos de red de usuarios, de conexiones con redes con terceros y del servicio de acceso a internet.

La división de estos segmentos debe ser realizada por medio de dispositivos perimetrales e internos de enrutamiento y de seguridad si así se requiere. La Oficina TIC, es la encargada de establecer el perímetro de seguridad necesario para proteger dichos segmentos, de acuerdo con el nivel de criticidad y del flujo de la información transmitida.

15.2. TRANSFERENCIA DE INFORMACIÓN – *(Categoría 13.2).*

Objetivo: Mantener la seguridad de la información transferida dentro de la Institución y con cualquier entidad externa.

15.2.1. Políticas y procedimientos de transferencia de información – *(Control 13.2.1).*

Las políticas formales de transferencia, procedimientos y controles deben estar en posición de proteger la transferencia de información a través del uso de todo tipo de medios de comunicación, por lo que se debe tener en cuenta para la transferencia de activos tipo información el **Plan de transferencias documentales - GA-DG-04 y el Procedimiento Gestión Administrativa - Organización de archivos de gestión y transferencias documentales - GA-PR-11**

Para el trámite de las comunicaciones internas, se debe tener en cuenta lo siguiente:

A. Se utilizará la firma electrónica en PDF, evitando imprimir innecesariamente estos documentos al ser viables el trámite de forma digital y dando cumplimiento a la Directiva Permanente de Cero Papel.

B. La documentación de carácter interno de la ALFM (excepto carácter legal) será firmada electrónicamente a través del Adobe.
C. Se tramitarán las comunicaciones internas y externas por el Sistema de Información ORFEO.

Para el trámite de las comunicaciones oficiales externas, se debe tener en cuenta lo siguiente:

A. 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.
B. La documentación firmada electrónicamente en Adobe será válida siempre y cuando se tramite a través del Sistema de Información en general 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.
C. 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.

15.2.2. Acuerdos sobre transferencia de información – *(Control 13.2.2).*

Todo funcionario o contratista es responsable de proteger la confidencialidad e integridad de la información de la ALFM y debe tener especial cuidado en el uso de los diferentes medios para el intercambio de información que puedan generar una divulgación o modificación no autorizada.

Los propietarios que requieran intercambiar información, son responsables de definir los niveles y perfiles de autorización para acceso, modificación y eliminación de la misma; por su parte, los custodios de esta información son responsables de implementar los controles que garanticen el cumplimiento de los criterios de confidencialidad, integridad y disponibilidad de acuerdo a la reglamentación vigente.

Los protocolos de intercambio de información, deben cumplir las regulaciones legales, de propiedad intelectual y protección de datos personales. Así mismo, deben especificar las consideraciones de seguridad y reserva de la información y las responsabilidades por el mal uso o divulgación de la misma.

Cuando la información sea solicitada por autoridad judicial o administrativa competente, la entrega se realizará de acuerdo a los controles establecidos para la protección de los activos de información (Confidencialidad, Integridad y Disponibilidad).

El intercambio de información deberá contemplar las siguientes directrices:

A. Uso de web services, para la publicación y consumo de información electrónica.
B. Uso de canales cifrados.
C. Respeto por los derechos de autor del software intercambiado.
D. Términos y condiciones de la licencia bajo la cual se suministra el software.
E. Informar al titular de los datos, el intercambio de estos.
F. Informar sobre la propiedad de la información suministrada y las condiciones de su uso.

15.2.3. Mensajería electrónica – *(Control 13.2.3).*

El servicio de mensajería electrónica institucional de la ALFM, debe ser empleado únicamente para enviar y recibir mensajes de orden institucional.

Los usuarios que tienen asignada una cuenta de correo institucional, son los únicos responsables 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).

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

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”.

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.

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 TIC, con el fin de evitar la posible pérdida de información.

Los usuarios del servicio de correo, al momento de retiro de la entidad, deberán hacer entrega formal del archivo “.pst” (que contiene los correos entrantes y salientes), al jefe directo quien garantizará la entrega de este archivo.

