DESTINAR FONDO MUTUO DE AHORRO E INVERSION.

POLITICA DE SEGURIDAD DE LA INFORMACION

INTRODUCCION 5
1. Objetivo de la política de seguridad de la información 7
1.1 Objetivos específicos 7
1.2 Alcance 7
1.3 Organización y Responsabilidades 8
1.3.1 Gerencia 8
1.3.2 Líder de Seguridad de la Información (Analista de TI) 8
1.4 Cumplimiento y manejo de violaciones a la política 9
1.4.1 Propiedad Intelectual 9
1.4.2 Cumplimiento Legal y de Regulaciones 9
1.5 TÉRMINOS Y DEFINICIONES 10
2. LINEAMIENTOS GENERALES 15
2.1 El uso responsable de los Recursos 15
2.2 Responsabilidad del Usuario ante Procedimientos Administrativos 16
2.3 Las Autorizaciones 16
2.3.1 Autorización de acceso 16
2.3.2 Identificaciones de usuarios 16
2.3.3 Las contraseñas 16
2.3.4 La propiedad de los datos 17
2.4 Los Dispositivos de red 17
2.4.1 Los Dispositivos no autorizados 17
2.4.2 Utilización del Computador 17
2.5 El Hacking 18
2.6 Usos Prohibidos 19
2.7 Consideraciones Generales de Seguridad 20
3. POLÍTICAS, PROCEDIMIENTOS Y CONTROLES 22
3.1 Política general de seguridad de la información 22
3.2 Política para uso de dispositivos móviles 23
3.3 Responsabilidad de la Administración de Seguridad 25
3.4 Asignación De Derechos De Propiedad Intelectual 25

3.5 Ley de Derechos de Autor 26
3.6 Información Privada de Afiliados y Empresas Patrocinadoras 26
3.7 Instalación de Software 27
3.8 Política de uso de los activos 27
3.9 Envío de Información Privada por Correo Electrónico 30
3.10 Circular Externa 038 de 2009 de la Superfinanciera 31
3.11 Aspectos de Seguridad en Los Contratos con Terceros 31
3.12 Análisis de Riesgos 32
3.13 Seguros para los Recursos TI 32
3.14 Clasificación de la información. 33
3.15 Rotulado de medios de almacenamiento. 33
3.16 Contraseñas de Cifrado 34
3.17 Borrado Seguro o Destrucción de Medios 34
3.18 Aviso de Confidencialidad en Los Correos Electrónicos 34
3.19 Cumplimiento de las Políticas de Seguridad de la Información 35
3.20 Política de tratamiento de datos personales 35
3.21 Política de uso de estaciones cliente 36
3.22 Política de uso de Internet. 37
3.23 Política de clasificación de la información. 38
3.24 Política de manejo disposición de información, medios y equipos 39
3.25 Política de control de acceso 40
3.26 Política de establecimiento, uso y protección de claves de acceso 41
3.27 Política de uso de discos de red o carpetas virtuales. 42
3.28 Política de uso de puntos de red de datos (red de área local – LAN). 43
3.29 Política de uso de impresoras y del servicio de Impresión 44
3.30 Política de controles criptográficos 45
3.31 Política de Seguridad Física 46
3.32 Políticas de seguridad de los Equipos 46
3.33 Política de escritorio y pantalla limpia. 48
3.34 Política de respaldo y restauración de información 49
3.35 Política de registro y seguimiento de eventos de sistemas de información y comunicaciones 51

3.36 Política de uso de correo electrónico 52
3.37 Políticas específicas para el rol de Webmaster..... 53
3.38 Políticas específicas para funcionarios y contratistas del Área de Tecnología y Sistemas de la Información..... 54
3.39 Política de Tercerización u Outsourcing. 55
3.40 Política de Gestión de los Incidentes de la Seguridad de la Información..... 57
3.41 Política para la Gestión de la Continuidad de Seguridad de la Información..... 57
3.42 Política de uso de mensajería instantánea y redes sociales. 58
4. Proceso Disciplinario..... 59

INTRODUCCION

¿Qué es la seguridad de la información?

DESTINAR determina la información como un activo de alta importancia para la entidad que permite el desarrollo continuo de 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. El presente manual se establece las políticas de seguridad de la información las cuales deben ser adoptadas por los funcionarios, contratistas, personal en comisión administrativa, visitantes y terceros que presten sus servicios o tengan algún tipo de relación con Destinar; estas se encuentran enfocadas al cumplimiento de la normatividad legal Colombiana vigente y a las buenas prácticas de seguridad de la información, basadas en la norma ISO 27001/2013.

La seguridad de la información se define aquí como la preservación de las siguientes características:

a) *confidencialidad:* se garantiza que la información sea accesible sólo a aquellas personas autorizadas a tener acceso a ella.
b) *integridad:* se salvaguarda la exactitud y totalidad de la información y los métodos de procesamiento.
c) *disponibilidad:* se garantiza que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con ella toda vez que se requiera.

Criterios de Calidad de la información

a) *Efectividad:* La información relevante debe ser pertinente y su entrega oportuna, correcta y consistente.
b) *Eficiencia*: El procesamiento y suministro de información debe hacerse utilizando de la mejor manera posible los recursos.
c) *Confiabilidad:* La información debe ser la apropiada para la administración de la entidad y el cumplimiento de sus obligaciones.

Por qué es necesaria la seguridad de la información

La información y los procesos, sistemas y redes que le brindan apoyo constituyen importantes recursos de la empresa. La confidencialidad, integridad y disponibilidad de la información pueden ser esenciales para mantener la ventaja competitiva, el flujo de fondos, la rentabilidad, el cumplimiento de las leyes y la imagen comercial.

Las organizaciones, sus redes y sistemas de información, se enfrentan en forma creciente con amenazas relativas a la seguridad, de diversos orígenes, incluyendo el fraude asistido por computadora, espionaje, sabotaje, vandalismo, incendio o inundación. Daños tales como los

ataques mediante virus informáticos, "hacking" y denegación de servicio se han vuelto más comunes, ambiciosos y crecientemente sofisticados. Es de anotar que las entidades financieras, son el primer objetivo, para ser blancos de cibercrimenes.

La administración de la seguridad de la información, exige, compromiso y participación de todos los empleados de la organización. También puede requerir la participación de proveedores, clientes y accionistas.

1. Objetivo de la política de seguridad de la información

Establecer las políticas que regulan la seguridad de la información en Destinar y presentar en forma clara y coherente los elementos que conforman la política de seguridad que deben conocer, acatar y cumplir todos los directivos, funcionarios, contratistas y terceros que presten sus servicios o tengan algún tipo de relación con Destinar, bajo el liderazgo del Área de Tecnología y Sistemas de la Información.

1.1 Objetivos específicos

Los objetivos específicos de la Política de Seguridad de la Información son:

a) Preservar La confidencialidad e integridad de la información independientemente del medio o formato donde se almacene y/o la forma en que se transmita.

b) Especificar la mejor practica para el acceso, uso, manejo y administración de los recursos de información.

c) Establecer las responsabilidades en el uso de los activos de información, que apoyan los procesos del negocio.

d) Administrar los riesgos en Seguridad de la Información y las medidas tomadas para su mitigación y corrección.

e) Garantizar que la privacidad de la información de Fondo Mutuo de Inversión debe ser preservada.

f) Estandarizar los métodos de comunicación segura y el intercambio de información con terceras partes.

g) Definir los métodos que eviten la divulgación, modificación, hurto o destrucción accidental o maliciosa de la información

1.2 Alcance

Las Políticas de Seguridad de la Información son aplicables para todos los aspectos administrativos y de control que deben ser cumplidos por los directivos, funcionarios, contratistas y terceros que presten sus servicios o tengan algún tipo de relación con Destinar FMI, para el adecuado cumplimiento de sus funciones y para conseguir un adecuado nivel de protección de las características de calidad y seguridad de la información, aportando con su participación en la toma de medidas preventivas y correctivas, siendo un punto clave para el logro del objetivo y la finalidad de dicho manual. Los usuarios tienen la obligación de dar cumplimiento a las presentes políticas emitidas y aprobadas por Destinar. Adicionalmente esta Política aplica a toda la información creada, procesada o utilizada para soporte del negocio, sin importar el medio, formato, presentación o lugar en el que se encuentre.

1.3 Organización y Responsabilidades

La responsabilidad de la administración de esta Política es de los siguientes comités y personas:

1.3.1 Gerencia

El primer responsable de la seguridad de la información es el Gerente de la compañía, él debe asegurar que exista y se aplique la política de seguridad, como también:

a) Inclusión de la seguridad en las responsabilidades en los puestos de trabajo.
b) Selección y política de personal.
c) Acuerdos de confidencialidad o no divulgación
d) Términos y condiciones de empleo
e) Capacitación al usuario
f) Designar Comité y Líder de seguridad
g) Disponer de los medios necesarios para asegurarse que cada miembro de la Comunidad preserve y proteja los activos de información de una manera consistente y confiable.

1.3.2 Líder de Seguridad de la Información (Analista de TI)

Es la persona responsable por asegurar la planeación, implantación y mantenimiento de la Política de Seguridad de la Información; al igual que la ejecución y reporte oportuno a la alta gerencia de las acciones requeridas para mantener los niveles de seguridad establecidos. Esta persona debe promover la seguridad dentro de la organización mediante un adecuado compromiso y una apropiada asignación de recursos, y debe:

a) revisar y aprobar la política y las responsabilidades generales en materia de seguridad de la información;
b) monitorear cambios significativos en la exposición de los recursos de información frente a las amenazas más importantes;
c) revisar y monitorear los incidentes relativos a la seguridad;
d) aprobar las principales iniciativas para incrementar la seguridad de la información.

NOTA: El analista de TI hará las funciones del Líder de Seguridad de la Información

La Comunidad

La Comunidad está conformada por todas las personas que directa o indirectamente de manera legítima y por el cumplimiento de sus funciones administran, acceden, consultan, custodian o procesan información que Destinar FMI utiliza para el desarrollo del negocio. Se incluyen las siguientes personas o entidades en La Comunidad:

- Miembros de Junta Directiva, Empleados incluidos regionales, Afiliados, Terceros: proveedores y contratistas, Entes de Control, Entidades.

La Comunidad es responsable de proteger los activos de información de Destinar FMI, por medio del cumplimiento de la Política de Seguridad de la información. Así mismo, deben estar alerta para identificar y reportar cualquier incidente de seguridad o incumplimiento a las normas y procedimientos establecidos.

1.4 Cumplimiento y manejo de violaciones a la política

El cumplimiento de La Política de Seguridad de la Información con sus respectivas normas es obligatorio. Cada miembro de la Comunidad 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 Destinar FMI.

Cualquier incumplimiento de esta Política que resulte comprometiendo la Confidencialidad, Integridad, Disponibilidad y/o Privacidad de la información resultará en una acción disciplinaria (*Ver numeral 4 de este misma política*) que puede llegar hasta la terminación del contrato de trabajo con justa causa y a un posible establecimiento 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 DESTINAR FMI seguirá el debido proceso, incluyendo las medidas legales aplicables, para proteger sus activos y el uso de ellos.

1.4.1 Propiedad Intelectual

La Propiedad Intelectual se define como cualquier patente, derecho de autor, invención o información que es propiedad de Destinar FMI.

Todo el material que es desarrollado mientras se trabaja para DESTINAR FMI se considera que es de propiedad intelectual y de uso exclusivo de DESTINAR FMI.

1.4.2 Cumplimiento Legal y de Regulaciones

DESTINAR FMI, debe cumplir con las regulaciones locales e internacionales de Privacidad y Seguridad de la Información, y con responsabilidades contractuales con terceros. Además debe velar que en los contratos se asigne responsabilidad a los terceros del cumplimiento de la Política de Seguridad de la Información.

1.5 TÉRMINOS Y DEFINICIONES

Acción correctiva: Remediación de los requisitos o acciones que dieron origen al establecimiento de no una conformidad, de tal forma que no se vuelva a presentar.

Acción preventiva: Disposición de operaciones que buscan de forma preliminar, que no se presente en su ejecución, desarrollo e implementación una no conformidad.

Aceptación del Riesgo: Después de revisar las consecuencias que puede acarrear el riesgo, se toma la decisión de afrontarlo.

Activo: Según [ISO/IEC 13335-12004]: Cualquier cosa que tiene valor para la organización. También se entiende por cualquier información o sistema relacionado con el tratamiento de la misma que tenga valor para la organización. Es todo activo que contiene información, la cual posee un valor y es necesaria para realizar los procesos misionales y operativos de DESTINAR FMI. Se pueden clasificar de la siguiente manera:

a) Datos: Son todos aquellos elementos básicos de la información (en cualquier formato) que se generan, recogen, gestionan, transmiten y destruyen en DESTINAR.
b) Aplicaciones: Es todo el software que se utiliza para la gestión de la información.
c) Personal: Es todo el personal de DESTINAR, el personal subcontratado, los afiliados, usuarios y en general, todos aquellos que tengan acceso de una manera u otra a los activos de información del DESTINAR FMI.
d) Servicios: Son tanto los servicios internos, aquellos que una parte de la organización suministra a otra, como los externos, aquellos que la organización suministra a afiliados y proveedores..
e) Tecnología: Son todos los equipos utilizados para gestionar la información y las comunicaciones.
f) Instalaciones: Son todos los lugares en los que se alojan los sistemas de información.

Administración de riesgos: Gestión de riesgos, es un enfoque estructurado para manejar la incertidumbre relativa a una amenaza, a través, de una secuencia de actividades humanas que incluyen evaluación, manejo y mitigación del riesgo utilizando recursos de DESTINAR FMI. Las estrategias incluyen transferir el riesgo a otra parte, evadir el riesgo, reducir los efectos negativos del riesgo y aceptar algunas o todas las consecuencias de un riesgo particular.

Administración de incidentes de seguridad: Procedimientos, estrategias y herramientas de control, enfocados a una correcta evaluación de las amenazas existentes, en este caso hacia toda la infraestructura de TI, se basa en un análisis continuo y mejorado del desempeño de todos los activos y recursos gerenciales que tiene la entidad. Su objetivo principal es atender y orientar las acciones inmediatas para solucionar cualquier situación que cause una interrupción de los diferentes servicios que presta la entidad, de manera rápida y eficaz. No se limita a la solución de problemas específicos sino a buscar las causas que determinaron el incidente limitando el marco de acción de futuras ocurrencias, su enfoque se base en tres pilares fundamentales:

• Detectar cualquier alteración en los servicios TI.
• Registrar y clasificar estas alteraciones.

