1. PROPOSITO

Este documento describe las políticas y normas de seguridad de la información definidas por FUNDELIMA SA con el fin de apoyar la gestión y administración de los planes y procedimientos de seguridad de la información, dando claridad sobre las prácticas de seguridad aplicadas en la organización.

2. ALCANCE

Las políticas de Seguridad de la información cubren todos los aspectos administrativos y de control que deben ser cumplidos por los directivos, empleados y terceros que laboren o tengan relación con Fundiciones De Lima SA, y así lograr un adecuado nivel de protección de las características de seguridad y calidad de la información relacionada.

3. DOCUMENTOS DERIVADOS

- Acuerdo de confidencialidad empleados
- Autorización de uso de tecnología para implementación de acciones de control y vigilancia
- Acuerdo de confidencialidad proveedores / contratistas FGR-04
- Autorización de tratamiento de datos personales FGR-02
- Política para tratamiento de datos personales POGR-02
- Registro de incidentes de seguridad de la información FGR-05

4. NORMATIVIDAD RELACIONADA.

- CONSTITUCIÓN POLÍTICA DE COLOMBIA 1991.
  - ✓ Artículo 15. Reconoce como Derecho Fundamental el Habeas Data.
  - ✓ Artículo 20. Libertad de Información.
- LEY 1581 DE 2012
- DECRETO 1377 DE 2013
- NORMA ISO- IEC 27001: 2013
- LEY 2157 DEL 29 DE OCTUBRE DE 2021
- DECRETO 255 de 2022

5. COMPROMISO DE LA DIRECCION

La Junta Directiva y Alta Dirección de Fundiciones De Lima SA, aprueba este Manual como muestra de su compromiso y apoyo en el diseño de Políticas de Seguridad y asignación de recursos eficientes que garanticen la seguridad de la información de la empresa.

6. APLICABILIDAD DE LAS POLITICAS DE SEGURIDAD DE LA INFORMACIÓN

Las políticas de Seguridad de la Información aplican y son de obligatorio cumplimiento para toda persona que labore en Fundiciones De Lima de manera directa o Indirecta, o todo aquel proveedor, contratista, cliente, visitante o persona perteneciente a empresas asociadas, que tengan acceso a cualquier medio, sistema de información o plataforma tecnológica en los cuales se procese información de la empresa.

7. POLITICAS DE SEGURIDAD DE LA INFORMACIÓN

7.1 Política General de Seguridad de la Información

FUNDICIONES DE LIMA SA reconoce la importancia de identificar y proteger sus activos de información, por lo cual se compromete a definir, coordinar y controlar la gestión necesaria para mitigar los riesgos asociados a la seguridad de la información de la organización.

7.2 Política de Estructura Organizacional de Seguridad de la Información.

NIVEL	NOMBRE	RESPONSABLE	COMPROMISOS
I	Gerencial	Gerente	✓ Definir y establecer los roles y responsabilidades relacionados con la seguridad de la información. ✓ Revisar y aprobar las Políticas de Seguridad de la Información contenidas en el presente manual. ✓ Facilitar la divulgación de las Políticas de Seguridad de la Información a todos los empleados de la organización y al personal provisto por terceras partes. ✓ Asignar los recursos, la infraestructura física y el personal necesario para la gestión de la seguridad de la información de la organización. ✓ Coordinar la creación del Comité de Seguridad de la Información. ✓ Designar el Coordinador de Seguridad de la Información.
II	Coordinador de Seguridad de La Información.	Dir. Administrativo	✓ Determinar los niveles de acceso a la información. ✓ Coordinar las acciones del Comité de Seguridad e impulsar la implementación y cumplimiento de la presente Política.

			✓ Asegurar la Seguridad de los sistemas de información y sistemas Informáticos. ✓ Documentar y mantener actualizada la información, y definir qué usuarios deberán tener permisos de acceso a la información y sistemas informáticos, de acuerdo a sus funciones, perfiles y competencias. ✓ Regular cambios y mejoras al sistema en cuanto a: objetivos, adecuación del alcance y política. ✓ Administrar el proveedor de Sistemas y garantizar el cumplimiento óptimo de su gestión.
III	Líder de Sistemas	AS Sistemas	✓ Deberá asesorar todos los aspectos de seguridad informática y recomendar las herramientas necesarias para que puedan ser ejercidas. ✓ Deberá participar en la definición de la seguridad informática de los sistemas que traten la información o los ambientes bajo su responsabilidad. ✓ Deberá velar porque el software de seguridad de la plataforma tecnológica que se encuentre instalado se mantenga siempre actualizado y sólo instalarán productos con licencia y software autorizado. ✓ Deberá participar en la definición de la seguridad física de los centros de cómputo donde reside la información de Fundelima S.A. y de la estructura de red. ✓ Participará en la definición del plan de contingencia de Fundelima S.A. ✓ Deberá mantener informado a los usuarios sobre las políticas, normas, procedimientos y estándares de seguridad informática.

			✓ Deberán establecer e implantar planes de formación sobre medidas de seguridad informática. ✓ Garantizar que los documentos y en general la información de procedimientos, seriales, software etc. Se mantengan custodiados en todo momento para evitar el acceso a personas no autorizadas. ✓ Garantizar que para el cambio o retiro de equipos de funcionarios, se sigan políticas de saneamiento, es decir llevar a cabo mejores prácticas para la eliminación de la información de acuerdo al software disponible en la entidad. Ej: Formateo seguro, destrucción total de documentos o borrado seguro de equipos electrónicos. ✓ Los funcionarios del Área de Tecnología y Sistemas de Información no deben otorgar privilegios especiales a los usuarios sobre las estaciones de trabajo, sin la autorización correspondiente de la Gerencia o la Dirección Administrativa. ✓ No utilizarán la información para fines comerciales o diferentes al ejercicio de sus funciones.
IV	Comité de Seguridad de la Información	Dir. Administrativo Jefe Gestión Humana Jefe de Contabilidad Jefe de Cartera Asist. Administrativo Analista TIC Coord. SIG	✓ Realizar comités cada 4 meses para verificar el cumplimiento de la seguridad de la información. ✓ Revisar periódicamente el estado general de la seguridad de la información. ✓ Proponer modificaciones o nuevas políticas de seguridad de la información. ✓ Apoyo, revisión y regulación de los temas referentes a la seguridad de la información. ✓ Evaluar y coordinar la implementación de controles específicos de seguridad de la información en la organización. ✓ Monitorear los incidentes de seguridad de la información. ✓ Velar por el cumplimiento de las Políticas de la Seguridad de la Información expuestas en el presente manual.