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 este caso se hace necesario que el usuario periódicamente de apertura al Outlook en la estación de trabajo asignada, de tal forma que los archivos gestionados en la plataforma web sean descargados (se debe descargar tanto los correos entrantes como los salientes); en cualquiera de estos casos se deberán respetar las políticas establecidas en este documento para el uso adecuado del servicio de correo.

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 TIC, a fin de hacer el respectivo

seguimiento y tomar las medidas pertinentes de bloqueo a ese remitente y a 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.

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.

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, para lo cual la Oficina TIC procederá a liberarlo y le llegará normalmente ese correo al usuario destinatario que lo solicitó, para que pueda gestionarlo.

Si el usuario considera que un correo entrante que le llegó directamente a su bandeja de correo corresponde a un mensaje riesgoso o clasificado como SPAM, debe reportar el bloqueo de este, enviando un email a la cuenta de correo electrónico liberarspam@agencialogistica.gov.co, para lo cual la Oficina TIC previa validación procederá a bloquear el remitente y los link que contenga.

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.

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, saturando y bloqueando 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 institucional oficial y solo por las personas que están previamente autorizadas para realizar dicho envío.

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.

Los mensajes según su utilidad, deberán por parte de los usuarios, 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; para lo cual se tendrá el apoyo del personal de la Oficina TIC.

Permanentemente se debe abrir la herramienta 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.

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.

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 los establecidos por la ALFM.

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 de la información de la Entidad.

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 de almacenamiento interno “SAN_NAS2”). Si es el caso se debe solicitar el respectivo apoyo a la Oficina TIC para establecer el canal que cumpla con las condiciones apropiadas para garantizar que la transferencia o publicación sea efectiva.

La Oficina TIC 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 Solicitud Creación o Actualización de Usuarios - GTI-FO-04**, debidamente diligenciado y firmado.

Al crear las cuentas de correo electrónico Institucional, la Oficina TIC 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.

Para el caso de que un usuario tenga asignada una cuenta de correo institucional y sea desvinculado de la entidad u ordenada la restricción de acceso por uso indebido a través de la Alta Dirección, debe ser reportado inmediatamente (a la Oficina TIC, Dirección Financiera y Dirección de Contratos) por parte de la Dirección Administrativa y de Talento Humano (Sede principal y de regionales).

La Dirección Administrativa y de Talento Humano (Sede principal y de regionales) es responsable de reportar periódicamente y cada vez que exista cambios o movimientos de personal informando todas las novedades para garantizar la desvinculación de usuarios de los sistema y plataformas. La Oficina TIC 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).

Cuando un funcionario o contratista al que le haya sido autorizado el uso de una cuenta de correo institucional y se retire de la ALFM, su cuenta de correo será desactivada de forma inmediata previa firma del **Formato Paz y Salvo por Retiro de la Institución - GTH-FO-61.**

15.2.4. Acuerdos de confidencialidad y no divulgación – *(Control 13.2.4).*

Todos los funcionarios y contratistas deben firmar los acuerdos de confidencialidad y no divulgación que debe ser parte integral de los contratos, empleando la promesa de reserva y contemplando factores como responsabilidades y acciones de los firmantes para evitar la divulgación de información no autorizada. Este requerimiento también se aplicará para los casos de contratación de personal temporal o cuando se permita el acceso a la información o a los recursos a personas o entidades externas, de acuerdo al **Formato Acuerdo de Confidencialidad Servidores Públicos - GTH-FO-119** para funcionarios y el **Formato Acuerdo de confidencialidad y no divulgación contratistas - GTI-FO-01** para contratistas.

16. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS – *(Dominio 14).*

16.1. REQUISITOS DE SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN – *(Categoría 14.1).*

Objetivo: Garantizar que la seguridad de la información sea una parte integral de los sistemas de información durante todo el ciclo de vida. Esto incluye también los requisitos para sistemas de información que prestan servicios sobre redes públicas.

16.1.1. Análisis y especificación de requisitos de seguridad de la información – *(Control 14.1.1).*

Los requisitos relacionados con la seguridad de la información serán incluidos en los requerimientos para los nuevos sistemas de información o mejoras a los sistemas de información existentes en la ALFM.

Los requerimientos de seguridad de la información deben ser identificados previos al diseño o requisición de soluciones de información e infraestructura.