• Asignar el personal encargado de restaurar el servicio.

Alcance: Ámbito de la organización que queda sometido al Sistema de Gestión de Seguridad de la Información - SGSI. Debe incluir la identificación clara de las dependencias, interfaces y límites con el entorno, sobre todo si sólo incluye una parte de la organización.

Alerta: Una notificación formal de que se ha producido un incidente relacionado con la seguridad de la información que puede evolucionar hasta convertirse en desastre.

Amenaza: Según [ISO/IEC 13335-1:2004): causa potencial de un incidente no deseado, el cual puede causar el daño a un sistema o la organización.

Análisis de riesgos: Según [ISO/IEC Guía 73:2002): Uso sistemático de la información para identificar fuentes y estimar el riesgo.

Auditabilidad: Los activos de información deben tener controles que permitan su revisión. Permitir la reconstrucción, revisión y análisis de la secuencia de eventos.

Auditor: Persona encargada de verificar, de manera independiente, la calidad e integridad del trabajo que se ha realizado en un área particular.

Auditoria: Proceso planificado y sistemático en el cual un auditor obtiene evidencias objetivas que le permitan emitir un juicio informado sobre el estado y efectividad del SGSI de una organización.

Autenticación: Proceso que tiene por objetivo asegurar la identificación de una persona o sistema.

Autenticidad: Los activos de información solo pueden estar disponibles verificando la identidad de un sujeto o recurso, es la propiedad que garantiza que la identidad de un sujeto o recurso es la que declara y se aplica a entidades tales como usuarios, procesos, sistemas de información. Base de datos de gestión de configuraciones

COBIT - Control Objectives for Information and related Technology: – (Objetivos de Control para la información y Tecnologías Relacionadas): es el marco aceptado internacionalmente como una buena práctica para el control de la información, TI y los riesgos que conllevan. **COBIT** se utiliza para implementar el gobierno de IT y mejorar los controles de IT.

Computo forense: El cómputo forense, también llamado informática forense, computación forense, análisis forense digital o examinación forense digital, es la aplicación de técnicas científicas y analíticas especializadas a infraestructura tecnológica que permiten identificar, preservar, analizar y presentar datos que sean válidos dentro de un proceso legal.

Confiabilidad: Se puede definir como la capacidad de un producto de realizar su función de la manera prevista, De otra forma, la confiabilidad se puede definir también como la probabilidad en que un producto realizará su función prevista sin incidentes por un período de tiempo especificado y bajo condiciones indicadas.

Confidencialidad: Acceso a la información por parte únicamente de quienes estén autorizados, Según [ISO/IEC 13335-1:2004]:" característica/propiedad por la que la información no está disponible o revelada a individuos, entidades, o procesos no autorizados.

Control: son todas aquellas políticas, procedimientos, prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido, (Nota: Control es también utilizado como sinónimo de salvaguarda).

Denegación de servicios: Acción iniciada por agentes externos (personas, grupos, organizaciones) con el objetivo de imposibilitar el acceso a los servicios y recursos de una organización durante un período indefinido de tiempo. La mayoría de ocasiones se busca dejar fuera de servicio los servidores informáticos de una compañía o en su defecto en situaciones más complejas ocasionar graves daños, para que no puedan utilizarse ni consultarse servicios importantes.

Desastre: Cualquier evento accidental, natural o malintencionado que interrumpe las operaciones o servicios habituales de una organización durante el tiempo suficiente como para verse afectada de manera significativa.

DESTINAR FMI: Destinar Fondo Mutuo de Ahorro e Inversión.

Disponibilidad: Según [ISO/IEC 13335-1: 2004): característica o propiedad de permanecer accesible y disponible para su uso cuando lo requiera una entidad autorizada.

Evaluación de riesgos: Según [ISO/IEC Guía 73:2002]: proceso de comparar el riesgo estimado contra un criterio de riesgo dado con el objeto de determinar la importancia del riesgo.

Evento: Según [ISO/IEC TR 18044:2004]: Suceso identificado en un sistema, servicio o estado de la red que indica una posible brecha en la política de seguridad de la información o fallo de las salvaguardas, o una situación anterior desconocida que podría ser relevante para la seguridad.

Gestión de claves: Controles referidos a la gestión de claves criptográficas. Gestión de riesgos: Proceso de identificación, control y minimización o eliminación, a un coste aceptable, de los riesgos que afecten a la información de la organización. Incluye la valoración de riesgos y el tratamiento de riesgos. Según [ISO/IEC Guía 73:2002]: actividades coordinadas para dirigir y controlar una organización con respecto al riesgo.

Impacto: Resultado de un incidente de seguridad de la información.

Incidente: Evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.

Información: La información constituye un importante activo, esencial para las actividades de una organización y, en consecuencia, necesita una protección adecuada. La información puede

existir de muchas maneras, es decir, puede estar impresa o escrita en papel, puede estar almacenada electrónicamente, ser transmitida por correo o por medios electrónicos, se la puede mostrar en videos, o exponer oralmente en conversaciones.

Ingeniería Social: Es la manipulación de las personas para conseguir que hagan que algo debilite la seguridad de la red o faciliten información con clasificación confidencial o superior. En el campo de la seguridad informática, es un método o forma de ataque con técnicas que buscan persuadir al atacado ganando su confianza, obteniendo información privilegiada de carácter personal (contraseñas de cuentas bancarias, datos personales), igualmente apropiarse de información vital para una organización. Existen en la actualidad diversidad de medios para llevar a cabo esta actividad, un uso común es a través, de correos electrónicos o llamadas al lugar de trabajo o residencia, de ahí la importancia de tener una buena cultura digital respecto a que información suministramos.

Integridad: propiedad/característica de salvaguardar la exactitud y completitud de los activos.

Inventario de activos: Lista de todos aquellos recursos (físicos, de información, software, documentos, servicios, personas, reputación de la organización, etc.) dentro del alcance del SGSI, que tengan valor para la organización y necesiten por tanto ser protegidos de potenciales riesgos.

IPS: Sistema de prevención de intrusos. Es un dispositivo que ejerce el control de acceso en una red informática para proteger a los sistemas computacionales de ataques y abusos.

ISO 17799: Código de buenas prácticas en gestión de la seguridad de la información adoptado por ISO (Organización Internacional de Normalización).

Keyloggers: Usualmente puede ser un tipo de software o un dispositivo hardware que se encarga de registrar las pulsaciones que se hacen con el teclado, para posteriormente memorizarlas en un archivo o enviarlas a través de internet.

No conformidad: Situación aislada que, basada en evidencias objetivas, demuestra el incumplimiento de algún aspecto de un requerimiento de control que permita dudar de la adecuación de las medidas para preservar la confidencialidad, integridad o disponibilidad de información sensible, o representa un riesgo menor.

No conformidad grave: Ausencia o fallo de uno o varios requerimientos de la ISO 27001 que, basada en evidencias objetivas, permita dudar seriamente de la adecuación de las medidas para preservar la confidencialidad, integridad o disponibilidad de información sensible, o representa un riesgo inaceptable.

No repudio: Los activos de información deben tener la capacidad para probar que una acción o un evento han tenido lugar, de modo que tal evento o acción no pueda ser negado posteriormente.

PDCA Plan-Do-Check-Act: Modelo de proceso basado en un ciclo continuo de las actividades de planificar (establecer el SGSI), realizar (implementar y operar el SGSI), verificar (monitorizar y revisar el SGSI) y actuar (mantener y mejorar el SGSI).

Phishing: Tipo de delito encuadrado dentro del ámbito de las estafas, que se comete mediante el uso de un tipo de ingeniería social caracterizado por intentar adquirir información confidencial de forma fraudulenta (como puede ser una contraseña o información detallada sobre tarjetas de crédito u otra información bancaria), mediante una aparente comunicación oficial electrónica.

Plan de continuidad del negocio (Bussines Continuity Plan): Plan orientado a permitir la continuación de las principales funciones de la Entidad en el caso de un evento imprevisto que las ponga en peligro.

Plan de tratamiento de riesgos (Risk treatment plan): Documento de gestión que define las acciones para reducir, prevenir, transferir o asumir los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma.

Política de seguridad: Documento que establece el compromiso de la Dirección y el enfoque de la organización en la gestión de la seguridad de la información.

Riesgo: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Según [ISO Guía 73:2002]: combinación de la probabilidad de un evento y sus consecuencias.

Segregación de tareas: Separar tareas sensibles entre distintos funcionarios o contratistas para reducir el riesgo de un mal uso de los sistemas e informaciones deliberado o por negligencia.

Seguridad de la información: Preservación de la confidencialidad, integridad y disponibilidad de la información; además, otras propiedades como autenticidad, responsabilidad, no repudio, trazabilidad y fiabilidad pueden ser también consideradas.

Selección de controles: Proceso de elección de los controles que aseguren la reducción de los riesgos a un nivel aceptable.

SGSI Sistema de Gestión de la Seguridad de la Información: Según [ISO/IEC 27001: 20005]: la parle de un sistema global de gestión que, basado en el análisis de riesgos, establece, implementa, opera, monitoriza, revisa, mantiene y mejora la seguridad de la información. (Nota: el sistema de gestión incluye una estructura de organización, políticas, planificación de actividades, responsabilidades, procedimientos, procesos y recursos.)

Spamming: Se llama spam, correo basura o sms basura a los mensajes no solicitados, habitualmente de tipo publicitario, enviados en grandes cantidades (incluso masivas) que perjudican de alguna o varias maneras al receptor. La acción de enviar dichos mensajes se denomina spamming. La vía más usada es el correo electrónico.

Sniffers: Programa de captura de las tramas de red. Generalmente se usa para gestionar la red con una finalidad docente o de control, aunque también puede ser utilizado con fines maliciosos.

Spoofing: Falsificación de la identidad origen en una sesión: la identidad es por una dirección IP o Mac Address.

Tratamiento de riesgos: Proceso de selección e implementación de medidas para modificar el riesgo.

Trazabilidad: Propiedad que garantiza que las acciones de una entidad se puede rastrear únicamente hasta dicha entidad.

Troyano: Aplicación que aparenta tener un uso legítimo pero que tiene funciones ocultas diseñadas para sobrepasar los sistemas de seguridad.

Usuario: en el presente documento se emplea para referirse a directivos, funcionarios, contratistas, terceros y otros colaboradores de DESTINAR FMI, debidamente autorizados para usar equipos, sistemas o aplicativos informáticos disponibles en la red de DESTINAR y a quienes se les otorga un nombre de usuario y una clave de acceso.

Valoración de riesgos: Proceso completo de análisis y evaluación de riesgos.

Virus: Programas informáticos de carácter malicioso, que buscan alterar el normal funcionamiento de una red de sistemas o computador personal, por lo general su acción es transparente al usuario y este tarda tiempo en descubrir su infección; buscan dañar, modificar o destruir archivos o datos almacenados.

Vulnerabilidad: Debilidad en la seguridad de la información de una organización que puede ser explotado por una amenaza.

2. LINEAMIENTOS GENERALES

2.1 El uso responsable de los Recursos

Los recursos informáticos son recursos compartidos que proporcionan los servicios vitales a nuestra institución. Por consiguiente, se espera que el personal que utilice estos recursos informáticos lo haga de manera responsable, incluyendo el cuidado físico de los mismos. Aún en los casos en que estos recursos hayan sido asignados por préstamo, al estar conectados a la red, cada usuario es solidariamente responsable por los daños y perjuicios que su mal uso cause a la red institucional.

2.2 Responsabilidad del Usuario ante Procedimientos Administrativos

Los usuarios son responsables de entender y seguir los procedimientos administrativos establecidos para la utilización y el mantenimiento de dichos recursos. Los usuarios también son responsables de informarse y seguir las directivas administrativas comunicadas por mail u otros medios de información implementados o a implementarse.

2.3 Las Autorizaciones

2.3.1 Autorización de acceso

La autorización para el acceso personal al equipamiento de conectividad y a los servidores de datos debe ser gestionada ante el Analista de TI y deberá contar con la autorización expresa del mismo. Después que la autorización es otorgada, el encargado pondrá el recurso solicitado a disposición del usuario. Los usuarios no pueden acceder a ningún recurso informático hasta que les sea autorizado propiamente. No se permite la utilización de ningún usuario anónimo.

A menos que sea especificado, la autorización de acceso a los recursos es exclusiva al usuario al que le fue asignada y no es transferible a otros usuarios o dispositivos.

2.3.2 Identificaciones de usuarios

Computadores Portátiles, de escritorio y dispositivos móviles deben ser autorizadas para usar cualquier puerto de la red.
El mal uso de la identidad de un usuario o un dispositivo constituye falsificación o falsedad. Las acciones que involucren accesos desautorizados, impropios o el mal uso de recursos informáticos de Destinar Fondo Mutuo de Inversión están sujetas a sanciones disciplinarias.

2.3.3 Las contraseñas

Política	Identificación y Autenticación.
Título	Identificación y Autenticación de Usuarios.
Objetivo	Identificar y autenticar a las personas o programas que local o remotamente utilicen los recursos de información de Destinar Fondo Mutuo de Inversión.
A quién aplica	• La Comunidad.
quién Implementa	• Analista de IT.

Norma	Se debe implementar un proceso que identifique y autentique a las personas o programas, antes de conceder el acceso local o remoto para que utilicen los recursos de información de DESTINAR FMI de acuerdo con un perfil previamente asignado.

Los usuarios tienen la responsabilidad de resguardar el acceso a los recursos informáticos de esta entidad con las contraseñas confidenciales. Estas contraseñas deben construirse obedeciendo las siguientes recomendaciones:

a) Longitud del Password: Mínimo 8 caracteres.
b) Manejo de contraseñas complejas de carácter obligatorio. (Las contraseñas deben involucrar: números, letras minúsculas y mayúsculas y caracteres especiales).
c) Cambio de Clave: Debe cambiarse cada 90 días.
d) Usar historial de claves, es decir, no se pueden reutilizar las últimas 24 claves.
e) Las contraseñas nunca deben ser almacenadas en sistemas informáticos sin protección, y obviamente ser escritas, porque es altamente riesgoso.
f) Todas las acciones realizadas bajo los auspicios de un identificador de usuario y sus consecuencias legales son responsabilidad del usuario titular del identificador.

2.3.4 La propiedad de los datos

De acuerdo a las Políticas de Seguridad informática se define que los roles de ***Propietarios de los Datos*** recaen en los Jefes/Directores de cada área de DESTINAR FMI, quienes son los responsables máximos de la información en cada una de sus dependencias.