V	Propietarios de los Activos de la Información	Responsables de Procesos Usuarios de la Información.	✓ Definir la clasificación de la información. ✓ Determinar los niveles de acceso a la información. ✓ Autorizar la asignación de permisos de acceso. ✓ Apoyar en la generación de los controles necesarios para el almacenamiento, procesamiento, distribución y uso de la información.
VI	Usuarios de la información	Empleados. Contratistas. Proveedores	Todos los empleados de Fundiciones De Lima SA. y personal que directa o indirectamente prestan sus servicios profesionales dentro de la empresa son responsables de la información que manejan y deberán cumplir los lineamientos establecidos para proteger y preservar la información a la cual accedan y procesen; evitando el uso indebido, accesos no autorizados, exposiciones, modificaciones y entrega a externos. Todo funcionario que utilice la infraestructura tecnológica de Fundiciones De Lima SA, tiene la responsabilidad de velar por la integridad, confidencialidad, disponibilidad y confiabilidad de la información que maneje, especialmente si dicha información está clasificada como confidencial y/o crítica; así mismo reportar los incidentes de seguridad, eventos sospechosos y el mal uso de los recursos que identifique.

7.3 Política de Seguridad para el Talento Humano

- ✓ **Selección de Personal**

Toda vinculación laboral realizada por Fundiciones De Lima SA, se rige por las leyes de la República de Colombia y por lo dispuesto en el Código Sustantivo de Trabajo.

Todo empleado contratado por Fundelima es seleccionado adecuadamente, de acuerdo con el perfil de cada cargo, y siguiendo las tareas descritas en el Procedimiento de Selección, Inducción y Capacitación del Personal PGH-01. En caso que el proceso de selección o contratación se realice por intermedio de terceros, la empresa debe asegurar la definición

clara de responsabilidades y los mecanismos para manejar el incumplimiento de los requisitos. Sin importar la forma de contratación, todo colaborador recibe y acepta las políticas de seguridad de la compañía.

El jefe de Gestión Humana es responsable de verificar la información brindada durante el proceso de vinculación del personal; así como de definir a qué cargos se les efectúa estudio de seguridad (Visita domiciliaria / Polígrafo).

- ✓ **Términos y condiciones de contratación**

El Jefe de Gestión Humana incluirá las funciones referentes a la seguridad de la información en las descripciones de las funciones de cada uno de los empleados e informará a todo el personal que ingresa, de sus obligaciones respecto del cumplimiento de la Política de Seguridad de la Información.

- ✓ **Compromisos de Confidencialidad**

Todos los empleados de Fundiciones De Lima SA o empleados en misión, que realicen labores en la organización y que involucre el manejo de información y de los sistemas de información, deben conocer, entender, firmar y aceptar el correspondiente acuerdo de confidencialidad, donde se comprometan a no divulgar, usar o explotar la información confidencial de Fundiciones De Lima SA. y proteger y hacer buen uso de la misma, respetando los niveles de clasificación en cuanto a criticidad y protección, por consecuente cualquier violación de lo establecido será considerado un incidente de seguridad y tendrá su sanción dependiendo la magnitud de los hechos: Llamado de atención, suspensión sin remuneración y/o terminación de contrato.

Toda persona que ingrese a laborar, debe firmar en su proceso de Inducción el ACUERDO DE CONFIDENCIALIDAD, el cuál debe reposar en su carpeta de empleado.

Se debe capacitar y sensibilizar al personal durante la inducción sobre las políticas de seguridad de la información.

Se debe asegurar que los empleados de Fundiciones De Lima SA, adopten sus responsabilidades en relación con las políticas de seguridad de la información actúen de manera consistente frente a las mismas, con el fin de reducir el riesgo de hurto, fraude, filtraciones o uso inadecuado de la información o los equipos empleados para el tratamiento de la información.

En situaciones de incumplimiento y/o violaciones a las políticas de seguridad de la información se deberá proceder de acuerdo a lo consignado en el Reglamento Interno de Trabajo.

- ✓ **Capacitación en seguridad de la información**

Todos los empleados recibirán una adecuada capacitación en materia de las políticas y procedimientos relativas a la seguridad de la información. Esto comprende los requerimientos de seguridad, las responsabilidades legales y el uso correcto de las instalaciones y de la información a su cargo.

- ✓ **Desvinculación del Personal**

Previo al retiro o cambio de cargo de alguno de los empleados, el Jefe de Gestión Humana deberá reportar por escrito al Coordinador de Seguridad de la Información la desvinculación o modificación del cargo con el fin de realizar las actividades de: Devolución de activos, des-habilitación de equipos de la red, des-habilitación de usuario de correo, dispositivos de seguridad físicos y biométricos. La vigencia de los derechos de acceso y su revocatoria, deben estar estrechamente relacionadas con la terminación de la relación laboral.

7.4 Política de Seguridad de Activos de Información

7.4.1 Clasificación de Activos

Los propietarios de la información y el Coordinador de Seguridad de la Información serán los encargados de clasificar los activos de información de acuerdo con su grado de sensibilidad y criticidad, de documentar y mantener actualizada la clasificación efectuada, y de definir las funciones que deberán tener permisos de acceso a la información.

7.4.2 Inventario de Activos

Fundiciones De Lima SA contará con un inventario de activos identificados y clasificados, donde defina su nivel de sensibilidad, criticidad y medidas de tratamiento de acuerdo a su clasificación con el objeto de garantizar que reciban el nivel apropiado de protección.

Así mismo, el nivel de acceso de cada Activo, personal autorizado para ello, los perfiles de usuarios, entre otros.

7.5 Política de Uso de Los Activos

Toda la información relacionada con el negocio de Fundelima S.A. que se encuentre almacenada en archivos, planta física o recursos informáticos a su servicio, pertenece a Fundelima S.A. a menos que un documento formal exprese lo contrario.

En razón de lo anterior, se establece lo siguiente:

- Los activos de información pertenecen a Fundelima S.A. y el uso de los mismos debe emplearse exclusivamente con propósitos laborales.
- Los usuarios deberán utilizar únicamente los programas y equipos autorizados por la GERENCIA.
- Todos los requerimientos de aplicativos, sistemas y equipos informáticos deben ser solicitados por el Director del área, y ésta debe ser autorizada por la Gerencia o quien asigne, con el visto bueno del líder de sistemas.
- Toda Información ò recursos informáticos de Fundelima S.A. no podrán ser utilizados, sin previa autorización escrita, para divulgar, propagar o almacenar contenido personal o comercial, programas destructivos (virus), propaganda política, material religioso o cualquier otro uso que no esté autorizado.
- 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, navegación en páginas con contenido sexual, uso permanente de redes sociales personales, navegación en sitios peligrosos, conexión de periféricos o equipos que causen molestia a compañeros de trabajo, etc.
- Todos los usuarios tienen el deber de informar al Jefe Inmediato de cualquier violación de las políticas de seguridad, uso indebido y debilidades de seguridad de la información de Fundelima S.A. que tenga conocimiento, así como al líder de Sistemas, en el caso del uso indebido de los recursos informáticos.
- Los usuarios no deben almacenar videos, fotografías o información personal en los equipos móviles ni en los dispositivos móviles asignados.
- Los usuarios no deben utilizar medios de almacenamiento extraíbles (memorias USB, Discos, CD’s, Disquettes, cintas magnéticas, o similares) personales en la empresa.
- Los usuarios no deben conectar medios extraíbles en los puertos de comunicación de los equipos de cómputo y dispositivos móviles (usb, firewire, entre otros) para copiar información desde y hacia ellos. En caso de requerirse, debe contar con la autorización debida para realizarlo. Listado de usuarios autorizados
- El usuario será responsable de todas las transacciones o acciones efectuadas con su “cuenta de usuario”.
- Ningún usuario deberá acceder a la red o a los aplicativos adquiridos por la empresa, utilizando una cuenta de usuario o clave de otro usuario.
    - Los usuarios no podrán efectuar ninguna de las siguientes labores sin previa autorización del Coordinador de Seguridad de la Información o el Líder de Sistemas:
        - ❖ Instalar software en cualquier equipo de Fundelima S.A.
        - ❖ Bajar o descargar software de Internet u otro servicio en línea en cualquier equipo de Fundelima S.A.
        - ❖ Modificar, revisar, transformar o adaptar cualquier software propiedad de Fundelima S.A.