Antes de la puesta en producción de una aplicación nueva o de la modificación de las plataformas existentes, se debe asignar un número de edición o versión a la misma, cuyo cambio se debe plasmar mediante el **Formato Gestión del Cambio - GI-FO-17.**

Todas las versiones deben ser almacenadas en bibliotecas, repositorios o directorios y deben contar con controles de acceso lógicos donde sólo se permita el acceso al personal autorizado por la Oficina TIC.

Las versiones que se encuentran en los ambientes de producción deben ser verificadas contra la documentación de los controles de cambio con el fin de determinar si los dos son congruentes.

16.1.2. Seguridad de servicios de las aplicaciones en redes públicas – *(Control 14.1.2).*

La información pública producida por la ALFM, deberá estar resguardada de posibles modificaciones que afecten la imagen institucional, de acuerdo con los parámetros y normatividad vigente.

El portal institucional deberá contener la política de privacidad y uso, de acuerdo a la normatividad vigente.

La ALFM deberá garantizar el derecho de Habeas Data y la Ley de transparencia al público que hace uso de los servicios de sus respectivos portales institucionales y propender por la seguridad de la información ingresada a través de ellos, aclarando que la veracidad de la misma es responsabilidad del ciudadano.

Toda la información publicada en el portal institucional por parte de los funcionarios autorizados deben contar con la revisión y aprobación de los Directores, Subdirectores o Jefes de Oficina, quienes serán responsables por la información publicada por los editores web de su dependencia.

La información de los servicios de las aplicaciones que pasan sobre redes públicas se debe proteger de actividades fraudulentas y modificación no autorizadas.

16.1.3. Protección de transacciones de los servicios de las aplicaciones – *(Control 14.1.3).*

La Oficina TIC, brinda mecanismos (SFTP, VPN, Bases de datos de prueba) para que la información de la ALFM involucrada en las transacciones de los servicios de las aplicaciones se proteja para evitar la transmisión incompleta, el enrutamiento errado, la alteración no autorizada de mensajes, la divulgación no autorizada y la duplicación o reproducción no autorizada de mensajes.

La Oficina TIC, debe incluir las consideraciones de seguridad de la información para las transacciones de los servicios de las aplicaciones, entre otras:

El uso de firmas electrónicas por parte de cada una de las partes involucradas en la transacción.

Todos los aspectos de la transacción, deben asegurar que:

A. La información de autenticación secreta de usuario, de todas las partes, se valide y verifique.
B. La transacción permanezca confidencial. Se mantenga la privacidad asociada con todas las partes involucradas.
C. La trayectoria de las comunicaciones entre todas las partes involucradas este cifrada.
D. Los protocolos usados para comunicarse entre todas las partes involucradas sean seguras.
E. El almacenamiento de los detalles de la transacción se realice en un entorno que no sea accesible públicamente, como lo es el almacenamiento existente en la intranet de la ALFM, el cual no debe ser retenido ni expuesto en un medio de almacenamiento accesible directamente desde internet.

16.2. SEGURIDAD EN LOS PROCESOS DE DESARROLLO Y DE SOPORTE – *(Categoría 14.2).*

Objetivo: Asegurar que la seguridad de la información este diseñada e implementada dentro del ciclo de vida de desarrollo de los sistemas de información.

16.2.1. Política de desarrollo seguro – *(Control 14.2.1).*

La Oficina TIC debe aplicar los mismos controles en al ambiente de producción y ambiente de desarrollo, tales como, control de acceso, copias de respaldo, registro de eventos y separación de ambientes (desarrollo y producción).

La Oficina TIC debe implementar los controles necesarios para asegurar que las migraciones entre los ambientes de desarrollo y producción han sido aprobadas, de acuerdo con el **Formato Gestión del Cambio - GI-FO-17.**

La Oficina TIC debe contar con sistemas de control de versiones para administrar los cambios de los sistemas de información de la ALFM.