2.4 Los Dispositivos de red

2.4.1 Los Dispositivos no autorizados

Todo el hardware conectado a la red debe ser autorizado por el oficial de seguridad. No pueden conectarse computadores desautorizados, servidores, hubs, switches, routers, memorias USB o cualquier otro hardware a la red sin la autorización correspondiente.

2.4.2 Utilización del Computador

El usuario es responsable del cuidado del hardware suministrado. El oficial de seguridad es responsable por la coordinación de mantenimiento y reparación de los computadores de los usuarios. Las reparaciones y/o ampliaciones de estos equipos no pueden ser hechas o contratadas por el usuario. El mantenimiento y reparación del equipamiento adquirido de cualquier otro modo, queda a cargo del responsable de la seguridad. Aquellos equipos o

sistemas que proponen un riesgo al funcionamiento razonable de la red u otro recurso informático de la Red de DFM serán desconectados sin aviso previo por el Oficial de Seguridad.

El software. El usuario no instalará ningún tipo de software (estandarizado o no, shareware, freeware, demo, de dominio público, redes p2p, aplicativos de chat o de mensajería, etc.) en los equipos servidores sin la aprobación expresa del Oficial De Seguridad. Toda instalación será considerada como falta plausible de sanción disciplinaria. Dicha aprobación se solicitará por escrito.

El acceso. El Oficial de Seguridad puede acceder e inspeccionar todos los dispositivos informáticos conectados o no a la red, para los propósitos de resolución de problemas o para investigar violaciones a las políticas, toda vez que lo necesite y sin previo trámite. Dicho libre acceso debe preverse especialmente en períodos de receso parcial de la actividad laboral, por razones de mantenimiento correctivo y o preventivo.

El Correo electrónico. El uso del correo electrónico estará sujeto a las disposiciones nacionales e internacionales vigentes. Todas las Dependencias que guarden relación institucional con Destinar FMI, deberán poseer una cuenta de correo electrónico, para incorporarse a las listas de correo pertinentes, a fin de facilitar la comunicación y conectividad institucional. Quienes no posean una, podrán solicitarla al Analista de TI. La consulta de esta cuenta será de obligación diaria.

Las Licencias de Software. Los dispositivos y sistemas conectados a la Red de Destinar FMI, deben en todo momento, estar por completo en conformidad con las licencias de software y hardware que fueron adquiridos. El uso o conexión a recursos informáticos de la Red Destinar FMI, implica el total conocimiento y aceptación de las políticas y leyes que garantizan el uso de estos medios. Al ingresar a la Red de la compañía, el usuario acepta cualquier responsabilidad legal que surja de una violación a estas políticas.

2.5 El Hacking

Toda tarea de utilización de técnicas y/o herramientas de hacking desde y hacia la Institución es considerada como faltas graves y se tomarán las medidas consecuentes con cada caso. Entre las técnicas de Hacking mencionamos:

1. La ingeniería inversa, cracking o desencripción de contraseñas.
2. El escaneo de puertos de TCP/IP.
3. La sustitución de usuarios o Hijacking.
4. La sustitución de paquetes IP, también conocida como IP spoofing
5. La utilización de analizadores de protocolos o scanners de tráfico de red.
6. Grabadoras de teclas o KeyLogger
7. Grabadoras de pantallas o KeyLogger Screen Capture
8. Hardware para ataques de Tempesting.
9. Herramientas de denegación de servicio.
10. La ingeniería social.

2.6 Usos Prohibidos

Destinar FMI considera el abuso en la utilización de recursos informáticos como una falta grave. A continuación se detalla una lista de algunos usos de recursos informáticos que se prohíben en esta Institución:

1. Utilización de cualquier recurso informático de la Red de la compañía para los propósitos comerciales personales o para ganancia personal.

2. Está prohibido el cobro por el uso/acceso a servicios de la Red Destinar FMI.

3. Utilización de cualquier recurso informático de la Red de Institucional de una manera que viole cualquier ley local o nacional.

4. Utilización de cualquier recurso informático de la Red Destinar FMI para guardar o transportar material ilegal, pornográfico, que haga apología del crimen o violencia, ofensivo, lesivo al buen nombre y honor de otros, propagandas comerciales, cadenas, difusión de actividades lucrativas en general, ni para ninguna actividad no institucional.

5. Conexiones desautorizadas a la Red de la compañía.

6. Instalación de hardware y/o software sin la autorización apropiada de la Dirección de TI en los equipos que requieren esta autorización.

7. Permitir a personal externo acceder a recursos informáticos de la Red Corporativa sin la autorización de la Gerencia General y/o el Analista de de TI.

8. Privar o intentar privar a otros usuarios la utilización y/o acceso a recursos informáticos de la Red de Destinar FMI.

9. Intentar penetrar la seguridad establecida sin los privilegios necesarios de cualquier equipo y comunicaciones de la red.

10. El uso desautorizado de cuentas del Computador u otras formas de acceso a Recursos informáticos de la Red corporativa.

11. Utilización de identificadores (nombre de usuarios y passwords) de usuarios ajenos.

12. Crear, utilizar o distribuir los programas que puedan dañar los datos, archivos, aplicaciones, funcionamientos del sistema, o funcionamientos de la red como ser virus, troyanos, key loggers, etc.

13. Capturar, desencriptar contraseñas y/o protocolos de comunicaciones.

14. Inspeccionar, modificar, o copiar programas o datos sin la autorización de su dueño o que atenten contra las leyes vigentes de legalidad del software y/o propiedad intelectual.

15. Utilizar cualquier correo electrónico o sistema de mensajería, ajenos a la Red de la compañía o no, para enviar contenido abusivo, ofensivo, obsceno, o saturar los canales de comunicaciones, o el envío "cadenas de cartas", y otros esquemas que pueden causar tráfico excesivo en la red o cargar los sistemas informáticos, incluyendo los dispositivos móviles.

16. Alterar el software o la configuración del hardware de cualquier equipo de cómputo o agregar cualquier dispositivo o sistema a la red sin el permiso del Analista de TI.

17. La utilización de software comercial ilegalmente copiado, ya sea texto, imágenes gráficas, o grabaciones de audio o video.

18. Utilización de la Red Corporativa para ganar o intentar ganar el acceso desautorizado a los recursos de información locales o remotos.

19. Saturar los canales de comunicación, con el envío masivo y excesivo de correos electrónicos, con adjuntos mayores a 10 Mb, igualmente acceder a páginas de videos, streaming y radio por internet.

20. Posesión o utilización de cualquier software o hardware que pueda comprometer la seguridad de la red o cualquier recurso informático de la Red de la compañía

21. Revelar, descubrir el secreto profesional que perjudique la competitividad de Destinar FMI.
22. Editar, vender, reproducir y falsificar, la información de Destinar FMI.

23. Los computadores instalados en una red institucional, y el uso que de ellas se haga, podrán ser monitoreados, tanto a nivel nacional como internacional, pudiendo ser identificadas fehacientemente. Está prohibido su uso para ingresar a páginas de contenido erótico, pornográfico, de violencia o terrorismo, y cualquier otro tipo de información no laboral y que sea lesiva a la finalidad de la red.

24. Emitir comentarios sobre la plataforma tecnológica, que generen alarma en los demás usuarios de la red, cualquier problema y/o inconsistencia que observe, remitirla al oficial de seguridad, la sugestión colectiva no ayuda para nada a solucionar un eventual problema, y si aumenta la incertidumbre en la calidad de los servicios.

2.7 Consideraciones Generales de Seguridad

El Analista de TI se reserva el derecho de quitar usuarios o dispositivos de la red de equipos de DESTINAR FMI sin notificación previa si se descubre o se sospecha cualquier vulnerabilidad en la seguridad. Los usuarios son responsables de ayudar a mantener la seguridad de la Red del Fondo siguiendo los procedimientos de seguridad establecidos. La presente política es solo un marco de referencia para los usuarios y en virtud de la imposibilidad de enumerar toda prohibición existente, dejamos aquí constancia de que todo aquello que no se encuentra

expresamente permitido se encuentra prohibido. Todas las disposiciones incluidas en este documento son aplicables a la red DESTINAR FMI.

El uso incorrecto del equipamiento informático de la Red del fondo compromete directamente a la Institución y al área y/o responsable del lugar en que el que se encuentre instalado, por lo que cada área y/o titular será responsable por los daños y perjuicios técnicos y/o legales que se generen por esta causa, aun cuando se hayan utilizado servicios de uso público irrestricto, como Yahoo, Hotmail, Gmail, etc., tanto en sus servicios de correo, como de foros, Chat y otros. La detección de este uso indebido podrá ocasionar la inhabilitación temporal o definitiva del sistema para el usuario responsable, a criterio de la Alta Gerencia, en relación directa con la gravedad del perjuicio ocasionado, y en el marco de las regulaciones institucionales.

Todo lo referido a sanciones por la trasgresión de estas normativas, se enmarca en las Reglamentaciones y Procedimientos ético-legales vigentes en el ámbito de Destinar FMI, y rigen para todo el personal de éste.

Toda sospecha de vulnerabilidad en la seguridad debe ser notificada inmediatamente al Encargado de Área y/o al Oficial de Seguridad.

3. POLÍTICAS, PROCEDIMIENTOS Y CONTROLES

3.1 Política general de seguridad de la información

Política	Política general de seguridad de la información.
Objetivo	Definir las pautas para asegurar una adecuada protección y seguridad de la información para todos los procesos de DESTINAR FMI, con el fin de alinear los procesos bajo la norma NTCISO-27001:2013
A quién aplica	• La Comunidad.
quién Implementa	• Líder de Seguridad de la Información (Analista de TI)

Directrices

a) Se debe verificar que se definan, implementen, revisen y actualicen las políticas de seguridad de la información.

b) Se debe establecer un programa que permita el fomento continuo de la creación de cultura y conciencia de seguridad en los funcionarios, contratistas, proveedores, personas, usuarios de los sistemas de información y telecomunicaciones de DESTINAR FMI.

c) Todos los usuarios de los sistemas de información y telecomunicaciones del DESTINAR FMI, 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 de la política de seguridad de la información.

g) Diseñar, programar y realizar los programas de auditoría del sistema de gestión de seguridad de la información, los cuales estarán a cargo de la Auditoria Interna.

h) Todo aplicativo informático o software debe ser comprado o aprobado por el Analista de TI.

i) DESTINAR FMI debe contar con un firewall o dispositivo de seguridad perimetral para la conexión a Internet o cuando sea inevitable para la conexión a otras redes en outsourcing o de terceros.

j) La conexión remota a la red de área local del DESTINAR FMI debe realizarse a través de una conexión VPN segura suministrada por la entidad, la cual debe ser aprobada, registrada y auditada, por el Analista de TI.

i) Los jefes de área o dependencia deben asegurarse que todos los procedimientos de seguridad de la información dentro de su área de responsabilidad, se realizan

correctamente para lograr el cumplimiento de las políticas y estándares de seguridad de la información de DESTINAR FMI.

j) DESTINAR FMI en caso de tener un servicio de transferencia de archivos deberá realizarlo empleando protocolos seguros. Cuando el origen sea DESTINAR FMI hacia entidades externas, DESTINAR FMI establecerá los controles necesarios para preservar la seguridad de la información; cuando el origen de la transferencia sea una entidad externa, se acordarán las políticas y controles de seguridad de la información con esa entidad; en todo caso se deben revisar y proponer controles en concordancia con las políticas de seguridad de la información del DESTINAR FMI; los resultados de la revisión de requerimientos de seguridad se documentarán y preservarán para futuras referencias o para demostrar el cumplimiento con las políticas y con los controles de seguridad del DESTINAR FMI.

k) DESTINAR FMI debe mantener correspondencia y vínculos técnicos entre las normas NTC-IS0 9001 y NTC-IS0 27001.

l) El Líder de Seguridad de la Información (Analista de TI) de DESTINAR FMI definirá de acuerdo a la clasificación de la información, qué datos deben ser cifrados y dará las directrices necesarias para la implementación de los respectivos controles (dispositivos a emplear, mecanismos de administración de claves, políticas de uso de sistemas de cifrado de datos).

3.2 Política para uso de dispositivos móviles

Política	Seguridad de la Información. Desarrollo de tareas de Administración de la Seguridad.
Objetivo	Establecer las directrices de uso y manejo de dispositivos móviles (teléfonos móviles, teléfonos inteligentes “smart phones”, tabletas), entre otros, suministrados por la entidad y personales que hagan uso de los servicios de información de DESTINAR FMI.
A quién aplica	Analista de TI
A quién compete	Líder de Seguridad de la Información (Analista de TI)
Directrices	

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

b) Los dispositivos móviles institucionales deben estar integrados a una plataforma de administración controlada por el Analista de TI.

c) Los usuarios de dispositivos móviles institucionales deben tener instaladas únicamente

las aplicaciones distribuidas, autorizadas y configuradas por el administrador de la plataforma.

d) Los dispositivos móviles asignados por DESTINAR FMI deben tener la configuración realizada por el Analista de TI, así mismo, solo podrá configurarse únicamente las cuentas de correo electrónico asignadas al usuario por la entidad.

e) El sistema de mensajería instantánea autorizado para los dispositivos móviles institucionales es Skype y WhatsApp, no se permite por esta aplicación, el envío de fotografías, audios y videos clasificados como información restringida, ni datos sensibles de afiliados.

f) Los sistemas de mensajería instantánea para dispositivos móviles institucionales a implementar en DESTINAR FMI debe incluir métodos de cifrado de extremo a extremo de la comunicación.

g) Los dispositivos móviles deben tener contraseña de ingreso y bloqueo del equipo de manera automática y manual, tener activado la función de borrado remoto, cifrar la memoria de almacenamiento.

h) 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 por la entidad.

i) Ante la pérdida del equipo, ya sea por extravío o hurto, el usuario deberá informar de manera inmediata al Analista de TI, y continuar con el procedimiento administrativo por perdida de elementos establecido por la entidad.