- ❖ Descompilar o realizar ingeniería inversa en cualquier software de propiedad de Fundelima S.A.
- ❖ Copiar o distribuir cualquier software de propiedad de Fundelima S.A.
- ❖ Cambiar la configuración de hardware de propiedad del Fundelima S.A.
- ❖ Los usuarios no deben realizar cambios en las estaciones de trabajo relacionados a la configuración de los equipos, tales como conexiones de red, usuarios locales del equipo, imágenes de perfil y pantalla y protectores de pantalla corporativos, entre otros.

- Los empleados deberán realizar la devolución de todos los activos físicos y/o electrónicos asignados por Fundelima S.A. en el proceso de desvinculación, de igual manera deberán documentar y entregar al encargado que designe Gestión Humana, los conocimientos importantes que posee de la labor que ejecutan.

7.6 Política de Acceso a la Información.

Todas las personas que laboran para Fundelima S.A. y todos los terceros a quienes Fundelima S.A. suministra información, tendrán acceso sólo a la información necesaria para el desarrollo de sus actividades. No obstante, la facultad de otorgar acceso a la información es responsabilidad del Director del área que genera dicha información

7.7 Política de Procesamiento de la Información

Para cualquier plataforma tecnológica, medios físicos o impresos, en donde se procese información de Fundelima S.A., o información relacionada con los servicios que presta a sus asociados, se deben cumplir las políticas, normas, estándares y procedimientos de seguridad que garanticen los principios de confidencialidad, integridad, auditabilidad y disponibilidad de la información, que Fundelima S.A. ha definido o aceptado.

7.8 Política de Clasificación de la Información.

Es obligación de los Responsables de Procesos clasificar la información dentro de los criterios que Fundelima S.A. establezca en sus normas de seguridad física e informática. La información generada por las áreas, relacionada con los servicios que Fundelima S.A. presta a sus asociados, debe ser clasificada de acuerdo con los criterios que haya establecido en sus normas de seguridad informática.

7.9 Política de Protección de la Información.

Cualquier información clasificada como confidencial, que entre o salga de Fundelima S.A. por medio físico, magnético, transmisión electrónica o hardware, deberá tener los mecanismos de seguridad apropiados que garanticen su integridad, confidencialidad, auditabilidad y disponibilidad.

Para todas las personas que laboran para Fundelima S.A. y para todos los terceros a quienes Fundelima S.A. presta servicios informáticos, está totalmente prohibido el uso de cualquier tipo de herramienta (software o hardware) de diagnóstico de seguridad de redes o que de alguna forma ponga en peligro la seguridad de la red de Fundelima S.A.

Cualquier alianza o convenio de procesamiento de información con terceros no puede vulnerar en forma alguna el contenido de las políticas de seguridad informática definidas, ni las normas emitidas para su implantación. Así mismo, cualquier convenio o alianza para procesar información de terceros en las instalaciones de Fundelima S.A., se regirá por el conjunto de políticas, normas, procedimientos y estándares definidos o aceptados por Fundelima S.A.

7.10 Política de Continuidad de la Información.

Todo medio, sistema de información o plataforma tecnológica en los cuales se procese información de Fundelima S.A., o información relacionada con los servicios que Fundelima S.A. presta a sus asociados, tendrá los planes de contingencias y recursos necesarios que aseguren la continuidad de los procesos del negocio en un tiempo razonable para cada caso y contemplando como mínimo los riesgos más probables de ocurrencia que afecten su continuidad. Esto es responsabilidad del Coordinador de Seguridad de la Información y los terceros asociados.

7.11 Política de Manejo, disposición y mantenimiento de la Información, medios y equipos.

Los medios y equipos donde se almacena, procesan 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.

Está restringido el uso de medios removibles de almacenamiento, por lo cual se deshabilita la funcionalidad de los puertos USB, unidades ópticas de grabación en todos los equipos de cómputo corporativos; la autorización de uso de los medios removibles debe ser tramitada a través del Coordinador de Seguridad de la Información de Fundelima S.A.

Todas las personas que laboren en Fundelima S.A. deben velar por la protección de documentos, medios externos (cintas, discos, y discos duros), datos de entrada y salida y reportes con información clasificada contra daño, robo y acceso no autorizado.

Los contenidos de los medios externos deben borrarse en caso de no ser requerida la información contenida en ellos, antes del proceso de destrucción de los mismos. Cuando ya no son requeridos, los medios informáticos y los reportes impresos con información confidencial deben eliminarse de manera segura evitando filtrarse a personas ajenas a la organización.

Para retirar cualquier medio informático de la organización se requiere autorización de la Gerencia y se debe diligenciar un registro con toda la información relacionada con el retiro.

Los siguientes controles deben considerarse a la hora de destruir físicamente los medios externos:

- Los medios que contienen información sensible deben ser almacenados y/o eliminados de manera segura.
- Los reportes con información confidencial deben ser triturados o incinerados
- El proceso de eliminación de los medios externos y/o reportes con información clasificada deben realizarse con la autorización del Coordinador de Seguridad de la Información ò el Líder de Sistemas, según corresponda, quienes serán los garantes de que el proceso se realizó correctamente.
- De toda eliminación de medios y/o reportes debe quedar como resultado del proceso, un acta firmada por los asistentes al proceso, como: Coordinador de Seguridad de la Información y un empleado de AS Sistemas S.A.S

Los elementos que requieren una eliminación segura son: documentos en papel, voces u otras grabaciones, papel carbónico, informes de salida, cintas de impresora de un solo uso, cintas magnéticas, discos o cassetes removibles, medios de almacenamiento óptico (todos los formatos incluyendo todos los medios de distribución de software del fabricante o proveedor), listados de programas, datos de prueba, documentación de sistemas.

7.12 Política de Control de Acceso

Esta Política define la forma como Fundelima S.A. asegura un acceso controlado, físico o lógico, a todo sistema de información y plataforma tecnológica en los cuales se procese información de Fundelima S.A. y se describen los detalles de seguridad física referentes a los aspectos de seguridad que controlan el acceso de personas, tanto las que laboran para Fundelima S.A. como para terceros, y ya sea que los lugares de procesamiento y los equipos sean propios o de terceros, así como los lugares de archivos físicos.

- ✓ **Control de acceso a redes**

Los Servidores de Fundelima S.A., están ubicados en un(a) gabinete de red que cumple con los requisitos básicos de soporte, seguridad y respaldo.