16.2.2. Procedimientos de control de cambios en sistemas – *(Control 14.2.2).*

Los cambios en los procesos de negocio, en las instalaciones y en los sistemas de procesamiento de información se debe realizar de acuerdo con los lineamientos establecidos en el **Formato Gestión del Cambio - GI-FO-17.**

16.2.3. Revisión técnica de las aplicaciones después de cambios en la plataforma de operación – *(Control 14.2.3).*

Cuando se cambien las plataformas de operación, se debe revisar las aplicaciones críticas de la ALFM, y ponerlas a prueba, para asegurar que no haya impacto adverso en las operaciones o seguridad de la información.

Se debe asegurar que la notificación de los cambios en la plataforma operativa se hace a tiempo, para permitir las pruebas y revisiones apropiadas antes de la implementación.

16.2.4. Restricciones en los cambios a los paquetes de software – *(Control 14.2.4).*

La ALFM debe desalentar las modificaciones a los paquetes de software, los cuales se deben limitar a los cambios necesarios, y todos los cambios serán controlados estrictamente.

16.2.5. Desarrollo contratado externamente – *(Control 14.2.7).*

Cuando se contrata desarrollo externo se debe acordar el cumplimiento de los niveles de soporte requeridos por la ALFM. Adicionalmente, se debe acordar la entrega de manuales técnicos, que describan la estructura interna del sistema, así como el diccionario de datos, librerías ejecutables, entidad relación de la base de datos, manuales funcionales, manual del usuario y manual de instalación, además:

A. Las dependencias deben asegurase que los sistemas de información adquiridos o desarrollados por terceros cuenten con un acuerdo de licenciamiento en el cual se especifiquen las condiciones de uso del software y los derechos de propiedad intelectual.
B. Las dependencias deben exigir el suministro de evidencia de que se realizaron pruebas de seguridad al software desarrollado por terceros.
C. Los principios de desarrollo seguro se deben aplicar, en donde sea pertinente, a desarrollos contratados externamente.
D. Las dependencias que contraten desarrollos externos deben asegurar que se realicen pruebas de aceptación del software, con el fin de verificar el cumplimiento de los requisitos de seguridad acordados.
E. Las dependencias deben tener en cuenta e incluir en los acuerdos contractuales la necesidad de que el software cumpla con las leyes aplicables.

F. Las dependencias deben incluir en acuerdos contractuales, en donde sea posible, el derecho de la ALFM a realizar verificaciones durante el desarrollo del contrato.

16.2.6. Prueba de aceptación de sistemas – *(Control 14.2.9).*

Independientemente de que sea un desarrollo interno o un desarrollo contratado externamente, con el fin de validar los requisitos de seguridad de la información y la adherencia a prácticas de desarrollo de sistemas seguros (en donde sea aplicable). En estas pruebas se puede hacer uso de herramientas automatizadas, tales como herramientas de análisis de códigos o escáneres de vulnerabilidad, y se debe verificar que se han corregido las brechas de seguridad, además:

A. Se debe realizar pruebas de aceptación del software que sea una persona diferente de quien han desarrollado el software, además estas pruebas evidenciadas a través de un documento deben estar firmadas por quienes realizaron las pruebas, en donde se acepte que el software desarrollado cumple con los lineamientos y funcionalidades para su uso.
B. De ser posible, las pruebas se deben llevar a cabo en un ambiente de pruebas realista, para asegurar que el sistema no introducirá vulnerabilidades al ambiente productivo de la ALFM, y que las pruebas son confiables.
C. En donde la funcionalidad de la seguridad no satisface el requisito especificado, antes de comprar el software se debe reconsiderar el riesgo introducido y los controles asociados.

16.3. DATOS DE PRUEBA – *(Categoría 14.3).*

Objetivo: Asegurar la protección de los datos usados para pruebas.

16.3.1. Protección de datos de prueba – *(Control 14.3.1).*

Los datos de prueba que se utilicen en la ALFM serán seleccionados, protegidos y controlados cuidadosamente.

En la ALFM la información operacional clasificada como restringida, se deberá borrar del ambiente de pruebas inmediatamente después de finalizar las pruebas.

17. RELACIONES CON LOS PROVEEDORES – *(Dominio 15).*

17.1. SEGURIDAD DE LA INFORMACIÓN EN LAS RELACIONES CON LOS PROVEEDORES – *(Categoría 15.1).*

Objetivo: Asegurar la protección de los activos de la ALFM que sean accesibles a los proveedores.