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

k) Es responsabilidad del usuario hacer buen uso del dispositivo suministrado por DESTINAR FMI con el fin de realizar actividades propias de su cargo o funciones asignadas en la entidad.

l) Los usuarios no están autorizados a cambiar la configuración, ni a la desinstalación de software de los equipos móviles institucionales posterior a su recibo; únicamente se deben aceptar y aplicar las actualizaciones.

m) Los usuarios de dispositivos móviles asignados por la entidad, deben evitar hacer uso de estos en lugares con algún riesgo de seguridad, evitando el extravío o hurto del equipo.

n) Los usuarios de dispositivos móviles institucionales no deben ser conectados en computadores y/o puertos USB de uso público (Restaurantes, café internet, aeropuertos, etc.).

o) Los usuarios de dispositivos móviles institucionales deben mantener desactivados las funciones de redes inalámbricas WiFi, puertos infrarrojos, puerto Bluetooth.

p) Los usuarios de dispositivos móviles institucionales NO deben hacer uso de redes inalámbricas públicas.

q) En caso de requerir instalación de aplicaciones adicionales en el dispositivo móvil institucional se debe solicitar al Analista de TI para su aprobación.

3.3 Responsabilidad de la Administración de Seguridad

Política	Responsabilidad de la Administración de Seguridad
Objetivo	Establecer que la responsabilidad de la Administración de Seguridad de la Información en primer lugar es de Destinar FMI y en caso que hubiere que delegar algunos aspectos a un tercero, se debe evaluar todos los riegos asociados.
A quién aplica	• La comunidad
A quién compete	• Líder de Seguridad de la Información (Analista de TI)
Norma	La administración de la Seguridad de la Información es una actividad de Destinar y en caso de que un tercero intervenga por decisión de la Alta Gerencia, se debe garantizar contractualmente que se garantiza la confidencialidad e integridad de la información.

3.4 Asignación De Derechos De Propiedad Intelectual

Política	Asignación de derechos de Propiedad Intelectual.
Objetivo	Asegurar que los desarrollos realizados por empleados de Destinar involucren los derechos de propiedad intelectual.
A quién aplica	• La Comunidad.
A quién compete	• Líder de Recursos Humanos. • Líder de Seguridad de la Información (Analista de TI) • La Comunidad. • Auditor de Destinar.
Norma	Se debe establecer en los contratos de trabajo cláusulas sobre la propiedad intelectual de Destinar sobre el material y los trabajos generados por los empleados en desarrollo de sus funciones normales del negocio. El personal de Destinar y terceros contratados, le conceden a la

	Compañía los derechos exclusivos de las patentes, derechos de propiedad literaria, invenciones, procesos, procedimientos metodologías, controversias jurídicas en las que se encuentre involucrado, archivos comerciales jurídicos, archivos de personal e información privada personal o familiar del personal, normas y/o medidas de seguridad u otra propiedad intelectual que ellos originen y/o desarrollen como parte de sus funciones en el desarrollo normal del negocio de acuerdo con el contrato de trabajo.

3.5 Ley de Derechos de Autor

Política	Cumplimiento de la ley de Derechos de Autor.
Objetivo	Garantizar la instalación de software legal.
A quién aplica	La Comunidad
A quién compete	Líder de Seguridad de la Información (Analista de TI) Auditor de Destinar. Asesor Jurídico Destinar.
Norma	**Protección de Creaciones de Terceros:** La instalación de software o el uso de información externa en los recursos informáticos de Destinar FMI deben cumplir con las exigencias de la ley de derechos de autor, que legitimen su utilización. Se debe implementar controles para asegurar el cumplimiento con las exigencias de tipo legal en la utilización de software que puede estar supeditado a derechos de propiedad intelectual tales como licenciamiento, derechos de autor y derechos de diseño. De acuerdo a lo previsto por el artículo 91 de la Ley 23 de 1982, los derechos de autor sobre las obras creadas por los empleados y funcionarios en virtud de su vinculación a la Entidad correspondiente, en este caso a DESTINAR, son de propiedad de ésta con las excepciones que la misma ley han señalado.

3.6 Información Privada de Afiliados y Empresas Patrocinadoras

Política	Protección de Información Privada de los Afiliados y Empresas patrocinadoras.
Objetivo	Proteger la información de los afiliados para evitar que sea divulgada.
A quién aplica	Líder de Seguridad de la Información (Analista de TI)
A quién compete	La Comunidad. Auditor de Destinar.

Norma	Atendiendo lo establecido en el artículo 15 de la Constitución Política de Colombia, y en la ley 1581 de 2012 se considera Privada la información propia de los afiliados suministrada a Destinar FMI para el desarrollo del negocio. Entre otra la siguiente: a) Información Básica. b) Actividad Económica. c) Información financiera y crediticia. d) Referencias Comerciales y/o Bancarias. e) Obligaciones con entidades bancarias.

3.7 Instalación de Software

Política	Instalación de Software Autorizado. Cumplimiento Legal.
Objetivo	Implementar controles para evitar la instalación de software no autorizado en los recursos informáticos de Destinar.
A quién aplica	Analista de IT. La Comunidad.
A quién compete	Líder de Seguridad de la Información (Analista de TI) Auditor de Destinar.
Norma	El software instalado en los recursos de información al servicio de la Empresa, debe ser autorizado por la alta Gerencia de Destinar. Se deben implementar mecanismos de que ayuden al Analista de IT controlar el software instalado en los recursos de información. El Analista de IT debe efectuar periódicamente revisiones del software instalado y reportar su resultado a la alta Gerencia. El Analista de TI definirá e implementará el procedimiento de instalación y actualización de software sobre los sistemas operativos de DESTINAR FMI, dentro del cual se debe prever una estrategia de retroceso, registros de auditoria, control y copia de versiones, control de cambio, pruebas en su respectivo ambiente y configuraciones de seguridad.

3.8 Política de uso de los activos

Política	Política de uso de los activos
Objetivo	Lograr y mantener la protección adecuada de los activos de información mediante la asignación a los usuarios finales que deban

	administrarlos de acuerdo a sus roles y funciones Establecer la custodia y preservación de los originales de licencias, medios y manuales del software adquiridos por Destinar.
A quién aplica	Analista de IT.
A quién compete	Líder de Seguridad de la Información (Analista de TI) Auditor de Destinar.

Directrices

Inventario de activos de información:

DESTINAR FMI mantendrá un inventario actualizado de sus activos de información, bajo la responsabilidad de cada propietario de información y centralizado por el Analista de TI.

a) Propietarios de los activos de información

DESTINAR FMI es el dueño de la propiedad intelectual de los avances tecnológicos e intelectuales desarrollados por los funcionarios de DESTINAR FMI y los contratistas, derivadas del objeto del cumplimiento de funciones y/o tareas asignadas, como las necesarias para el cumplimiento del objeto del contrato.

DESTINAR FMI es propietario de los activos de información y los administradores de estos activos son los funcionarios, contratistas o demás colaboradores de DESTINAR FMI (denominados “usuarios”) 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 de Tecnología y Sistemas de Información (TIC).

b) Los activos de información pertenecen a DESTINAR FMI y el uso de los mismos debe emplearse exclusivamente con propósitos laborales.

c) 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 el Analista de TI.

d) DESTINAR FMI proporcionará al usuario, los equipos informáticos y los programas instalados en ellos; los datos/información creados, almacenados y recibidos, serán propiedad de DESTINAR FMI, los funcionarios solo podrán realizar backup de sus archivos personales o de información pública, para copiar cualquier tipo de información clasificada o reservada debe pedir autorización a su jefe inmediato, de acuerdo a las normas sobre clasificación de la información de acuerdo a los niveles de seguridad establecidos por DESTINAR FMI; la copia, sustracción, daño intencional o utilización para fines distintos a las labores propias del fondo, serán sancionadas de acuerdo con las normas y legislación vigentes.

e) Una vez al año, el Analista de TI efectuará la revisión de los programas utilizados en cada dependencia. La descarga, instalación o uso de aplicativos o programas informáticos

NO autorizados será considera como una violación a las Políticas de Seguridad de la Información de DESTINAR FMI.

f) Todos los requerimientos de aplicativos, sistemas y equipos informáticos deben ser solicitados por el usuario, a través, del envió de un correo electrónico al Analista de TI.

g) Estarán bajo custodia del Analista de TI los medios magnéticos/electrónicos (disquetes, CDs u otros) que vengan originalmente con el software y sus respectivos manuales y licencias de uso, adicionalmente las claves para descargar el software de fabricantes de sus páginas web o sitios en internet y los passwords de administración de los equipos informáticos, sistemas de información o aplicativos.

h) En caso de ser necesario y previa autorización del Gerente General, el Líder de Seguridad de la Información (Analista de TI) de DESTINAR FMI, podrá acceder a revisar cualquier tipo de activo de información y material que los usuarios creen, almacenen, envíen o reciban, a través de Internet o de cualquier otra red o medio, en los equipos informáticos a su uso.

i) Los recursos informáticos de DESTINAR FMI no podrán ser utilizados, sin previa autorización escrita, para divulgar, propagar o almacenar contenido personal o comercial de publicidad, promociones, ofertas, programas destructivos (virus), propaganda política, material religioso o cualquier otro uso que no esté autorizado.

j) Los usuarios 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, practica de juegos en línea, uso permanente de redes sociales personales, conexión de periféricos o equipos que causen molestia a compañeros de trabajo, etc.

k) Los usuarios no podrán efectuar ninguna de las siguientes labores sin previa autorización del Analista de TI:

1) Bajar o descargar e instalar software de Internet u otro servicio en línea en cualquier equipo de DESTINAR FMI;
2) Modificar, revisar, transformar o adaptar cualquier software propiedad de DESTINAR FMI;
3) Descompilar o realizar ingeniería inversa en cualquier software de propiedad de DESTINAR FMI.
4) Copiar o distribuir cualquier software de propiedad de DESTINAR FMI.
6) Cambiar la configuración de hardware de propiedad de DESTINAR FMI

l) El usuario a través del correo electrónico deberá informar al Jefe Inmediato de cualquier violación de las políticas de seguridad, uso indebido y debilidades de seguridad de la información de DESTINAR FMI que tenga conocimiento al Analista de TI.

m) El usuario será responsable de todas las transacciones o acciones efectuadas con su “cuenta de usuario”.

n) Ningún usuario deberá acceder a la red o a los servicios TIC de DESTINAR FMI, utilizando una cuenta de usuario o clave de otro usuario.

o) Los usuarios no están autorizados para hacer uso de redes externas a través de dispositivos personales en las instalaciones de la entidad (modem USB, router, wifi público, etc), esto compromete la seguridad de los recursos informáticos de DESTINAR FMI.

p) El Analista de TI, es el responsable de realizar el aseguramiento de los accesos a internet, acceso a redes de terceros y a las redes de la entidad; esta responsabilidad incluye, pero no se limita a prevenir que intrusos tengan acceso a los recursos informáticos y a prevenir la introducción y propagación de virus.

q) Todo archivo o material descargado o recibido a través de medio magnético/electrónico o descarga de Internet o de cualquier red o equipo externo, deberá ser revisado para detección de virus y otros programas maliciosos antes de ser instalados en la infraestructura de DESTINAR FMI.

r) Todo cambio a la infraestructura informática deberá estar controlado y será realizado de acuerdo con los procedimientos de control de cambios de DESTINAR FMI.

s) La información de DESTINAR FMI debe ser respaldada de forma frecuente, debe ser almacenada en lugares apropiados en los cuales se pueda garantizar que la información este segura y podrá ser recuperada en caso de un desastre o de incidentes con los equipos de procesamiento, se puede utilizar los servicios de Cloud Backup.

t) Los funcionarios deberán realizar la devolución de todos los activos físicos y/o electrónicos asignados por DESTINAR FMI en el proceso de desvinculación, de igual manera deberán documentar y entregar al DESTINAR FMI los conocimientos importantes que posee de la labor que ejecutan.

u) Las licencias, medios y manuales del software adquirido por Destinar pueden sacárseles copia para tareas de instalaciones y consultas de soporte técnico, para evitar el deterioro y pérdida de las licencias originales. Destinar debe establecer un lugar adecuado para custodiar las licencias originales y las eventuales copias.
Adicionalmente, se debe implementar mecanismos de control del inventario de estos recursos.

3.9 Envío de Información Privada por Correo Electrónico

Política	Se prohíbe el envío de Información Privada de afiliados a correos no registrados. Cumplimiento Legal.
A quién aplica	La Comunidad.

A quién compete	Líder de Seguridad de la Información (Analista de TI) Auditor de Destinar.
Norma	Está prohibido el envío de mensajes a correos no registrados con información objeto de protección legal por reserva bancaria y por protección de datos personales. Ningún usuario está autorizado para enviar correos a cuentas que el cliente no hubiere.

3.10 Circular Externa 038 de 2009 y Circular Externa 007 de 2019 de la Superfinanciera

Política	Cumplimiento de las obligaciones expresadas en la Circular Externa 038 y 007 de la Superfinanciera. Cumplimiento Legal.
Objetivo	Garantizar el cumplimiento de los requerimientos que la Superfinanciera menciona en la circular 038 y 007.
A quién aplica	Gerencia.
A quién compete	Líder de Seguridad de la Información (Analista de TI) Auditor de Destinar. La Comunidad.
Norma	Se debe cumplir de manera permanente los requerimientos enunciados en la Circular 038 de 2009 y 007 de 2019. Cualquier modificación a la reglamentación sucedida al interior de Destinar debe tener presente las exigencias enunciados en la Circular 038 de 2009 y 007 de 2019.

3.11 Aspectos de Seguridad en Los Contratos con Terceros

Política	Aspectos de Seguridad en los contratos con Terceros. Cumplimiento Legal.
Objetivo	Incorporar aspectos de seguridad de la información en los contratos firmados con terceros.
A quién aplica	Asesor Legal Destinar. La Comunidad.
A quién compete	Líder de Seguridad de la Información (Analista de TI)
Norma	Los contratos firmados con Terceros para la prestación de servicios de TI, deben incluir cláusulas de confidencialidad y cumplimiento de la Política de Seguridad de la Información. Entro otros, se debe incluir los siguientes temas:

	a) Normas sobre la propiedad de la información. b) Compromiso de confidencialidad. c) Restricciones sobre el software empleado. d) Normas de seguridad física. e) Uso y disposición de la información. f) Cumplimiento de Niveles de servicio.

3.12 Análisis de Riesgos

Política	Administración del riesgo en Seguridad de la Información. Análisis de riesgos.
Objetivo	Instaurar la ejecución periódica de un análisis de riesgos de Seguridad de la Información.
A quién aplica	Líder de Seguridad de la Información (Analista de TI)
A quién compete	Auditor de Destinar.
Norma	Se debe efectuar periódicamente (1 año) un inventario de los activos de tecnología de la información utilizados por Destinar y con base en este inventario, realizar un análisis de riesgos con el objeto de determinar los recursos que tienen un nivel crítico de exposición, y de esta manera reforzar los controles de una manera adecuada.