El Líder de Sistemas (AS Sistemas), definirá controles para garantizar la seguridad de los datos y los servicios conectados a las redes de la organización, contra el acceso no autorizado y evitar la afectación de los equipos a través de redes.

- ✓ **Gestión de acceso de usuario**

El acceso a la información se hace a través de la infraestructura de red instalada en las sedes de la empresa, y para la comunicación remota a través de una vpn configurada en un dispositivo que cuenta con la seguridad adecuada para el acceso por parte de los usuarios.

Los usuarios que ingresan y realizan consultas de la información se encuentran validados dentro del dominio interno, mediante contraseñas que impiden el acceso a personal no autorizado. Por otra parte, en el sistema de información administrativo y contable, se tiene establecidos usuarios y perfiles de acceso de acuerdo con las funciones de cada usuario.

- ✓ **Control para usuarios remotos**

Todas las personas que laboran para Fundelima S.A. y todos los terceros a quienes Fundelima S.A. presta servicios informáticos, que requieran acceso remoto a cualquier equipo, debe contar con la respectiva autorización de Gerencia o la Dirección Administrativa.

El líder de Sistemas solo habilitará este acceso, previa autorización escrita.

Las comunicaciones remotas deberán realizarla siempre los usuarios mediante una identificación y autenticación (código de acceso/usuario y contraseña).

Para garantizar la invulnerabilidad de las comunicaciones remotas, estas deberán encriptarse con alguno de los siguientes estándares:

- Sistema de conexión por VPN
- Sistema de encriptación asimétrico para autenticación
- Sistema que se comunique vía protocolo TCP/IP.

El líder de Sistemas deberá establecer el estándar de comunicación y cualquier comunicación nueva que se establezca deberá ser homologada antes de su implantación y revisada luego de la misma. Para estar homologada deberá cumplir con todos los estándares establecidos.

Es responsabilidad del Líder de Sistemas obtener y ejercer los controles necesarios para que esta norma se cumpla.

Así mismo, se deberá considerar la restricción horaria, en caso de ser necesario, dependiendo de las necesidades del usuario a configurar.

- ✓ **Control de Acceso de Terceros**

Cualquier persona o empresa que no pertenezca a Fundelima S.A. sea proveedor, contratista, cliente, visitante o persona perteneciente a empresas asociadas, que requiera acceso a cualquier, equipo, medio, sistema de información o plataforma tecnológica en los

cuales se procese información de Fundelima S.A. debe tener previa autorización Gerencial o de la Dirección Administrativa según sea el caso, y estar en pleno conocimiento del Líder de Sistemas.

En caso de requerir claves de control de acceso, perfiles de usuarios, entre otros, estas deben ser tramitadas por el Coordinador de Seguridad de La Información ante el Líder de Sistemas.

- ✓ **Administración de Claves de Acceso**

Las claves de acceso están asociadas a la identificación de un usuario y permiten autenticarlo.
Todo usuario que accede a un ambiente tecnológico y/o aplicación debe tener definido una clave de acceso, personal e intransferible.
El uso de claves de acceso deberá ser obligatorio en todos los sistemas (equipos, correos, software, seguridad física, entre otros). Nunca se definirá un usuario o perfil de acceso que no tenga una clave correspondiente.
Deberá hacerse conocer a los usuarios las siguientes recomendaciones sobre la utilización de claves de acceso:

- Que no usen claves basadas en meses, nombres de áreas o departamento, o de un proyecto.
- En lo posible usen códigos aleatorios sin lógica.
- No sean almacenadas bajo ningún concepto en archivos electrónicos de sus estaciones de trabajo.
- No estén legibles en ningún tipo de archivo.
- No estén codificadas en programas.
- No compartir la clave con nadie.
- El usuario que tenga que acceder a un sistema colocando una clave, dada la información crítica o confidencial que maneja el mismo, debe tener en cuenta que la misma debe ser diferente de la que usa habitualmente para conectarse a la red.
- Ante una sospecha de utilización de sus usuarios, la primera medida deberá ser el cambio de clave.
- Diferentes usuarios no pueden usar la misma clave.
- Las claves que le son otorgadas a un usuario (por seguridad Informática, o personal técnico) deben ser inmediatamente cambiadas.
- No evidenciar jamás ni el código de usuario ni la clave ante sistemas que le sean desconocidos, antes debe asesorarse ya que puede ser un sistema de captura de claves.
- No se deberá usar el nombre de la persona responsable del usuario, iniciales o el mismo código del usuario.

Las claves de acceso deben tener las siguientes características:

- Invisibles.
- Longitud mínima de 8 caracteres.
- Obligación de cambio de clave
- No permitir repetición de la clave antes de seis veces.
- Las claves archivadas deberán estar encriptadas.
- Bloqueo del usuario después del tercer intento fallido.
- Claves no obvias.

Las excepciones a una o más de estas características deberán ser justificadas técnicamente por el líder de la aplicación de informática y estos informarán al Gerencia y/o al personal correspondiente.

Todo el personal de Fundelima S.A. debe cumplir estrictamente las recomendaciones que con respecto al tratamiento de claves acá descrito.

7.13 Uso de Servidor o carpetas virtuales compartidas

Los usuarios que tengan acceso a la información compartida ubicada en el servidor, deben estar relacionados en el Listado de Perfiles y Usuarios, de lo contrario para ser incluido en este listado, el director del área, deberá solicitar por escrito la inclusión de este y detallar el acceso y permisos, correspondientes al rol y funciones a desempeñar, al Coordinador de Seguridad de la Información, quien tramitará la actualización con el Líder de Sistemas. Los usuarios tendrán permisos de escritura, lectura o modificación de información en los discos de red, dependiendo de sus funciones y su rol.

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

Está prohibido almacenar archivos con contenido que atente contra la moral y las buenas costumbres de la organización 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 de red.

Se prohíbe extraer, divulgar o publicar información de cualquiera de los discos de red o estaciones de trabajo, sin expresa autorización de su jefe inmediato.

Se prohíbe el uso de la información de los discos de red con fines publicitarios, de imagen negativa, lucrativa o comercial.

7.14 Uso de Puntos de Red de Datos.

Esta Política aplica para todos los usuarios de la información que cumplan con los propósitos generales de Fundelima S.A.

- Los usuarios deberán emplear los puntos de red, para la conexión de equipos informáticos Institucionales.
- Los equipos de uso personal, que no son de propiedad de Fundelima S.A, 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 Coordinador de Seguridad de La Información y el Líder de Sistemas.
- La instalación, activación y gestión de los puntos de red es responsabilidad del Líder de Sistemas.

7.15 Política de Seguridad Física

Esta Política define el control de acceso físico que debe existir en cualquier lugar donde se almacene o realice procesamiento de datos o se almacenen archivos físicos de Fundelima S.A., a su vez define los detalles de seguridad física referentes a los aspectos de seguridad que controlan el acceso de personas, tanto las que laboran para Fundelima S.A. como para terceros, y ya sea que los lugares de procesamiento y los equipos sean propios o de terceros, así como los archivos físicos, con el fin de fortalecer la integridad y disponibilidad la información.