17.1.1. Política de seguridad de la información para las relaciones con proveedores – *(Control 15.1.1).*

Cuando exista la necesidad de trabajar con partes externas y se requiera acceso a la información, datos de la entidad, a sus plataformas tecnológicas, sistemas de información, procesamiento de información, o de obtener o suministrar productos y servicios de o para una parte externa, se deberá diligenciar el **Formato Acuerdo de confidencialidad y no divulgación contratistas - GTI-FO-01** y se deberá realizar el diligenciamiento del **Formato Estudio de**

Seguridad Personal - **GA-FO-38** tanto a la empresa como a los funcionarios o empleados de las terceras partes involucradas.

En todos los contratos cuyo objeto sea la prestación de servicios a título personal, bajo cualquier modalidad jurídica, que deban desarrollarse dentro de las instalaciones de la ALFM, se establecerán los controles, requerimientos de seguridad y compromisos de confidencialidad aplicables al caso, restringiendo al mínimo necesario los permisos a otorgar.

En ningún caso se otorgará acceso a terceros a la información, a las instalaciones de procesamiento u otras áreas de servicios críticos, hasta tanto se hayan implementado los controles apropiados y se haya firmado un contrato o acuerdo que defina las condiciones para la conexión o el acceso.

17.1.2. Tratamiento de la seguridad dentro de los acuerdos con proveedores – *(Control 15.1.2).*

Se deben tener en cuenta las responsabilidades derivadas de las leyes nacionales y debe haber restricciones contra la copia y la revelación no autorizada de información institucional.

Se deberá explicar al funcionario, el contratista o usuario de tercera parte sobre las acciones de carácter legal, administrativo, penal, disciplinario o civil, a que puede estar sujeto, si viola u omite el cumplimiento de las normas de seguridad o la violación de la reserva establecida en la entidad.

Los contratos o acuerdos de tercerización total o parcial para la administración y control de sistemas de información, redes e infraestructura, contemplarán como mínimo los siguientes aspectos:

A. Forma en los que se cumplirán los requisitos legales aplicables.
B. Medios para garantizar que todas las partes involucradas en la tercerización incluyendo los subcontratistas, conozcan sus responsabilidades en materia de seguridad.
C. Forma en que se mantendrá y comprobará la integridad y confidencialidad de los activos.
D. Controles físicos y lógicos que se utilizarán para restringir y delimitar el acceso a la información sensible.
E. Forma en que se mantendrá la disponibilidad de los servicios ante la ocurrencia de desastres.
F. Niveles de seguridad física que se asignará al equipamiento tercerizado.
G. Derecho a la verificación por parte de las dependencias de la ALFM.

17.2. GESTIÓN DE LA PRESTACIÓN DE SERVICIOS DE PROVEEDORES – *(Categoría 15.2).*

Objetivo: Mantener el nivel acordado de seguridad de la información y de prestación del servicio en línea con los acuerdos con los proveedores.

17.2.1. Seguimiento y revisión de los servicios de los proveedores – *(Control 15.2.1).*

Cada servicio con proveedor deberá tener un supervisor encargado de revisar y auditar la prestación de servicios de proveedores.

17.2.2. Gestión de cambios en los servicios de los proveedores – *(Control 15.2.2).*

Los cambios en la prestación de servicios por parte de los proveedores, incluyendo el mantenimiento y la mejora de las actuales políticas de seguridad de la información, procedimientos y controles, se gestionarán, teniendo en cuenta la criticidad de la información, sistemas y procesos que intervienen y re-evaluación de los riesgos.

18. GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN – *(Dominio 16).*

18.1. GESTIÓN DE INCIDENTES Y MEJORAS EN LA SEGURIDAD DE LA INFORMACIÓN – *(Categoría 16.1).*

Objetivo: Asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación sobre eventos de seguridad y debilidades.

18.1.1. Responsabilidades y procedimientos – *(Control 16.1.1).*

La priorización del tratamiento de los incidentes se realiza conforme a la criticidad de la información.

Se debe establecer y mantener actualizado un directorio de los encargados de la Gestión de Incidentes de Seguridad de la entidad, el cual será consolidado por la Oficina TIC.