3.13 Seguros para los Recursos TI

Política	Seguros para los recursos de tecnología de la información. Administración del riesgo en Seguridad de la Información.
Objetivo	Instituir la adquisición de seguros para los recursos informáticos.
A quién aplica	Analista de IT. Gerente General.
A quién compete	Líder de Seguridad de la Información (Analista de TI) Auditor de Destinar.
Norma	Se deben adquirir seguros que protejan los recursos de tecnología de la información de Destinar, como el hardware, los datos, el software y la documentación.

3.14 Clasificación de la información.

Política	Clasificación de la información.
Objetivo	Clasificar la información y establecer niveles de seguridad.
A quién aplica	La Comunidad.
Responsable de implementar	Líder de Seguridad de la Información (Analista de TI) Auditor de Destinar.
Norma	La información de Destinar debe clasificarse, de acuerdo con el estándar establecido, en una de las siguientes categorías: a) Restringida. b) Uso Interno. c) Pública. d) No Clasificada Se deben aplicar los siguientes criterios para asignar la clasificación a la información: a) Confidencialidad. b) Riesgo de pérdida o compromiso. c) Aspectos legales. d) Requerimientos de retención. e) Facilidad de recuperación.

3.15 Rotulado de medios de almacenamiento.

Política	Rotulado de medios de almacenamiento. Clasificación de la información.
Objetivo	Establecer la obligación de rotular los medios de almacenamiento indicando la Clasificación de la información que contienen.
A quién aplica	La Comunidad.
A quién compete	Líder de Seguridad de la Información (Analista de TI) Auditor de Destinar.
Norma	Todos los medios digitales y físicos que contienen información clasificada como “Restringida” o de “Uso Interno” deben ser rotulados indicando claramente la Clasificación. En el evento que un medio contenga partes de información de diferente tipo, éste debe rotularse con la clasificación más alta. La información que no haya sido clasificada deberá considerarse como “No Clasificada”.

3.16 Contraseñas de Cifrado

Política	Confidencialidad de las contraseñas de cifrado. Clasificación de la información.
Objetivo	Establecer el carácter de confidencialidad de las Contraseñas de cifrado.
A quién aplica	Analista de IT.
A quién compete	Líder de Seguridad de la Información (Analista de TI) Auditor de Destinar.
Norma	Se debe implementar un procedimiento de gestión de custodia de las contraseñas de cifrado de información, en razón a que estas contraseñas son consideradas como un activo de información altamente crítico.

3.17 Borrado Seguro o Destrucción de Medios

Política	Borrado seguro o destrucción de medios digitales o físicos. Clasificación de la información.
Objetivo	Instituir el borrado seguro o destrucción de medios en desuso, que contengan información Restringida o de Uso Interno.
A quién aplica	Analista de IT. La Comunidad.
A quién compete	Líder de Seguridad de la Información (Analista de TI) Auditor de Destinar.
Norma	Se debe aplicar un procedimiento de borrado seguro o destrucción de los medios digitales o físicos, que contengan Información Restringida o de Uso Interno, en los siguientes casos: a) Cuando se necesite dar de baja un medio de almacenamiento o un recurso Informático. b) Cuando se tenga almacenada copia de información, y ya no se necesite. c) Cuando las Copias de seguridad lleguen a la obsolescencia. d) Cuando un recurso Informático va a ser entregado a un tercero por cambio o por servicio.

3.18 Aviso de Confidencialidad en Los Correos Electrónicos

Política	Aviso de confidencialidad en los correos electrónicos. Clasificación de la información.

Objetivo	Propender por el buen uso, responsabilidad e impacto de la información contenida en los correos electrónicos.
A quién aplica	Analista de IT. La Comunidad.
A quién compete	Líder de Seguridad de la Información (Analista de TI) Auditor de Destinar.
Norma	Los correos electrónicos corporativos enviados deben incluir en su cuerpo un aviso de confidencialidad que avise al destinatario su compromiso con la Seguridad de la Información contenida o adjunta en el mensaje.

3.19 Cumplimiento de las Políticas de Seguridad de la Información

Política	Cumplimiento de la política de Seguridad de la Información por parte de los empleados. Seguridad en el personal.
Objetivo	Implementar un documento formal en el que los empleados se comprometan a dar cumplimiento a la Política de Seguridad de la Información de Destinar.
A quién aplica	Gerente General. Líder de Seguridad de la Información (Analista de TI)
A quién compete	Analista de TI. Auditor de Destinar. La Comunidad.
Norma	Los empleados de Destinar deben firmar un compromiso de cumplimiento a la política de Seguridad de la Información, haciendo énfasis en la preservación de la confidencialidad de la información clasificada como Restringida y de Uso Interno. Debe ser de obligatorio cumplimiento y el no acatarlo debe implicar acciones tanto disciplinarias como legales.

3.20 Política de tratamiento de datos personales

Política	**Política de tratamiento de datos personales para dar cumplimiento de la ley 1581 de 2012**
Objetivo	Establecer los lineamientos para administración y tratamiento de datos personales para cubrir los aspectos que demanda la ley 1581 de 2012 y decretos reglamentarios.
A quién aplica	Gerente General.

	Líder de Seguridad de la Información (Analista de TI)
A quién compete	Analista de TI. Auditor de Destinar. La Comunidad.
Norma	Dar cumplimiento a la ley 1581 y decretos reglamentarios para garantizar la protección de datos personales de los afiliados, proveedores, etc., en concordancia con GTI-PD01-MP02 Política Protección Datos Destinar FMI

3.21 Política de uso de estaciones cliente

Política	Política de uso de estaciones cliente.
Objetivo	Garantizar que la seguridad es parte integral de los activos de información y la correcta utilización por los usuarios finales
A quién aplica	La Comunidad.
quién Implementa	Líder de Seguridad de la Información (Analista de TI)

Directrices

a) La instalación de software en los computadores suministrados por DESTINAR FMI, es una función exclusiva del Analista de TI el cual mantendrá una lista actualizada del software autorizado para instalar en los computadores.

b) Se definirán un (1) perfil de Administrador local, denominado soporte, para actividades de soporte técnico y/o recuperación de errores, y solo puede tener control de esta cuenta el Analista de TI y, se permite la creación de una cuenta administradora para aquellos Usuarios que necesitan utilizar software específico, que por su naturaleza requieren permisos de administrador local para su ejecución.

c) Los usuarios que hagan uso de equipos institucionales en préstamo, NO deberán almacenar información en estos dispositivos y deberán borrar aquellos que copien en estos al terminar su uso.

d) Los usuarios no deben mantener almacenados en los discos duros de las estaciones cliente o discos virtuales de red, archivos de vídeo, música y fotos que no sean de carácter institucional.

e) En el Disco C:\ de las estaciones cliente se tiene configurado el sistema operativo, aplicaciones y perfil de usuario. El usuario deberá abstenerse de realizar modificaciones a éstos archivos.

f) Los usuarios podrán trabajar sus documentos institucionales en borrador en la estación

cliente asignado por DESTINAR FMI y deberán ubicar copias y documentos finales en las carpetas virtuales centralizadas que se establezca para cumplir con las tablas de retención documental TRD de la Entidad.

g) El préstamo de equipos de cómputo, computadores portátiles y vídeo proyectores se debe tramitar a través de un correo electrónico al Analista de TI con anticipación y se proveerá de acuerdo a la disponibilidad.

h) Los equipos que ingresan temporalmente al DESTINAR FMI que son de propiedad de terceros: deben ser registrados en los controles de acceso de la entidad para poder realizar su retiro; posteriormente DESTINAR FMI no se hará responsable en caso de pérdida o daño de algún equipo informático de uso personal o que haya sido ingresado a sus instalaciones.

i) El Analista de TI no prestará servicio de soporte técnico (revisión, mantenimiento, reparación, configuración y manejo e información) a equipos que no sean del DESTINAR FMI.

3.22 Política de uso de Internet.

Política	Política de uso de Internet.
Objetivo	Establecer unos lineamientos que garanticen la navegación segura y el uso adecuado de la red por parte de los usuarios finales, evitando errores, pérdidas, modificaciones no autorizadas o uso inadecuado de la información en las aplicaciones WEB.
A quién aplica	La Comunidad.
quién Implementa	Líder de Seguridad de la Información (Analista de TI)
Directrices	

a) La infraestructura, servicios y tecnologías usados para acceder a internet son propiedad del DESTINAR FMI, por lo tanto se reserva el derecho de monitorear el tráfico de internet y el acceso a la información.

b) La navegación en Internet debe realizarse de forma razonable y con propósitos laborales.

c) No se permite la navegación a sitios con contenidos contrarios a la ley o a las políticas de DESTINAR FMI o que representen peligro para la entidad como: pornografía, terrorismo, hacktivismo, segregación racial u otras fuentes definidas por DESTINAR FMI. El acceso a este tipo de contenidos con propósitos de estudio de seguridad o de investigación, debe contar con la autorización expresa del Líder de Seguridad de la Información (Analista de TI) de DESTINAR FMI.

d) El Analista de TI administrará autorización de navegación a los usuarios de DESTINAR FMI, previa solicitud del Gerente General.

e) El Analista de TI implementará herramientas para evitar la descarga de software no autorizado y/o código malicioso en los equipos institucionales.

f) La descarga de archivos de Internet debe ser con propósitos laborales y de forma razonable para no afectar el servicio, en forma específica el usuario debe cumplir los requerimientos de la política de uso de internet descrita en este manual.

g) Los usuarios de los activos de información de DESTINAR FMI tienen prohibido la publicación de información de Destinar FMI en redes sociales, sistemas de mensajería instantánea y cuentas de correo no institucional. De igual manera abstenerse de utilizar lenguaje inapropiado y/o vulgar.

3.23 Política de clasificación de la información.

Política	Política de clasificación de la información.
Objetivo	Asegurar que la información recibe el nivel de protección apropiado de acuerdo al tipo de clasificación establecido por la ley y el gobierno interno de DESTINAR FMI
A quién aplica	La Comunidad.
quién Implementa	Líder de Seguridad de la Información (Analista de TI)

Directrices

a) Se considera información toda forma de comunicación o representación de conocimiento o datos digitales, escritos en cualquier medio, ya sea magnético, papel, visual u otro que genere DESTINAR FMI como por ejemplo:

- Formularios / comprobantes propios o de terceros.
- Información en los sistemas, equipos informáticos, medios magnéticos/electrónicos o medios físicos como papel.
- Otros soportes magnéticos/electrónicos removibles, móviles o fijos.
- Información o conocimiento transmitido de manera verbal o por cualquier otro medio de comunicación.

b) Los usuarios responsables de la información del DESTINAR FMI, deben identificar los riesgos a los que está expuesta la información de sus áreas, teniendo en cuenta que la información pueda ser copiada, divulgada, modificada o destruida física o digitalmente por personal interno o externo.

c) Un activo de información es un elemento definible e identificable que almacena registros, datos o información en cualquier tipo de medio y que tiene valor para DESTINAR FMI; Independiente del tipo de activo, se deben considerar las siguientes características:

1. El activo de información es reconocido como valioso para DESTINAR FMI.
2. No es fácilmente reemplazable sin incurrir en costos, habilidades especiales, tiempo, recursos o la combinación de los anteriores.
3. Forma parte de la identidad de la organización y sin el cual DESTINAR FMI puede estar en algún nivel de riesgo. La determinación del nivel y tipo de riesgo se estima sobre la base de la relación de activos de información de DESTINAR para la información digital o electrónica (FMI GTI-PD01-F02-Relacion_Activos_Informacion) y para la documentación en medio físico (papel).
4. Los niveles de clasificación de la información valiosa que se ha establecido son:

INFORMACIÓN DE USO INTERNO, INFORMACIÓN RESTRINGIDA y INFORMACIÓN PÚBLICA.

5. Los aspectos detallados de la política de clasificación, tratamiento y control de la información se encuentran en el documento.

d) Se debe actualizar el inventario anualmente de los activos de información para todos los usuarios.

3.24 Política de manejo disposición de información, medios y equipos

Política	Seguridad de la Información.
Objetivo	Contrarrestar las interrupciones en las actividades de DESTINAR FMI, proteger sus procesos críticos contra los efectos de fallas importantes en los sistemas de información o contra desastres y propender por su recuperación oportuna, permitiendo la confidencialidad, integridad y disponibilidad de la información.
A quién aplica	La Comunidad.
quién Implementa	Líder de Seguridad de la Información (Analista de TI)

Directrices

a) Los medios y equipos donde se almacena, procesa o comunica la información, deben mantenerse con las medidas de protección físicas y lógicas, que permitan su monitoreo y correcto estado de funcionamiento, para ello se debe realizar los mantenimientos preventivos y correctivos que se requieran.

b) Se debe realizar la aplicación del borrado seguro de la información.

c) Está restringido el uso de medios removibles de almacenamiento, por lo cual se deshabilita la funcionalidad de los puertos USB y unidades ópticas de grabación en

todos los equipos de cómputo institucionales; la autorización de uso de los medios removibles debe ser aprobada por la Gerencia General, y ejecuta por el Analista de TI.