Todas las áreas o espacios físicos donde se almacene o archive información, o de procesamiento principal de información se deben encontrar en recintos cerrados en donde exista acceso físico restringido por medio de algún tipo de cerradura (electrónica o mecánica) que impida el paso de personas no autorizadas a la misma.

Por lo anterior se dispone:

- Fundelima S.A y el Área Administrativa debe implementar un sistema de seguridad física para sus instalaciones, en cooperación con el proveedor encargado de la Seguridad y Vigilancia.
- La gerencia debe garantizar la implementación de barreras y/o sistemas de control de acceso a las instalaciones, o espacios físicos donde se archive o almacene información, así como en los lugares de procesamiento electrónico, y la asignación de niveles de acceso.
- El Líder de Sistemas debe implementar alarmas de detección de intrusos a los centros de datos y servidores.
- La alta dirección implementará y mantendrá en operación sistemas de control de incendio, así como planes integrales a las instalaciones para prevenir inundaciones o humedad en los centros de datos, centros de cableado y de archivo.

- El Área de Sistemas, 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.
- No está permitido el uso de equipo fotográfico, de video, de audio u otro dispositivo de grabación de audio o video al interior de los espacios físicos en las instalaciones de la empresa sin previa autorización de la Gerencia.

7.16 Política de control de acceso físico

Para todas las personas que laboran para Fundelima S.A. y para todos los terceros a quienes Fundelima S.A. presta servicios informáticos, está totalmente restringido el acceso al centro de cómputo sin previa autorización de la Dirección Administrativa. El personal que no posea acceso autorizado al centro de cómputo deberá estar siempre acompañado por el personal de informática de la empresa, el cual controlará las actividades que los visitantes desarrollen.

7.17 Política de Seguridad de los Equipos.

Esta política tiene como fin asegurar la protección de la información en los equipos.

- ✓ **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 Líder de Sistemas.

- ✓ **Protecciones en el Suministro de Energía.**

A la red de energía regulada de los puestos de trabajo solo se pueden conectar equipos electrónicos; los otros elementos deberán conectarse a la red no regulada. Esta labor debe ser revisada por el proceso de Mantenimiento de Equipos e Instalaciones.
El Área de Mantenimiento de Equipos e Instalaciones, debe implementar sistemas redundantes de alimentación eléctrica, como por ejemplo: plantas generadoras de energía que permita soportar la operación de los sistemas de información durante una falta de suministro de un proveedor de energía.

- ✓ **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 Área de Tecnología y Sistemas de Información establecerá un programa de revisiones y/o inspecciones físicas al cableado, con el fin de detectar dispositivos no autorizados.

- ✓ **Uso y Protección de Microcomputadores**

Los computadores propiedad de Fundelima S.A. sólo pueden ser usados para la ejecución de los procesos de negocio de Fundelima S.A. Cualquier otro uso debe ser autorizado formalmente por la Gerencia.

Dentro del desarrollo de las actividades de negocio, los recursos de informáticos deben ser utilizados adecuadamente tanto por sí mismos como en interfaces con sistemas centrales a fin de siempre obtener la modalidad de uso más segura y eficiente.

La conexión del computador con redes de telefonía y redes de datos públicas sólo debe realizarse ante una necesidad de ejecutar un proceso de negocio; esto implica, por ejemplo, no realizar conexiones innecesarias a Internet.

En general toda información que se considere confidencial o altamente confidencial no debe resguardarse en los computadores, y por ende debe evitarse el “bajar” a este ambiente este tipo de información residente en los diferentes aplicativos de Fundelima S.A., a menos que sea de imperiosa necesidad y se tengan los controles de acceso y de encripción necesarios para proteger dicho tipo de información. De ser necesario, una vez terminado el proceso, dicha información debe ser removida del correspondiente soporte magnético (tales como disquete, CD-ROM).

No debe modificarse en forma alguna la estructura de seguridad que se ha instalado por defecto en cada uno de los microcomputadores, sin autorización expresa del Líder de Sistemas de la respectiva plataforma tecnológica.

La siguiente regla no tiene excepciones.

Está terminantemente prohibido instalar cualquier tipo de herramientas de acceso que no fueran las determinadas por la empresa. De poseer cada equipamiento una clave de acceso inicial (setup), será responsabilidad del usuario, sin embargo la clave de acceso inicial del administrador será responsabilidad del Líder de Sistemas.

Los responsables del mantenimiento del inventario de computadores de Fundelima S.A. deben actualizar el mismo ante cualquier cambio de estado.

Cada equipo debe tener un único responsable; en el caso del equipo portátil el usuario es responsable de cumplir toda la normativa precedente cuando realice tránsito con el mismo.

Deberá desarrollarse monitoreo a fin de constatar con una periodicidad adecuada el cumplimiento de esta norma.

- ✓ **Mantenimiento de los Equipos.**

El líder de Sistemas es el responsable de la programación y ejecución del mantenimiento de los equipos críticos, y esta programación debe ser previamente informada al proceso de compras y la Dirección Administrativa.

Las actividades de mantenimiento de los servidores, elementos de comunicaciones, energía o cualquiera que pueda ocasionar una suspensión en el servicio, deben ser previamente programadas.
Los equipos que requieran salir de las instalaciones de Fundelima S.A, a reparación o mantenimiento, deben estar debidamente autorizados por el proceso de Compras y el líder de Sistemas y el contrato de dicho servicio externo deberá contemplar cláusulas de mantenimiento de confidencialidad de la información contenida en los microcomputadores, la no instalación de software no autorizado y el respeto de la normativa referente a software ilegal.

Cuando un dispositivo vaya a ser reasignado o retirado de servicio debe contar con aprobación del Área de Tecnología y Sistemas de Información, así mismo debe garantizarse la eliminación de toda información de acuerdo a las políticas establecidas en este documento en el numeral 6.1.11

- ✓ **Normas de Protección.**

Los Colaboradores que hagan uso de los equipos de Fundiciones De Lima S.A, 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.

Ante cualquier evento que suceda a un colaborador con sus equipos electrónicos a cargo, este debe dirigirse a Gestión Humana para el respectivo descargo.

7.18 Adquisición, Instalación y Mantenimiento de los Sistemas de Información

No se podrá instalar ningún tipo de software en el equipo central o en servidores, cualquiera que sea su clase y característica, sin la autorización del Líder de Sistemas. Este último deberá evaluar el impacto sobre la seguridad.

Es responsabilidad del Líder de Sistemas obtener las correspondientes licencias de cada uno de los aplicativos que se ejecuten en los equipos PC's y servidores de la empresa las mismas y de velar porque se posea un número equivalente de licencias a las instalaciones realizadas de acuerdo con el tipo de contratación que se presente.

En el equipo (hardware) personal que se le provee a cada una de las personas que laboran para Fundelima S.A., no se podrá instalar software de dudosa propiedad, de ningún tipo, sin autorización expresa de Gerencia y conocimiento del Líder de Sistemas. Previo a la autorización, deberá justificarse la necesidad y la licencia de la instalación deberá quedar en custodia de Fundelima S.A. en cabeza del Líder de Sistemas, mientras dicho software permanezca instalado en Fundelima S.A.