La Oficina TIC deberá difundir el directorio consolidado de los encargados de gestionar los incidentes de seguridad de la ALFM.

Se debe llevar un registro detallado de los incidentes de seguridad de la información y la respuesta que fue implementada.

Se debe propender por la adquisición de herramientas que faciliten el proceso de gestión de incidentes de seguridad de la información.

Los resultados de las investigaciones que involucren a los funcionarios de la ALFM deberán ser informados a las áreas de competencia.

La ALFM deberá establecer los mecanismos de control necesarios para recolectar y preservar la evidencia de las investigaciones que se realicen durante el análisis de un incidente de seguridad de la información.

En caso de presentarse una investigación se deberá realizar seguimiento a los avances de la misma. De igual forma se debe coordinar y establecer los mecanismos de control necesarios para recolectar y preservar la evidencia de las investigaciones que se realicen durante el análisis de un incidente de seguridad de la información.

18.1.2. Reporte de eventos de seguridad de la información – *(Control 16.1.2).*

Los funcionarios, contratistas y terceros deberán informar a la Oficina TIC cualquier situación sospechosa o incidente de seguridad que comprometa la confidencialidad, integridad y/o

disponibilidad de la información, y la Oficina TIC será la encargada de comunicar las novedades a los entes externos y a la alta Dirección de acuerdo a los protocolos establecidos.

18.1.3. Reporte de debilidades de seguridad de la información – *(Control 16.1.3).*

Los funcionarios, contratistas y terceros deberán informar a la Oficina TIC cualquier situación sospechosa o incidente de seguridad que comprometa la confidencialidad, integridad y/o disponibilidad de la información, y la Oficina TIC será la encargada de comunicar las novedades a los entes externos y a la alta Dirección de acuerdo a los protocolos establecidos.

18.1.4. Evaluación de eventos de seguridad de la información y decisiones sobre ellos – *(Control 16.1.4).*

Los eventos de seguridad de la información los evalúa la Oficina TIC e informará a los entes externos y a la alta Dirección de acuerdo a los protocolos establecidos.

Todos los incidentes informáticos deben ser reportados y se deberá adelantar un análisis con un informe escrito y detallado que identifique el incidente, los resultados, acciones tomadas y recomendaciones, el cual debe ser presentado a la alta Dirección.

18.1.5. Respuesta a incidentes de seguridad de la información – *(Control 16.1.5).*

La Oficina TIC, debe responder a los incidentes de la información que se presenten en la ALFM, donde se debe incluir lo siguiente:

A. Recolección de evidencia lo más pronto posible después de que ocurra el incidente.
B. Llevar a cabo un análisis de seguridad de la información, en caso de requerirse.
C. Escalar el incidente a una instancia superior, en caso de requerirse.
D. Asegurarse de que todas las actividades de respuesta involucradas se registren adecuadamente para un análisis posterior.
E. Comunicar la existencia del incidente de seguridad de la información o de cualquier detalle pertinente a él, al personal interno o externo a las organizaciones que necesitan saberlo.
F. Tratar las debilidades de seguridad de la información que se encontraron y que causan o contribuyen al incidente.
G. Una vez que el incidente que haya tratado lo suficiente, cerrarlo formalmente y hacer un registro de esto.

18.1.6. Aprendizaje obtenido de los incidentes de seguridad de la información – *(Control 16.1.6).*

Los conocimientos adquiridos en la ALFM a partir del análisis y la resolución de incidentes de seguridad de información se deben utilizar para reducir la probabilidad o el impacto de los incidentes en el futuro.

18.1.7. Recolección de evidencia – *(Control 16.1.7).*

La ALFM debe definir y aplicar procedimientos para la identificación, recolección, adquisición y conservación de la información, que puede servir como evidencia.

19. ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE CONTINUIDAD DE NEGOCIO – *(Dominio 17)*

19.1. CONTINUIDAD DE SEGURIDAD DE LA INFORMACIÓN – *(Categoría 17.1).*

Objetivo: La continuidad de seguridad de la información se deberá incluir en los sistemas de gestión de continuidad del negocio de la ALFM.