3.25 Política de control de acceso

Política	**Política de control de acceso**
Objetivo	Definir las pautas generales para asegurar un acceso controlado, físico o lógico, a la información de la plataforma informática de DESTINAR, así como el uso de medios de computación móvil.
A quién aplica	La Comunidad.
quién Implementa	Líder de Seguridad de la Información (Analista de TI)

Directrices

a) El Analista de TI establecerá el procedimiento para establecer los niveles de acceso para usuarios de los servicios y sistemas de información de DESTINAR FMI.

b) El Analista de TI establecerá las configuraciones de las políticas en los sistemas de tecnología y comunicaciones para el control de acceso a los activos de información.

c) DESTINAR FMI proporcionará a los funcionarios, personal en comisión permanente y contratistas (personas naturales) todos los recursos tecnológicos necesarios para que puedan desempeñar las funciones para las cuales fueron contratados, por tal motivo no se permite conectar a la red o instalar dispositivos fijos o móviles, tales como: computadores portátiles, *tablets*, enrutadores, agendas electrónicas, celulares inteligentes, *access point*, el Analista de TI podrá realizar la mencionada conexión previa solicitud del interesado.

d) DESTINAR FMI suministrará a los usuarios las claves respectivas para el acceso a los servicios de red y sistemas de información a los que hayan sido autorizados, las claves son de uso personal e intransferible. Es responsabilidad del usuario el manejo apropiado de las claves que se le asignen.

e) El analista de TI debe garantizar que el software instalado esta en concordancia con el software autorizado para uso en los sistemas de información y comunicaciones de DESTINAR FMI

f) Solo el Analista de TI estará autorizado para instalar software y/o hardware en los equipos, servidores e infraestructura de telecomunicaciones de DESTINAR, así como el uso de herramientas que permitan realizar tareas de mantenimiento, revisión de software, recuperar datos perdidos, eliminar software maliciosos.

g) Todo trabajo a realizarse en los servidores de DESTINAR, por parte de sus funcionarios o contratistas, se debe realizar en las instalaciones, no se podrá realizar ninguna actividad de tipo remoto sin la debida aprobación del Analista de TI de DESTINAR.

h) En DESTINAR está prohibido el acceso 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.

i) El Analista de TI establecerá el procedimiento de registro, cancelación y periodicidad de revisión y ajuste a permisos de acceso a la red y servicios de red, asignados a los usuarios de los sistemas de información y comunicaciones de DESTINAR, tomando como base los múltiples factores de riesgo existentes en la seguridad de la información.

j) La conexión remota a la red de área local de DESTINAR FMI debe ser realizada, a través, de una conexión VPN segura suministrada por la entidad, la cual debe ser aprobada, registrada y auditada.

3.26 Política de establecimiento, uso y protección de claves de acceso

Política	**Política de establecimiento, uso y protección de claves de acceso**
Objetivo	Controlar el acceso a la información.
A quién aplica	La Comunidad.
quién Implementa	Líder de Seguridad de la Información (Analista de TI)
Directrices	

a) Se debe concientizar y controlar a los usuarios para que apliquen buenas prácticas de seguridad en la selección, uso y protección de claves o contraseñas, las cuales constituyen un medio de validación de la identidad de un usuario y consecuentemente un medio para establecer derechos de acceso a las instalaciones, equipos o servicios informáticos.

b) Los usuarios son responsables del uso de las claves o contraseñas de acceso que se le asignen para la utilización de los equipos o servicios informáticos de DESTINAR FMI.

c) Los usuarios deben tener en cuenta los siguientes aspectos:

d) No incluir contraseñas en ningún proceso de registro automatizado, por ejemplo almacenadas en un macro o en una clave de función.

e) El cambio de contraseña solo podrá ser solicitado por el titular de la cuenta o su jefe inmediato.

f) Terminar las sesiones activas cuando finalice, o asegurarlas con el mecanismo de bloqueo cuando no estén en uso.

g) Se bloqueara el acceso a todo usuario que haya intentado el ingreso, sin éxito, a un equipo o sistema informático, en forma consecutiva por cinco veces.

h) La clave de acceso será desbloqueada sólo por el Analista de TI, luego de la solicitud formal vía correo electrónico, por parte, del responsable de la cuenta.

Las claves o contraseñas deben:

b) Poseer algún grado de complejidad y no deben ser palabras comunes que se puedan encontrar en diccionarios, ni tener información personal, ni productos a resaltar de su entidad, evite asociarla con fechas especiales, por ejemplo: fechas de cumpleaños, nombre de los hijos, placas de automóvil, etc.
c) Nunca utilice sus contraseñas personales en el entorno laboral
d) Tener mínimo ocho caracteres alfanuméricos.
e) Cambiarse obligatoriamente la primera vez que el usuario ingrese al sistema.
e) Cambiarse obligatoriamente cada 90 días, o cuando por razones de seguridad lo establezca el Analista de TI
f) Cada vez que se cambien estas deben ser distintas por lo menos de las últimas tres anteriores.
g) Cambiar la contraseña si ha estado bajo riesgo o se ha detectado anomalía en la cuenta de usuario.
h) No se deben usar caracteres idénticos consecutivos, ni que sean todos numéricos, ni todos alfabéticos.
i) No debe ser visible en la pantalla, al momento de ser ingresada o mostrarse o compartirse.
j) No ser reveladas a ninguna persona, incluyendo al Analista de TI.
k) No regístralas en papel, archivos digitales o dispositivos manuales, a menos que se puedan almacenar de forma segura y el método de almacenamiento este aprobado.

3.27 Política de uso de discos de red o carpetas virtuales.

Política	**Política de uso de discos de red o carpetas virtuales.**
Objetivo	Asegurar la operación correcta y segura de los discos de red o carpetas virtuales.
A quién aplica	La Comunidad.

quién Implementa	Líder de Seguridad de la Información (Analista de TI)
Directrices	

a) El dueño de cada proceso o responsable de área deberá enviar un correo al Analista de TI autorizando el acceso y permisos, correspondientes para los archivos que desea compartir a la Comunidad. Los usuarios tendrán permisos de escritura, lectura o modificación de información en los discos del servidor, dependiendo de sus funciones y su rol.

b) La información institucional que se trabaje en las estaciones cliente de cada usuario debe ser trasladada inmediatamente (máximo 5 días después de su creación) a los discos del servidor por ser información institucional, en caso que sean archivos de trabajo de pruebas o información de trabajo temporal, debe eliminarse periódicamente (90 días).

c) La información almacenada en cualquiera de los discos de red debe ser de carácter institucional.

d) Está prohibido almacenar archivos con contenido que atente contra la moral y las buenas costumbres de la entidad o las personas, como pornografía, propaganda racista, terrorista o cualquier software ilegal o malicioso, ya sea en medios de almacenamiento de estaciones de trabajo, computadores de escritorio o portátiles, tablets, celulares inteligentes, etc. o en los discos del servidor.

e) Se prohíbe extraer, divulgar o publicar información de cualquiera de los discos del servidor o estaciones de trabajo, sin expresa autorización del Gerente General.

f) Se prohíbe el uso de la información de los discos del servidor con fines publicitarios, de imagen negativa, lucrativa o comercial.

La responsabilidad de generar las copias de respaldo de la información de los discos de red, está a cargo del Analista de TI.

La responsabilidad de custodiar la información en copias de respaldo controladas, fuera de las instalaciones de DESTINAR FMI, estará a cargo del Analista de TI.

3.28 Política de uso de puntos de red de datos (red de área local – LAN).

Política	**Política de uso de puntos de red de datos (red de área local – LAN).**
Objetivo	Asegurar la operación correcta y segura de los puntos de red

A quién aplica	La Comunidad.
quién Implementa	Líder de Seguridad de la Información (Analista de TI)

Directrices

a) Los usuarios deberán emplear los puntos de red, para la conexión de equipos informáticos de propiedad de DESTINAR FMI.

b) Los equipos de uso personal, que no son de propiedad de DESTINAR, solo tendrán acceso a servicios limitados destinados a invitados o visitantes, estos equipos deben ser conectados a los puntos de acceso autorizados y definidos por el Analista de TI.

c) La instalación, activación y gestión de los puntos de red es responsabilidad del Analista de TI.

3.29 Política de uso de impresoras y del servicio de Impresión

Política	**Política de uso de impresoras y del servicio de Impresión**.
Objetivo	Asegurar la operación correcta y segura de las impresoras y del servicio de impresión.
A quién aplica	La Comunidad.
quién Implementa	Líder de Seguridad de la Información (Analista de TI)

Directrices

a) Los documentos que se impriman en las impresoras de DESTINAR FMI deben ser de carácter institucional.

b) Es responsabilidad del usuario conocer el adecuado manejo de los equipos de impresión (escáner y fotocopiado) para que no se afecte su correcto funcionamiento.

c) Ningún usuario debe realizar labores de reparación o mantenimiento de las impresoras. En caso de presentarse alguna falla, esta se debe reportar al Analista de TI.

d) Los funcionarios en el momento de realizar impresiones de documentos con clasificación Uso Interno o Restringida, debe mantener control de la impresora, por lo cual no la deberán dejar desatendida, preservando la confidencialidad de la información.

3.30 Política de controles criptográficos

Política	**Política de controles criptográficos**
Objetivo	Implementar actividades para proteger activos de información clasificada, fortaleciendo la confidencialidad, disponibilidad e integridad, mediante el uso de herramientas criptográficas.
A quién aplica	La Comunidad.
quién Implementa	Líder de Seguridad de la Información (Analista de TI)

Directrices

a) El Analista de TI debe verificar los sistemas o aplicaciones que realicen y/o permitan la transmisión de información Uso Interno y/o Restringida, lo realicen mediante herramientas de cifrado de datos.

b) El Analista de TI proveerá la herramienta de encripción datos a los usuarios, previa solicitud formal.

c) La asignación de la clave para el cifrado de la información en la herramienta, debe ser establecida por el usuario que administra dicha información, teniendo siempre presente que en caso de olvidar la clave, la información cifrada no es recuperable.

d) La contraseña de cifrado debe cumplir con la política de establecimiento de contraseñas de DESTINAR.

e) Asegurar que la información clasificada como Uso Interno y/o Restringida, sea protegida por el usuario final generador de la información, con el uso de la herramienta de encripción para transferencias de archivos con esta clasificación, por medio de los sistemas de información y comunicaciones.

f) El Analista de TI debe transmitir y/o almacenar la información clasificada como Uso Interno y/o Restringida con técnicas de cifrado.

g) El Analista de TI establecerá los lineamientos de administración, protección y ciclo de vida de las llaves criptográficas.

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

3.31 Política de Seguridad Física

Política	**Política de Seguridad Física**.
Objetivo	Implementar el programa de seguridad física de para el acceso a las instalaciones, centros de datos y centros de cableado que permita fortalecer la integridad, disponibilidad e integridad la información
A quién aplica	r) La Comunidad.
quién Implementa	s) Líder de Seguridad de la Información (Analista de TI)
Directrices	

a) El Área Administrativa debe implementar un sistema de seguridad física para las instalaciones de DESTINAR. Teniendo en cuenta control de incendio, así como planes integrales a las instalaciones para prevenir inundaciones, humedad o desastres naturales en los Rack y equipos activos. Preguntar a Indelsy Sistema gestion

b) El Analista de TI debe implementar barreras y sistemas de control de acceso a las instalaciones, centros de datos y centros de cableado de existir. En caso contrario asegurar los rack con llave.

c) El Analista de TI informará las debilidades que encuentren a nivel de barreras físicas a la Área Administrativa de DESTINAR para aprobación y corrección.

d) El Analista de TI deberá implementar protecciones que eviten o mitiguen daños causados por incendios, inundaciones y otros desastres naturales o generados por el hombre a los centros de datos y centros de cableado.

3.32 Políticas de seguridad de los Equipos

Política	**Políticas de seguridad de los Equipos**
Objetivo	Asegurar la protección de la información en los equipos
A quién aplica	La Comunidad.
quién Implementa	Líder de Seguridad de la Información (Analista de TI)
Directrices	

a) Instalación de equipos de procesamiento y almacenamiento
Los equipos de procesamiento y almacenamiento deben ser instalados en las áreas de trabajo seguras definidas por el Analista de TI.

b) Protecciones en el suministro de energía

A la red de energía regulada de los puestos de trabajo solo se pueden conectar equipos como computadores, pantallas; los otros elementos deberán conectarse a la red no regulada. Esta labor debe ser revisada por el Analista de TI.

El Área Administrativa de DESTINAR debe implementar sistemas redundantes de alimentación eléctrica, como por ejemplo: UPS para soportar la operación de los sistemas de información durante una falta de suministro de un proveedor de energía.

c) Seguridad del cableado

Los cables deben estar claramente marcados para identificar fácilmente los elementos conectados y evitar desconexiones erróneas.
Deben existir planos que describan las conexiones del cableado.
El acceso a los centros de cableado (Racks), debe estar protegido.
El Analista de TI establecerá un programa de revisiones y/o inspecciones físicas al cableado, con el fin de detectar dispositivos no autorizados. Esta revisión puede incluirse en la inspección de puestos de trabajo del Sistema de Gestion y Seguridad en el Trabajo.

d) Mantenimiento de los Equipos

DESTINAR FMI debe efectuar mantenimiento de los equipos críticos. Las actividades de mantenimiento tanto preventivo como correctivo deben registrarse para cada elemento.
Las actividades de mantenimiento de los servidores, elementos de comunicaciones, energía o cualquiera que pueda ocasionar una suspensión en el servicio, deben ser realizadas y programadas.

Los equipos que requieran salir de las instalaciones de DESTINAR para reparación o mantenimiento, deben estar debidamente autorizados por DESTINAR y se debe garantizar que en dichos elementos no se encuentra información clasificada de acuerdo a los niveles de clasificación de la información Restringida o de Uso Interno.

Para que los equipos puedan salir de las instalaciones, se debe suministrar un nivel mínimo de seguridad, que al menos cumpla con los requerimientos internos de la entidad, teniendo en cuenta los diferentes riesgos que se pueden presentar al trabajar en un ambiente que no cuenta con las protecciones ofrecidas en el interior de DESTINAR.
Los equipos retirados de la entidad deben ser protegidos, no se deben dejar sin vigilancia en lugares públicos, de igual forma se debe continuar con las recomendaciones de uso de los fabricantes de estos y la conexión con los sistemas de información de DESTINAR FMI debe cumplir con la política de control acceso.

Cuando un dispositivo vaya a ser reasignado o retirado de servicio debe contar con aprobación del Analista de TI, así mismo, debe garantizarse la eliminación de toda información residente en los elementos utilizados para el almacenamiento, procesamiento y transporte de la información, utilizando herramientas para realizar borrado seguro de la información..

e) Ingreso y retiro de activos de información de terceros.

El retiro e ingreso de todo activo de información de propiedad de los usuarios de DESTINAR, utilizados para fines personales, se realizará mediante los procedimientos establecidos por el sistema de seguridad física. DESTINAR no se hace responsable de los bienes o los problemas que se presenten al conectarse a la red eléctrica corporativa.
El retiro e ingreso de todo activo de información de los visitantes que presten servicios a DESTINAR (consultores, pasantes, visitantes, etc.) será registrado e inspeccionado en los controles de accesos de las instalaciones de la Entidad. El personal de seguridad y vigilancia en los controles de acceso verificarán y registrarán las características de identificación del activo de información.
El traslado entre áreas o procesos de DESTINAR de todo activo de información, está a cargo del área Administrativa para el control de inventarios.