Cada persona o empresa que labore para Fundelima S.A. e ingrese equipos (hardware), en forma temporal por períodos cortos o prolongados de tiempo, será responsable de que el software que contenga dicho equipo, esté correctamente licenciado y deberá dejarlo por escrito en el formato correspondiente, en el momento que ingrese el equipo a las instalaciones de Fundelima S.A.

Tampoco se podrán hacer instalaciones de software, aunque éste sea gratuito. Cualquier instalación de software debe ser autorizado por la Directora Administrativa e instalado por el líder de Sistemas

Se encuentra prohibido el uso e instalación de juegos en los computadores de Fundelima S.A.

Todos los términos anteriores se aplican también al hecho de instalar software desde redes públicas (como Internet.) aunque este sea de uso libre, gratuito o demostraciones. Toda instalación por este medio deberá contar como mínimo con:

- Justificación de la necesidad.
- Autorización de la Gerencia.
- Autorización y verificación por parte del Líder de Sistemas que la dirección desde donde se instalará el software es legal.
- Pruebas que el software no se encuentra adulterado, y que sólo cumple el fin explícitamente indicado.
- Registro y reserva por parte del responsable de la dirección y fecha desde en donde se cargó el software.

No existen excepciones a esta norma ya que obrar en contrario expone a Fundelima S.A. y sus directivos a estar cometiendo un delito.

Deberán efectuarse monitoreos con el fin de constatar con una periodicidad adecuada que no se ha instalado software ilegal. Cualquier incidencia detectada deberá ser tratada como un “Evento crítico” ya que se considerará como un hecho doloso y se le dará curso ante el Gerencia y Sistemas.

7.19 Política de Respaldo y Restauración de la Información

El líder de Sistemas es el responsable de establecer y desarrollar las pautas para dar cumplimiento a esta Norma.

Se deben desarrollar procedimientos de resguardo diario de los archivos de información (incluyendo datos de usuarios y perfiles de los aplicativos administrativos, operativos y contables de la empresa y de la información almacenada en los servidores de la empresa. Así mismo, como mínimo de forma semanal, se debe resguardar la información usuarios almacenada en los equipos de usuarios. Previamente se deben definir las rutas o carpetas con información que se resguardarán para los equipos de los usuarios.

Se debe desarrollar resguardos como mínimo dos veces a la semana de la información de los aplicativos administrativos, operativos y contables de la empresa en un medio externo que deberá ser guardado en una caja fuerte para su protección.

Se deben desarrollar procedimientos de copia de la información de los usuarios y del servidor en la nube, a fin de que haya disponibilidad de la información para su uso.

Deberán existir dos copias de cada uno de los productos cubiertos por esta norma, que serán resguardadas en un sitio externo a las instalaciones de Fundelima S.A. con las medidas de seguridad física establecidas.

Deberá contemplar el registro de toda salida de un resguardo de elementos de seguridad y sólo podrá ser realizado por personas autorizadas a tal fin.

7.20 Política de Control de Software

Todo cambio a una aplicación informática debe ser solicitado por el Director del área solicitante y se realizará de tal forma que no vaya en contra del manual de seguridad de la Información existente. Todo cambio que afecte la plataforma tecnológica es aprobado formalmente por la Gerencia. Dicho cambio se realizará de tal forma que no disminuya la seguridad existente. Cualquier cambio de situación laboral o contractual de una persona (natural o jurídica) que acceda a los sistemas de información de Fundelima S.A. o bajo la responsabilidad de Fundelima S.A., se verá reflejado en su nivel de autorización para cada sistema de información. Bajo ninguna circunstancia un cambio puede ser aprobado, realizado e implantado por la misma persona.

Todo sistema de información relacionado con el negocio de Fundelima S.A., o con los servicios que Fundelima S.A. presta a sus asociados, será incorporado de acuerdo con los procedimientos definidos en este manual y existirá un contrato formal de propiedad o licencia de uso de los mismos.

7.21 Política de Prevención y Detección de Virus

Esta norma abarca todos los sistemas operativos y aplicaciones susceptibles de ser atacados por virus informáticos.

Se considerará una violación de seguridad informática el desarrollo, generación, compilación, copia, propagación, ejecución, o la introducción intencional o por irresponsabilidad dentro de la Red de Fundelima S.A., o a través de la comunicación con Fundelima S.A. a proveedores, clientes o cualquier tercero, de cualquier programa que se considere del tipo virus informático (se auto replique, consuma o perjudique de alguna forma el rendimiento del computador, dañe la memoria, archivos o software).

Prevención:

En todas las plataformas informáticas que contengan sistemas operativos o aplicaciones susceptibles de ser atacados por virus, deberá tenerse instalado un software antivirus que detecte la presencia de este tipo de ataque.

Es responsabilidad de Gerencia adquirir (el) los softwares antivirus más reconocidos, y del líder de Sistemas, instalarlos en cada una de las plataformas mencionadas en el párrafo anterior y mantener una versión actualizada de los mismos.

Detección:
Ante la detección de un virus informático el usuario final de Fundelima S.A. deberá:

- Informar inmediatamente al Líder de Sistemas.
- Apagar el equipo.
- Detectar el tipo de virus.
- Ejecutar la vacuna que posea el software antivirus.
- Volver a correr el antivirus.
- En caso de persistencia, apagar el equipo.

Ante la detección de un virus informático el Líder de Sistemas de Fundelima S.A. deberá:

- En caso de persistencia del virus aislar inmediatamente el ambiente infectado.
- Efectuar bajo su responsabilidad las tareas de remoción oportunas (tales como reinstalación del software base, remoción de disco duro).
- Verificar el alcance de la contaminación.
- Investigar las causas posibles de infección.
- Informar a Gerencia de la investigación realizada.
- Profundizar la investigación acerca de las causas de la infección en caso de que lo considere oportuno.
- Realizar las modificaciones al Manual de seguridad en el caso que la infección provenga de una debilidad del mismo.
- Informar a Gerencia acerca de la incidencia y el resultado final de las acciones tomadas.

No existen excepciones a esta norma.

Esta norma se hará conocer y se le recordará a todo el personal, con la periodicidad y por los medios que se considere apropiado.

El líder de Sistemas deberá desarrollar monitoreo a fin de constatar con una periodicidad adecuada el cumplimiento de esta norma.

7.22 Política de Seguridad de las Comunicaciones

Las comunicaciones electrónicas de Fundelima S.A., así como las de terceros que hagan uso de las herramientas de comunicación electrónica de Fundelima S.A., se establecerán de acuerdo con las normas definidas en este manual de seguridad informática de Fundelima S.A. y con los mecanismos que aseguren tanto la identidad de quienes realizan la conexión, como la confidencialidad, integridad, auditabilidad y disponibilidad de la misma.

Esta norma contempla todos los elementos, ya sean dispositivos de hardware o software que permitan o faciliten de forma alguna que ese ambiente informático pueda comunicarse con el exterior o el interior de Fundelima S.A., variando el diseño topológico de la red en forma alguna.