19.1.1. Planificación de la continuidad de la seguridad de la información – *(Control 17.1.1).*

La seguridad de la información es una prioridad y se incluye como parte de la gestión general de la continuidad y del compromiso de la Alta Dirección.

La ALFM deberá contar con un Plan de Continuidad que asegure la operación de los procesos críticos ante la ocurrencia de eventos no previstos o desastres naturales como sismos, terremotos, tsunami, etc.

Para la ALFM su activo más importante es el recurso humano y por lo tanto será su prioridad y objetivo principal, establecer las estrategias para mantenerlo.

Los niveles de recuperación mínimos requeridos, así como los requerimientos de seguridad, funciones, responsabilidades, estarán incorporados y definidos en el Plan de Continuidad del negocio de la ALFM.

Los responsables de los procesos serán los encargados de mantenerlos documentados y actualizados.

19.1.2. Implementación de la continuidad de la seguridad de la información – *(Control 17.1.2).*

La ALFM debe seguir una estrategia de recuperación alineada con los objetivos, formalmente documentada y con procedimientos perfectamente probados para asegurar la restauración de los procesos críticos del negocio, ante cualquier contingencia de acuerdo a los lineamientos del Plan de Continuidad de la ALFM.

La ALFM deberá establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel de continuidad requerido para la seguridad de la información durante una situación adversa.

19.1.3. Verificación, revisión y evaluación de la continuidad de la seguridad de la información – *(Control 17.1.3).*

La ALFM debe verificar la información de continuidad de los controles de seguridad establecidos y aplicados a intervalos regulares con el fin de asegurarse que son válidos y eficaces en situaciones adversas.

19.2. REDUNDANCIAS – *(Categoría 17.2)*

Objetivo: Asegurar la disponibilidad de instalaciones de procesamiento de información

19.2.1. Disponibilidad de instalaciones de procesamiento de información – *(Control 17.2.1).*

Las instalaciones para el procesamiento de información deben cumplir con algunos de los lineamientos que rigen los centros de datos y de acuerdo a los controles antes relacionados en este documento.

20. CUMPLIMIENTO – *(Dominio 18).*

20.1. CUMPLIMIENTO DE REQUISITOS LEGALES Y CONTRACTUALES – *(Categoría 18.1).*

Objetivo: Evitar el incumplimiento de las obligaciones legales, estatutarias, de reglamentación o contractuales relacionadas con seguridad de la información y de cualquier requisito de seguridad.

20.1.1. Identificación de la legislación aplicable y de los requisitos contractuales. – *(Control 18.1.1).*

Todos los requisitos pertinentes, legislativos estatutarios, reglamentarios y contractuales, y el planteamiento de la ALFM para cumplir con estos requisitos deberán estar explícitamente identificados, documentados y protegidos al día para cada sistema de información y la entidad.

20.1.2. Derechos de propiedad intelectual – *(Control 18.1.2).*

La ALFM cumplirá con la reglamentación vigente sobre propiedad intelectual, para lo cual implementarán los controles necesarios que garanticen el acatamiento de dicha reglamentación.

No se permite el almacenamiento, descarga de internet, intercambio, uso, copia, reproducción y/o instalación de software no autorizado, música, videos, documentos, textos, fotografías, gráficas y demás obras protegidas por derechos de propiedad intelectual, que no cuenten con la debida licencia o autorización legal.

Se permite el uso de documentos, cifras y/o textos de carácter público siempre y cuando se cite al autor de los mismos con el fin de preservar los derechos morales e intelectuales de las obras o referencias citadas.

Los procesos de adquisición de aplicaciones y paquetes de software deben cumplir con los requerimientos y obligaciones derivados de las leyes de propiedad intelectual y derechos de autor.

El software a la medida, adquirido a terceras partes que correspondan a desarrollos a la medida al igual que los desarrollos que tenga participación de funcionarios de la ALFM, debe quedar registrado ante la Dirección Nacional de Derechos de Autor (DNDA).

Todo el material que es desarrollado mientras se trabaja para la ALFM se considera que es de propiedad intelectual y de uso exclusivo de la entidad.