***f)* Normas de protección**

Los funcionarios que hagan uso de los equipos de DESTINAR, no deben dejar desatendidos los equipos de cómputo en sitios públicos y deben transportarlos en lugares visibles bajo medidas que le provean seguridad física.
Los computadores portátiles siempre deben ser transportados como equipaje de mano, evitando golpes, exponerlo a líquidos y prevenir la perdida y/o hurto.

3.33 Política de escritorio y pantalla limpia.

Política	**Política de escritorio y pantalla limpia.**
Objetivo	Definir las pautas generales para reducir el riesgo de acceso no autorizado, pérdida y daño de la información durante y fuera del horario de trabajo normal de los usuarios.
A quién aplica	La Comunidad.
quién Implementa	Líder de Seguridad de la Información (Analista de TI)
Directrices	

a) El personal de DESTINAR FMI debe conservar su escritorio libre de información, que pueda ser alcanzada, copiada o utilizada por terceros o por personal que no tenga autorización para su uso o conocimiento.

b) El personal de DESTINAR FMI debe bloquear la pantalla de su computador con el protector de pantalla, en los momentos que no esté utilizando el equipo o cuando por cualquier motivo deba dejar su puesto de trabajo.

c) Los usuarios de los sistemas de información y comunicaciones de DESTINAR FMI deberán cerrar las aplicaciones y servicios de red cuando ya no los necesite.

d) Los usuarios a los que DESTINAR les asigne equipos móviles como computadores, teléfonos inteligentes, tablets, deben activar el bloqueo de teclas o pantalla, que permita evitar el acceso no autorizado a estos dispositivos.

e) Al imprimir documentos con información Uso Interno o Restringida, deben ser retirados de la impresora inmediatamente y no se deben dejar en la impresora sin custodia.

f) No se debe utilizar fotocopiadoras, escáneres, equipos de fax, cámaras digitales y en general equipos tecnológicos que se encuentren desatendidos.

g) La información Uso Interno y Restringida que se encuentre en medio físico, es deber del Área Administrativa colocar las medidas de seguridad pertinentes.

h) Los documentos que se encuentran en archivo de Gestion en cada puesto de trabajo deben ser almacenados bajo llave en gabinetes y/u otro tipo de mobiliario seguro, cuando no están siendo utilizados, especialmente fuera del horario de trabajo.

3.34 Política de respaldo y restauración de información

Política	**Política de respaldo y restauración de información**
Objetivo	Proporcionar medios de respaldo adecuados para asegurar que toda la información esencial y el software, se pueda recuperar después de una falla.
A quién aplica	La Comunidad.
quién Implementa	Líder de Seguridad de la Información (Analista de TI)

Directrices

a) La información de cada sistema debe ser respaldada sobre un medio de almacenamiento en DVD. Se debe empezar a contemplar servicio de almacenamiento en la nube, cuando financieramente se permita.

b) El analista de TI es el responsable de definir la frecuencia de respaldo y los requerimientos de seguridad de la información (codificación), lo cual se detalla en el instructivo GTI-PD01-IT01.Procedimiento Generación y custodias de Copias se Seguridad

c) Todas las copias de información crítica deben ser almacenadas en un área adecuada y con control de acceso.

d) Las copias de respaldo se guardaran únicamente con el objetivo de restaurar el

sistema luego de la infección de un virus informático, defectos en los discos de almacenamiento, problemas de los servidores o computadores, materialización de amenazas, catástrofes y por requerimiento legal.

e) Debe ser desarrollado un plan de emergencia para todas las aplicaciones que manejen información crítica; el dueño de la información debe asegurar que el plan es adecuado, frecuentemente actualizado y periódicamente probado y revisado.

f) Ningún tipo de información institucional puede ser almacenada en forma exclusiva en los discos duros de las estaciones de trabajo; por lo tanto, es obligación del Analista de TI realizar las copias en las carpetas destinadas para este fin.

g) La restauración de copias de respaldo en ambientes de producción debe estar debidamente aprobada por el propietario de la información.

h) Semanalmente los administradores de infraestructura de DESTINAR, verificarán la correcta ejecución de los procesos de backup y se registrara dicha verificación GTI-PD01-F05-Bitácora de Soporte Técnico.

i) El Analista de TI debe mantener un inventario actualizado de las copias de respaldo de la información y los aplicativos o sistemas de DESTINAR. GTI-PD01-F04-Bitácora de copias de seguridad.

j) Los medios que vayan a ser eliminados deben surtir un proceso de borrado seguro y posteriormente serán eliminados o destruidos de forma adecuada. GTI-PD01-IT04.Borrado Seguro de la información

k) Es responsabilidad de cada dependencia mantener depurada la información de las carpetas virtuales para la optimización del uso de los recursos de almacenamiento que entrega DESTINAR a los usuarios.

l) En el evento de retiro de un funcionario o traslado de dependencia, previa notificación del Área de Talento Humano, el Analista de TI generará una copia de la información contenida en el equipo asignado específicamente a la carpeta Uso Interno del año actual y al pst del correo electrónico y; a la carpeta virtual del usuario, ubicada en el servidor de DESTINAR FMI.

m) Ningún usuario final debe realizar copias de la información contenida en la estación de trabajo a medios extraíbles de información, excepto aquellos que se encuentren con privilegios de escritura habilitados por puertos USB.

n) En caso de presentarse alguna falla en los equipos de cómputo, se debe reportar al Analista de TI y en caso de requerirse copia de la información, ésta se realizará de manera temporal durante las diferentes labores de reparación o mantenimiento.

o) Ningún usuario debe utilizar equipo diferente al asignado para copiar algún tipo de archivo, excepto al autorizado por jefe inmediato.

3.35 Política de registro y seguimiento de eventos de sistemas de información y comunicaciones

Política	**Política de registro y seguimiento de eventos de sistemas de información y comunicaciones**
Objetivo	Preservar la integridad, confidencialidad y disponibilidad de los registros de eventos (logs) generados por los sistemas de información y comunicaciones de Destinar FMI
A quién aplica	La Comunidad.
quién Implementa	Líder de Seguridad de la Información (Analista de TI)

Directrices

a) El Analista de TI debe implementar los lineamientos para elaborar, preservar y revisar los registros de actividades (logs) de los usuarios de los sistemas del DESTINAR.

b) El Analista de TI, no están facultados para modificar, borrar o desactivar registros (logs) de sus actividades propias, ni de los usuarios de los sistemas de información y telecomunicaciones, de igual forma se deben realizar las configuraciones de seguridad necesarias para evitar la eliminación o cambios no autorizados a los registros de información.

c) El acceso a los registros (logs) es restringido, por lo cual su consulta por usuarios se debe realizar con previa autorización del Gerente General.

d) La consulta y copia de la información de registros que se requiera con fines probatorios debe ser solicitada por autoridad judicial a la Gerencia General.

e) El Analista de TI deberá realizar copias de respaldo de los registros de auditoria.

f) El Analista de TI debe proteger y auditar periódicamente los registros de actividades (logs) de los administradores de los sistemas de información y telecomunicaciones

g) El Analista de TI debe implementar la sincronización de relojes de los sistemas de información a un único servidor NTP (Nertwork Time Protocol – protocolo de tiempo en la red)

3.36 Política de uso de correo electrónico

Política	**Política de uso de correo electrónico**
Objetivo	Definir las pautas generales para asegurar una adecuada protección de la información de DESTINAR FMI, en el servicio y uso del servicio de correo electrónico por parte de los usuarios autorizados.
A quién aplica	La Comunidad.
quién Implementa	Líder de Seguridad de la Información (Analista de TI)

Directrices

Esta política define y distingue el uso de correo electrónico aceptable/apropiado e inaceptable/inapropiado y establece las directrices para el uso seguro del servicio.
Los funcionarios de DESTINAR deberán hacer uso del correo electrónico institucional suministrado por el Analista de TI, para desarrollar las actividades oficiales inherentes al cargo asignado.
La cuenta de correo oficial para el cumplimiento de las funciones desempeñadas para DESTINAR, es la cuenta de correo electrónico institucional suministrado por el Analista de TI.

Principios guía

a) Los usuarios del correo electrónico corporativo son responsables de evitar prácticas o usos del correo que puedan comprometer la seguridad de la información.

b) Los servicios de correo electrónico corporativo se emplean para servir a una finalidad operativa y administrativa en relación con la entidad. Todos los correos electrónicos procesados por los sistemas, redes y demás infraestructura tecnologica de DESTINAR se consideran bajo el control de la entidad.

c) Este servicio debe utilizarse exclusivamente para las tareas propias de la función desarrollada en DESTINAR y no debe utilizarse para ningún otro fin.

d) No está autorizado el envío de cadenas de correo, envío de correos masivos con archivos adjuntos de gran tamaño que puedan congestionar la red.

e) No está autorizado el envío de correos con contenido que atenten contra la integridad y dignidad de las personas y el buen nombre de la entidad.

f) Cuando un funcionario, contratista o colaborador al que le haya sido autorizado el uso de una cuenta de correo electrónico y se retire de DESTINAR, su cuenta de correo será desactivada en 30 días.

g) Los correos electrónicos deben contener la siguiente nota respecto al manejo del

contenido:

NOTA CONFIDENCIAL. "La información contenida en este correo y en sus anexos y/o archivos adjuntos, es confidencial y tiene carácter reservado. La misma es propiedad de Destinar Fondo Mutuo de Ahorro e Inversión y está dirigida para conocimiento estricto de la persona o entidad destinataria(s), responsable(s) por su custodia y conservación. Si no es el receptor autorizado, cualquier retención, difusión, distribución o copia de este mensaje es prohibida y será sancionada por la ley. Si por error recibe este mensaje, borrar el mensaje recibido inmediatamente. La compañía no es responsable por la transmisión de virus informáticos, ni por las opiniones expresadas en este mensaje, ya que estas son exclusivas del autor.

h) El tamaño del buzón de correo electrónico estará determinado por el rol desempeñado por el usuario en DESTINAR y a las condiciones del proveedor del servicio.
i) Cada área deberá solicitar la creación de las cuentas electrónicas, sin embargo, las áreas de Recursos Humanos y de Contratación son las responsables de solicitar la modificación o cancelación de las cuentas electrónicas al Analista de TI DESTINAR.
j) Las cuentas de correo electrónico son propiedad de DESTINAR, las cuales son asignadas a personas que tengan algún tipo de vinculación laboral con la entidad, ya sea como personal de planta, en comisión permanente, contratistas, consultores o personal temporal, quienes deben utilizar este servicio única y exclusivamente para las tareas propias de la función desarrollada en DESTINAR y no debe utilizarse para ningún otro fin.
k) Cada usuario es responsable del contenido del mensaje enviado y de cualquier otra información adjunta al mismo, de acuerdo a la clasificación de la información establecida por DESTINAR.
l) Todos los mensajes pueden ser sujetos a análisis y conservación permanente por parte de DESTINAR.
m) Todo usuario es responsable por la destrucción de los mensajes cuyo origen sea desconocido y por lo tanto asumirá la responsabilidad y las consecuencias que puede ocasionar la ejecución de cualquier archivo adjunto. En estos casos no se debe contestar dichos mensajes, ni abrir los archivos adjuntos.
n) El único servicio de correo electrónico autorizado en la entidad es el asignado por el Analista de TI.

3.37 Políticas específicas para el rol de Webmaster.

Política	**Políticas específicas para el rol de Webmaster.**
Objetivo	Proteger la integridad de las páginas Web institucionales, el software y la información contenida.
A quién aplica	Analista de IT.
quién Implementa	Líder de Seguridad de la Información (Analista de TI)
Directrices	

a) El Analista de TI es responsable de los contenidos de las páginas Web (*webmasters*), debe tramitar los requerimientos de actualización de la página web; y debe reportar en GTI-PD01-F05-Bitácora de Soporte Técnico la información de la página inicial del sitio; y el cambio solicitado.

b) Se deberá seguir la Política Editorial y Actualización de Contenidos Web, que permita auditar la publicación o modificación de información oficial en las páginas web.

c) Las claves de acceso a los contenidos de las páginas Web (*webmasters*), son estrictamente confidenciales, personales e intransferibles.

3.38 Políticas específicas para funcionarios y contratistas del Área de Tecnología y Sistemas de la Información

Política	**Políticas específicas para funcionarios y contratistas del Área de Tecnología y Sistemas de la Información**
Objetivo	Definir las pautas generales para asegurar una adecuada protección de la información de DESTINAR por parte de los funcionarios y contratistas de TI de la entidad.
A quién aplica	La Comunidad.
quién Implementa	Líder de Seguridad de la Información (Analista de TI)

Directrices

a) El Analista de TI no debe dar a conocer su clave de usuario a terceros de los sistemas de información, sin previa autorización del Gerente General.

b) Los usuarios y claves de los administradores de sistemas y del Analista de TI son de uso personal e intransferible.

c) El Analista de TI debe emplear obligatoriamente las claves o contraseñas con un alto nivel de complejidad y utilizar los servicios de autenticación fuerte, siempre y cuando los aplicativos lo permitan.

d) Los administradores de los sistemas de información deben seguir las políticas de cambio de clave y utilizar procedimiento de salvaguarda o custodia de las claves o contraseñas en un sitio seguro.

e) Los documentos y en general la información de procedimientos, seriales, software etc.

deben mantenerse custodiados en todo momento para evitar el acceso a personas no autorizadas.

f) Los funcionarios encargados de realizar la instalación o distribución de software, sólo instalarán productos con licencia y software autorizado.

g) El Analista de TI no deben otorgar privilegios especiales a los usuarios sobre las estaciones de trabajo, sin la autorización correspondiente del Gerente General.

h) El analista de TI se obligan a no revelar a terceras personas, la información a la que tengan acceso en el ejercicio de sus funciones de acuerdo con la guía de clasificación de la información según sus niveles de seguridad. En consecuencia, se obligan a mantenerla de manera confidencial y privada y a protegerla para evitar su divulgación.

i) El analista de TI no utilizarán la información para fines comerciales o diferentes al ejercicio de sus funciones.

j) Toda licencia de software o aplicativo informático y sus medios, se deben guardar y relacionar de tal forma que asegure su protección y disposición en un futuro.

k) Las copias licenciadas y registradas del software adquirido, deben ser únicamente instaladas en los equipos y servidores de la entidad. Se deben hacer copias de seguridad en concordancia con las políticas del proveedor y de la entidad.

l) El acceso a cualquier servicio, servidor o sistema de información debe ser autenticado y autorizado.

m) Todos los servidores deben ser configurados con el mínimo de servicios necesarios y obligatorios para desarrollar las funciones designadas. Por defecto deben ser bloqueados, todos los protocolos y servicios que no se requieran en los servidores.

n) Todo software tipo freeware o shareware, debe ser instalado en un ambiente de prueba, el Analista de TI debe efectuar las verificaciones para autorizar la instalación del producto en producción.