La instalación de cualquier elemento que permita o facilite la conexión de un ambiente, afecta la seguridad e implica posibles intentos de penetración en la misma. También quedan comprendidos en este caso todos los elementos redundantes que ya no se utilicen para la conexión a la Red por haberse modificado el diseño topológico de la misma.

El Coordinador de Seguridad de la Información y el líder de Sistemas deben implementar medidas para asegurar la disponibilidad de los recursos y servicios de red de Fundelima S.A.

El Líder de Sistemas debe crear los estándares técnicos de configuración de la Red de Fundelima S.A y configuración de seguridad y de dispositivos de seguridad.

El Área de Tecnología y Sistemas de Información debe identificar y documentar los servicios, protocolos y puertos autorizados en las redes de datos e inhabilitar o eliminar los servicios, protocolos y puertos no utilizados.

Ninguna persona ajena al Líder de Sistemas podrá instalar o desinstalar elementos de conexión (hardware o software). Cualquier excepción a esto deberá estar justificada técnicamente, ya sea por necesidades propias del funcionamiento de los aplicativos, o por necesidades propias de la plataforma informática y deberá comunicarse a Gerencia o a la Dirección Administrativa.

El personal de AS-Sistemas comunicara a Gerencia cualquier variación del diseño topológico de la red. La instalación de cualquier elemento de comunicación que no respete el diseño establecido ya se considera una variación a dicho diseño.

No se considera variación el reemplazo o actualización de ambientes o elementos de conexión a menos que estos últimos posean diferentes características de seguridad. Tampoco se considera variación la incorporación de nuevos ambientes siempre que no se varíe la esencia del diseño de la Red.

7.23 Política de Escritorio y Pantalla Limpia

El personal del Fundelima S.A. debe conservar su escritorio libre de información, propia de la empresa, que pueda ser alcanzada, copiada o utilizada por terceros o por personal que no tenga autorización para su uso o conocimiento.

El personal de Fundelima S.A. debe bloquear la pantalla de su computador con el protector de pantalla, con la clave de acceso al equipo o apagarla, en los momentos que no lo esté utilizando o cuando por cualquier motivo deba dejar su puesto de trabajo.

Los usuarios de los sistemas de información y comunicaciones de Fundelima S.A. deberán cerrar las aplicaciones y servicios de red cuando ya no los necesite.

Los usuarios a los que Fundelima S.A. les asigne equipos móviles como computadores, teléfonos inteligentes, tabletas, deben activar el bloqueo de teclas o pantalla, que permita evitar el acceso no autorizado a estos dispositivos.

Al imprimir documentos con información pública reservada y/o pública clasificada (semiprivada o privada), deben ser retirados de la impresora inmediatamente y no se deben dejar en el escritorio sin custodia.

No se debe utilizar equipos de cómputo, fotocopiadoras, escáneres, equipos de fax, cámaras digitales y en general equipos tecnológicos que se encuentren no tengan un usuario asignado. El director del área es el responsable de asignar un responsable de cualquier equipo que quede libre.

7.24 Uso de Impresoras y del Servicio de Impresión

Esta Política aplica para todos los usuarios de la información que cumplan con los propósitos generales de Fundelima S.A.

- Los documentos que se impriman en las impresoras de Fundelima S.A. deben ser de carácter institucional.
- Todo colaborador en el momento de realizar impresiones de documentos con clasificación pública reservada o información pública clasificada (privada o semiprivada), debe mantener control de la impresora, por lo cual no la deberán dejar desatendida, preservando la confidencialidad de la información.
- Los documentos que contengan información confidencial, privada o sensible no pueden ser usados como papel reciclable, estos deben ser destruidos cuando ya no sean funcionales.

7.25 Política de Uso de Internet

Fundelima S.A. tiene contratados los servicios de canales de internet en sus sedes para la navegación y acceso a páginas y aplicativos Web, con el objetivo que sea un instrumento para la realización de las actividades laborales.

El acceso a Internet a través de los equipos de Fundelima S.A. es un privilegio, no un derecho, y el uso inapropiado, incluyendo la infracción de estas reglas puede tener como resultado, la aplicación de las sanciones disciplinarias previstas en el reglamento interno de la empresa.

Las prioridades de la empresa son:

- Acceder de forma remota y segura (vpn) al software contable que se encuentra instalado en uno de los servidores de la empresa.
- Posibilitar a los empleados el acceso a Internet minimizando el tiempo de respuesta.
- Utilizar el ancho de banda de forma óptima evitando la saturación por cargas indiscriminadas.

Con el propósito de hacer un buen uso del canal se establecen las siguientes responsabilidades para los usuarios:

- El servicio de navegación debe ser utilizado solamente para el desempeño de sus funciones en el trabajo e investigación relacionada durante la jornada laboral.
- Utilizar su dirección de correo electrónica corporativa sólo para la inscripción y/o solicitud de información vía Internet relacionada con la actividad laboral, de manera que no comprometa la imagen de la empresa.
- La navegación de Internet debe hacerse siempre por los canales que tiene contratados la empresa.
- Si tiene problemas para acceder a alguna página, necesaria dentro de sus actividades laborales, debe comunicarse con el área de sistemas para hacer las investigaciones y correctivos necesarios.

Y las siguientes restricciones:

- Se encuentra totalmente prohibido el acceso páginas relacionadas con pornografía, contenido obsceno, drogas, alcohol, webproxys, hacking y/o cualquier otra página que vaya en contra de la ética moral, las leyes vigentes o políticas establecidas en este documento; esta prohibición no es solamente para el acceso a través de la Web sino también a través de todos los demás servicios de Internet (e-mail, ftp, grupos de discusión, listas de distribución, etc.).
  No descargar ni instalar programas de cualquier tipo obtenidos en Internet o traídos en medios removibles (cintas, discos duros removibles, CDs, DVDs y unidades de almacenamiento USB, entre otras) en los equipos de cómputo y dispositivos móviles asignados para el desempeño de sus labores. Los usuarios deben asegurarse que los archivos descargados de internet o copiados de cualquier medio de almacenamiento, provienen de fuentes conocidas y seguras para evitar el contagio de virus informáticos y/o instalación de software malicioso en los recursos tecnológicos.

- En caso de necesitarse, el usuario debe justificar la necesidad al personal de sistemas para la revisión del licenciamiento, luego solicitar la autorización correspondiente para su compra, si es el caso, y posteriormente solicitar la descarga y/o instalación por parte del personal de sistemas.

- Los usuarios del servicio de internet tienen prohibido el acceso y el uso de servicios interactivos o aplicaciones de mensajería instantánea como, que tengan como objetivo crear comunidades para intercambiar información, o bien para fines diferentes a las actividades propias de Fundelima S.A.

- No está permitido la descarga, uso, intercambio y/o instalación de juegos, música, películas, protectores y fondos de pantalla, software de libre distribución, información y/o productos que de alguna forma atenten contra la propiedad intelectual de sus autores, o que contengan archivos ejecutables y/o herramientas que atenten contra la integridad, disponibilidad y/o confidencialidad de la infraestructura tecnológica (hacking), entre otros. La descarga, uso, intercambio y/o instalación de información audiovisual (videos e imágenes) utilizando sitios públicos en Internet debe ser previamente autorizada por la gerencia, o por quienes ellos deleguen de forma explícita para esta función, asociando los procedimientos y controles necesarios para el monitoreo y aseguramiento del buen uso del recurso.