Se debe establecer en los contratos de trabajo cláusulas sobre la propiedad intelectual de la ALFM sobre el material y los trabajos generados por los funcionarios y/o terceros en desarrollo de sus funciones y/o actividades en la ALFM.

20.1.3. Protección de registros – *(Control 18.1.3).*

Los registros en los sistemas de información se deben proteger contra pérdida, destrucción, falsificación, acceso no autorizado y liberación no autorizada, de acuerdo con los registros legislativos, reglamentación contractual y comercial.

20.1.4. Privacidad y protección de información de datos personales – *(Control 18.1.4).*

La ALFM en los procesos y aplicativos que requieran datos personales de usuarios, informa 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.

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.

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.

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

A. 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.
B. Cuando se trate de datos de naturaleza pública.
C. En casos de emergencia médica o sanitaria.

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

A. 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.
B. Mantener las condiciones de seguridad necesarias para impedir la adulteración, manipulación, pérdida, consulta, uso o acceso no autorizado o fraudulento de los datos personales.
C. Realizar oportunamente la actualización, rectificación o supresión de los datos en los términos señalados en la Ley 1581 de 2012.
D. Tramitar las consultas y reclamos formulados por los titulares en los términos señalados en la Ley 1581 de 2012.

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.

Cuando sea aplicable, se debe asegurar la privacidad y protección de la información de datos personales, como exige la legislación y la reglamentación pertinente.

20.2. REVISIONES DE SEGURIDAD DE LA INFORMACIÓN – *(Categoría 18.2).*

Objetivo: Asegurar que la seguridad de la información se implemente y opere de acuerdo con las políticas y procedimientos Institucionales.

20.2.1. Revisión independiente de la seguridad de la información – *(Control 18.2.1).*

El enfoque de la entidad para la gestión de seguridad de la información y su aplicación (es decir, los objetivos de control, políticas, procesos y procedimientos para la seguridad de la información) se revisará de forma independiente a intervalos planificados o cuando se produzcan cambios significativos.

20.2.2. Cumplimiento con las políticas y normas de seguridad – *(Control 18.2.2).*

Los Directores, Subdirectores y Jefes de Oficina deben revisar con regularidad el cumplimiento del procesamiento y procedimientos de información dentro de su área de responsabilidad, con las políticas y normas de seguridad apropiadas, y cualquier otro requisito de seguridad.

20.2.3. Revisión del cumplimiento técnico – *(Control 18.2.3).*

Los sistemas de información de la ALFM se deben revisar periódicamente para determinar el cumplimiento con las políticas y normas de seguridad de la información.

21. INSTRUCCIONES GENERALES DE COORDINACIÓN

El cumplimiento de la Política de Seguridad de la Información con sus respectivas normas es de obligatorio cumplimiento en la ALFM.

Cada funcionario, contratista y tercero de la ALFM, debe entender su rol y asumir su responsabilidad respecto a los riesgos en seguridad de la información y la protección de los activos de información de la entidad.

Cualquier incumplimiento de esta Política que resulte comprometiendo la Confidencialidad, Integridad y Disponibilidad, resultará en una acción disciplinaria o de un proceso judicial bajo las leyes nacionales o internacionales que apliquen.

La Política de Seguridad de la Información está basada en las mejores prácticas en seguridad de la información y está acorde con la legislación nacional e internacional y por ende la ALFM seguirá el debido proceso, incluyendo las medidas legales aplicables, para proteger sus activos de información y el uso correcto de ellos.

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, por lo cual deben conocer y aplicar los lineamientos específicos contenidos en la presente Política de Seguridad de la Información.

VERSIÓN	DESCRIPCIÓN DE CAMBIOS
00	Versión inicial.
01	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.
02	Adición de normatividad aplicable. Adición y eliminación de definiciones del glosario. Ordenamiento alfabético de las definiciones. Revisión de redacción a las políticas que aplique.
03	Actualización nombre del documento “Manual Políticas de la seguridad de la información”. Adición de normatividad vigente. Adición y eliminación de definiciones del glosario. Actualización objetivos del manual (General y específicos). Actualización alcance. Adición principios de seguridad de la información. Actualización, creación y/o eliminación de dominios, categorías y controles de seguridad de la información.