3.39 Política de Tercerización u Outsourcing.

Política	**Política de Tercerización u Outsourcing.**
Objetivo	Mantener la seguridad de la información y los servicios de procesamiento de información, a los cuales tienen acceso terceras partes, entidades externas o que son procesados, comunicados o dirigidos por estas.

A quién aplica	La Comunidad.
quién Implementa	Líder de Seguridad de la Información (Analista de TI)

Directrices

a) Se deben establecer criterios de selección que contemplen la experiencia y reputación de terceras partes, certificaciones y recomendaciones de otros clientes, estabilidad financiera de la compañía, seguimiento de estándares de gestión de calidad y de seguridad y otros criterios que resulten de un análisis de riesgos de la selección y los criterios establecidos por la entidad.

b) Se debe establecer mecanismos de control en las relaciones contractuales, con el objetivo de asegurar que la información a la que tengan acceso o servicios que sean provistos por los proveedores o contratistas, cumplan con las políticas de seguridad de la información de DESTINAR FMI, las cuales deben se divulgadas por los funcionarios responsables de la realización y/o firma de contratos o convenios.

c) En los contratos o acuerdos con los proveedores y/o contratistas se debe incluir una causal de terminación del acuerdo o contrato de servicios, por el no cumplimiento de las políticas de seguridad de la información

d) Los contratistas, oferentes y/o proveedores deben aceptar y firmar el acuerdo de confidencialidad establecido por DESTINAR FMI.

e) El analista de TI deberá mitigar los riesgos de seguridad con referencia al acceso de los proveedores y/o contratistas a los sistemas de información de DESTINAR FMI.

f) Se debe identificar y monitorear los riesgos relacionados con los contratistas o proveedores en relación a los objetos contractuales, incluyendo la cadena de suministro de los servicios de tecnología y comunicación.

g) Se deben identificar los riesgos para la información y los servicios de procesamiento de información que involucren partes externas DESTINAR FMI. El resultado del análisis de riesgos será la base para el establecimiento de los controles y debe ser presentado al Gerente General antes iniciar el estudio de mercado y publicación del proyecto de pliegos del contrato de *outsourcing*.

h) Los funcionarios de DESTINAR FMI que fungen como supervisores de contratos relacionados con sistemas de información deberán realizar seguimiento, control y revisión de los servicios suministrados por los proveedores y/o contratistas.

Se deben establecer mecanismos o condiciones con los contratistas o proveedores que permitan realizar la gestión de cambios en los servicios suministrados.

3.40 Política de Gestión de los Incidentes de la Seguridad de la Información

Política	**Política de Gestión de los Incidentes de la Seguridad de la Información**
Objetivo	Asegurar que los eventos e incidentes de seguridad que se presenten con los activos de información, sean comunicados y atendidos oportunamente, empleando los procedimientos definidos, con el fin de que se tomen oportunamente las acciones correctivas
A quién aplica	La Comunidad.
quién Implementa	Líder de Seguridad de la Información (Analista de TI)
Directrices	

a) DESTINAR FMI establecerá responsables y procedimientos de gestión para el tratamiento de incidentes de seguridad de la información asegurando una respuesta rápida, eficaz y eficiente, quienes investigarán y solucionarán los incidentes presentados, implementando las acciones necesarias para evitar su repetición, así mismo, debe escalar los incidentes de acuerdo con la criticidad del mismo.

b) El único canal acreditado para reportar incidentes de seguridad ante las autoridades y el pronunciamiento oficial ante entidades externas de DESTINAR es el Gerente General o quien este delegue.

c) Se debe establecer la implementación de lecciones aprendidas al término del análisis y solución de incidentes de seguridad de la información, estos deben ser socializados a los interesados conservando la confidencialidad de estas, así mismo, estas deben ser utilizadas como herramienta para la toma de decisiones y revisiones de la política de seguridad.

3.41 Política para la Gestión de la Continuidad de Seguridad de la Información

Política	**Política para la Gestión de la Continuidad de Seguridad de la Información**
Objetivo	Asegurar la continuidad de la seguridad de la información en situaciones de crisis o desastres
A quién aplica	La Comunidad.
quién Implementa	Líder de Seguridad de la Información (Analista de TI)
Directrices	

a) El Líder de Seguridad de la Información (Analista de TI) establecerá el Plan de

Continuidad del Negocio para la entidad, este debe incluir el plan de recuperación de desastres.

b) Se debe generar el plan de continuidad de seguridad de la información, documentado e implementando procesos y procedimientos para asegurar la continuidad requerida por la Entidad.

c) El analista de TI elaborará el plan de recuperación de desastres para los sistemas de información y comunicación de DESTINAR, el cual debe incluir mínimo procedimientos, condiciones de seguridad, recuperación y retorno a la normalidad.

d) El plan de continuidad del negocio de la entidad se debe verificar, revisar y evaluar, por la Auditoria Interna durante el desarrollo del plan anual de auditorías.

e) DESTINAR FMI propenderá por la implementación de una plataforma tecnológica redundante que satisfaga los requerimientos de disponibilidad necesarios para la Entidad, así como programación y ejecución de pruebas de funcionalidad de esta.

Nota: El numeral e) depende de la disponibilidad financiera del fondo. Si se evidencia dificultad con respecto al proveedor por el tamaño del fondo, documentar una soluciona alternativa.

f) El analista de TI debe analizar y establecer los requerimientos mínimos de redundancia para los sistemas de información críticos de DESTINAR FMI junto con la plataforma tecnológica que los soporta, de igual forma deberá investigar, evaluar y probar las soluciones de tecnología que supla la necesidad del Fondo.

3.42 Política de uso de mensajería instantánea y redes sociales.

Política	**Política de uso de mensajería instantánea y redes sociales.**
Objetivo	Definir las pautas generales para asegurar una adecuada protección de la información de Destinar FMI, en el uso del servicio de mensajería instantánea y de las redes sociales, por parte de los usuarios autorizados.
A quién aplica	La Comunidad.
quién Implementa	Líder de Seguridad de la Información (Analista de TI)
Directrices	
a) El uso de servicios de mensajería instantánea y el acceso a redes sociales estarán autorizados a los usuarios, teniendo en cuenta sus funciones y para facilitar canales de comunicación con los afiliados y proveedores.	

b) No se permite el envío de mensajes con contenido que atente contra la integridad de las personas, instituciones o cualquier contenido que represente riesgo de código malicioso.

c) La información que se publique o divulgue por cualquier medio de Internet, de cualquier funcionario, contratista o colaborador de DESTINAR, que sea creado a nombre personal en redes sociales como: *twitter*®, *facebook*®, *youtube*® likedink®, *blogs, instagram, etc.,* se considera fuera del alcance de la política de seguridad de la información de Destinar FMI y por lo tanto su confiabilidad, integridad, disponibilidad y los daños y perjuicios que pueda llegar a causar serán de completa responsabilidad de la persona que las haya generado.

d) Toda información distribuida en las redes sociales que sean originadas por la entidad deben ser autorizadas por los responsables de cada proceso para ser socializadas y con un vocabulario institucional.

e) No se debe utilizar el nombre de la entidad en las redes sociales para difamar o afectar la imagen y reputación de los seguidores cuando responden comentarios en contra de la filosofía de la institución.

4. Proceso Disciplinario

Dentro de la estrategia de seguridad de la información de DESTINAR FMI, está establecido un proceso disciplinario formal para los funcionarios que hayan cometido alguna violación de la Política de Seguridad de la Información. El proceso disciplinario también se debería utilizar como disuasión para evitar que los funcionarios, contratistas y los otros colaboradores de DESTINAR FMI 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 al proceso de gestión del Área de Talento Humano **Ver GTH--08 Procedimiento Disciplinario Ordinario.**

Actuaciones que conllevan a la violación de la seguridad de la información establecida por DESTINAR FMI:

1) No firmar los acuerdos de confidencialidad o de entrega de información o de activos de información.
2) Ingresar a carpetas de otros procesos o áreas, sin autorización con intención de manipular, borrar o adulterar la información.
3) No reportar los incidentes de seguridad o las violaciones a las políticas de seguridad, cuando se tenga conocimiento de ello.
4) No actualizar la información de los activos de información a su cargo.

5) Clasificar y registrar de manera inadecuada la información, desconociendo los estándares establecidos para este fin.
6) 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 de uso interno y restringida*".
7) No guardar la información digital, producto del procesamiento de la información perteneciente a su proceso en las carpetas oficiales.
8) Dejar información Uso interno, en carpetas compartidas o en lugares distintos al servidor de archivos, obviando las medidas de seguridad.
9) Dejar las gavetas abiertas o con las llaves puestas en los escritorios,
10) Dejar los computadores encendidos en horas no laborables.
11) Permitir que personas ajenas a DESTINAR FMI, deambulen sin acompañamiento, al interior de las instalaciones, en áreas no destinadas al público.
12) Almacenar en los discos duros de los computadores personales de los usuarios, la información de la entidad.
13) Solicitar cambio de contraseña de otro usuario, sin la debida autorización del titular o su jefe inmediato.
14) Hacer uso de la red de datos del fondo, 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.
15) Utilización de software no relacionados con la actividad laboral y que pueda degradar el desempeño de la plataforma tecnológica institucional.
16) Recibir o enviar información institucional a través de correos electrónicos personales, diferentes a los asignados por la institución.
17) Enviar información Uso Interno con clasificación Restringida por correo, copia impresa o electrónica sin la debida autorización y sin la utilización de los protocolos establecidos para la divulgación.
18) Utilizar equipos electrónicos o tecnológicos desatendidos o que a través de sistemas de interconexión inalámbrica, sirvan para transmitir, recibir y almacenar datos.
19) Usar dispositivos de almacenamiento externo en los computadores, cuya autorización no haya sido otorgada por el Analista de TI de DESTINAR FMI.
20) Permitir el acceso de personas externas a la red corporativa, sin la autorización del Analista de TI.
21) Utilización de servicios disponibles a través de internet, como FTP y Telnet, no permitidos por DESTINAR FMI o de protocolos y servicios que no se requieran y que puedan generar riesgo para la seguridad.
22) Negligencia en el cuidado de los equipos, dispositivos portátiles o móviles entregados para actividades propias de DESTINAR FMI.
23) No cumplir con las actividades designadas para la protección de los activos de información de DESTINAR FMI.
24) Destruir o desechar de forma incorrecta la documentación institucional.
25) Descuidar documentación con información Restringida o clasificada de la entidad, sin las medidas apropiadas de seguridad que garanticen su protección.
26) Registrar información Restringidas o datos sensibles de a los afiliados, en pos-it, apuntes, agendas, libretas, etc. Sin el debido cuidado.

27) Almacenar información de Uso Interno y Restringida, en cualquier dispositivo de almacenamiento que no permanezca a DESTINAR FMI o conectar computadores portátiles u otros sistemas eléctricos o electrónicos personales a la red de datos de DESTINAR FMI, sin la debida autorización.
28) Archivar información Restringida, sin claves de seguridad o cifrado de datos.
29) Promoción o mantenimiento de negocios personales, o utilización de los recursos tecnológicos de DESTINAR FMI para beneficio personal.
30) El que sin autorización acceda en todo o parte del sistema informático o se mantenga dentro del mismo en contra de la voluntad de DESTINAR FMI.
31) El que impida u obstaculice el funcionamiento o el acceso normal al sistema informático, los datos informáticos o las redes de telecomunicaciones de DESTINAR FMI, sin estar autorizado.
32) El que destruya, dañe, borre, deteriore o suprima datos informáticos o un sistema de tratamiento de información de DESTINAR FMI.
33) El que distribuya, envíe, introduzca software malicioso u otros programas de computación de efectos dañinos en la plataforma tecnológica de DESTINAR FMI.
34) El que viole datos personales de las bases de datos de DESTINAR FMI.
35) El que superando las medidas de seguridad informática suplante un usuario ante los sistemas de autenticación y autorización establecidos por DESTINAR FMI.
36) No mantener la confidencialidad de las contraseñas de acceso a la red de datos, los recursos tecnológicos o los sistemas de información de DESTINAR FMI o permitir que otras personas accedan con el usuario y clave del titular a éstos.
37) Permitir el acceso u otorgar privilegios de acceso a las redes de datos de DESTINAR FMI a personas no autorizadas.
38) Llevar a cabo actividades fraudulentas o ilegales, o intentar acceso no autorizado a cualquier computador de DESTINAR FMI o de terceros.
39) Ejecutar acciones tendientes a eludir o variar los controles establecidos por DESTINAR FMI.
40) Retirar de las instalaciones de la institución, estaciones de trabajo o computadores portátiles que contengan información institucional sin la autorización pertinente.
41) Sustraer de las instalaciones de DESTINAR FMI, documentos con información institucional calificada como información pública reservada o clasificada, o abandonarlos en lugares públicos o de fácil acceso.
42) Entregar, enseñar y divulgar información institucional, calificada como información pública reservada y clasificada a personas o entidades no autorizadas.
43) No realizar el borrado seguro de la información en equipos o dispositivos de almacenamiento de DESTINAR FMI, para traslado, reasignación o para disposición final.
44) Ejecución de cualquier acción que pretenda difamar, abusar, afectar la reputación o presentar una mala imagen de DESTINAR FMI o de alguno de sus funcionarios.
45) Realizar cambios no autorizados en la plataforma tecnológica de DESTINAR FMI.
46) Acceder, almacenar o distribuir pornografía infantil.
47) Instalar programas o software no autorizados en las estaciones de trabajo o equipos portátiles institucionales, cuyo uso no esté autorizado por el Área de Tecnología y Sistemas de Información de DESTINAR FMI.
48) Copiar sin autorización los programas de DESTINAR FMI, o violar los derechos de autor o acuerdos de licenciamiento.

CONTROL DE CAMBIOS			
No. versión	**Ítem del Cambio**	**Cambio realizado**	**Fecha del cambio**
1.0	NA	NA	NA

CONTROL DE DOCUMENTOS		
Elaborado Por: José Nicolai Cárdenas Pulido. Analista TI	**Revisado Por:** Diego Alexander Triana Gómez Gerente General	**Aprobado Por**: Diego Alexander Triana Gómez Gerente General Fecha Aprobación: 29/01/2019 ACTA JUNTA DIRECTIVA No.370