7.26 Política Para Uso de Dispositivos Móviles

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

Los dispositivos móviles asignados por Fundelima S.A deben tener la configuración sugerida por el Líder de Sistemas, así mismo podrán configurarse únicamente las cuentas de correo electrónico asignadas al usuario por la empresa.

En el caso del personal que tiene autorizado el uso de Mensajería instantánea en los dispositivos de las líneas corporativas, no se permite por esta aplicación, el envío de fotografías, audios y videos clasificados como información pública reservada o información pública clasificada (privada o semiprivada). Adicionalmente deben usarse como fotos de perfil o de estado y cualquier otra aplicación futura, fotos institucionales, que en ningún caso atenten contra las políticas de Protección de Datos Personales. Así mismo no está permitido tener las líneas corporativas incluidas en grupos de mensajería instantánea personales tales como Whastapp, Messenger, Instagram, Facebook, entre otros.

Los sistemas de mensajería instantánea para dispositivos móviles institucionales a implementar en Fundelima S.A., debe incluir métodos de cifrado de extremo a extremo de la comunicación, por lo tanto, el Líder de Sistemas debe verificar que esto se cumpla.

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

Ante la pérdida del equipo, ya sea por extravío o hurto, deberá informar de manera inmediata al Jefe de Gestión Humana y a la Dirección Administrativa, y continuar con el procedimiento administrativo al que haya lugar.

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.

Es responsabilidad del usuario hacer buen uso del dispositivo suministrado por Fundelima S.A. con el fin de realizar actividades propias de su cargo o funciones asignadas en la empresa.

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.

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

Los usuarios de dispositivos móviles institucionales no deben conectarlos en computadores de uso público (Restaurantes, café internet, aeropuertos, etc.).

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

En caso de requerir instalación de aplicaciones adicionales en el dispositivo móvil institucional se debe solicitar a la Dirección Administrativa para su aprobación.

Los usuarios de dispositivos móviles institucionales deben usar solo fotos y/o videos institucionales autorizadas para fondos de pantalla, de bloqueo, y perfil y estado de mensajería instantánea, y similares.

7.27 Política de uso del Correo Electrónico

Para todas las personas que laboran para Fundelima S.A. y para todos los terceros a quienes Fundelima S.A. presta servicios informáticos, se establece que toda información contenida en los buzones de correo que Fundelima S.A. asigna, pertenece a la empresa y puede utilizarse para los propósitos comerciales, legales, financieros o de cualquier otra índole que la empresa estime conveniente.

La creación de una cuenta de usuario de correo implica la aceptación sin restricciones de ningún tipo y entiende leídas y comprometidas las políticas y prohibiciones en el uso del correo electrónico y se compromete el usuario a cumplirlas y hacerlas cumplir. La cuenta de correo electrónico asignada es de carácter individual; por consiguiente, ningún usuario y/o trabajador de Fundelima S.A., bajo ninguna circunstancia debe utilizar una cuenta de correo que no sea la suya, salvo autorización expresa del Director del área.

Está expresamente prohibido: Difusión de material o información confidencial de la empresa, las violaciones de Derechos de Propiedad intelectuales, difusión masiva de e-mails no

solicitados por los destinatarios (spamming), la falsedad de información de la transmisión, los virus y otras actividades destructivas, la invasión de sitios Web (hacking), el envío de cadenas de mensajes de cualquier tipo, ya sea comercial, político, religioso, material audiovisual, contenido discriminatorio, pornografía, pederastia, material obsceno, difamatorio, abusivo o amenazante y demás condiciones que degraden la condición humana y resulten ofensivas. En resumen, los usuarios son completamente responsables de todas las actividades realizadas con sus claves y buzón de correo proporcionado por la empresa y asumirá las consecuencias legales en el evento de que sea usado el correo de forma inapropiada.

Prohibiciones para archivos adjuntos:

- No es permitido el envío de archivos que contengan extensiones ejecutables.
- No es permitido el envío de documentos adjuntos a correos electrónicos que contenga información sensible de la empresa, como son planos de piezas en el formato original de diseño (programa cad utilizado por la empresa); cualquier requerimiento al respecto debe ser autorizado previamente por la gerencia. Los archivos deben enviarse en formato de documento portátil, pdf, excepto aquellos que deban enviarse en otro formato debido a que requieran modificación por parte del destinatario.

Los correos electrónicos son objeto de trazabilidad y auditoría de forma aleatoria, por lo cual se debe guardar la autorización solicitada en caso de requerirse este soporte.

Los usuarios deben tener cuidado al momento de extraer archivos adjuntos de los correos electrónicos, analizando por el mensaje, su procedencia y el contenido si es veraz la información y si provienen de fuentes conocidas y seguras para evitar el contagio de virus informáticos y/o instalación de software malicioso o no apropiado para el buen uso de los sistemas informáticos de la empresa.

Los sistemas antivirus, de protección de contenido y antispam instalados verificarán automáticamente los mensajes de correo, eliminando posibles virus y filtrará lo que se haya clasificado como no apropiado por contenido, tamaño y otros criterios que establezca la empresa.

Cada usuario de correo tiene asignado una cuota de espacio en el servidor que se considera suficiente para el volumen y tipo de información que el maneja. Cualquier solicitud de ampliación de ese espacio deberá gestionarse con la Dirección Administrativa. Para no superar este espacio y mantener un adecuado nivel de carga y recursos de los servidores de correo, los usuarios son responsables de archivar los mensajes de cierta antigüedad, mientras el líder de Sistemas es responsable de compactar la base de datos.

La violación de la seguridad de los sistemas y/o red de Fundelima S.A., de sus empresas asociadas o de otra empresa o institución, por parte de algún usuario inscrito en el correo electrónico del dominio de Fundelima S.A. será responsabilidad única y exclusivamente del

usuario quien responderá a nombre propio por sus actos ante las autoridades que así lo requieran.

Todos los mensajes enviados deben respetar el estándar de formato e imagen corporativa definidos por la empresa y se establece como obligatorio el uso de una cláusula de confidencialidad en los mensajes electrónicos que se envíen a terceros con el siguiente enunciado:

AVISO LEGAL: Este mensaje y sus anexos pueden contener información confidencial o legalmente protegida y no puede ser utilizada ni divulgada por personas diferentes a su destinatario. Si por error, recibe este mensaje, por favor avise inmediatamente a su remitente y destruya toda copia que tenga del mismo. Cualquier uso, divulgación, copia, distribución, impresión o acto derivado del conocimiento total o parcial de este mensaje sin autorización de FUNDELIMA será sancionado de acuerdo con las normas legales vigentes. De otra parte, al destinatario se le considera custodio de la información contenida y debe velar por su confidencialidad, integridad y privacidad.

Las cuentas de correo podrán ser configuradas en los dispositivos móviles asignados; para ambos casos, esta configuración debe ser autorizada por el Director Administrativo de la empresa o superiores a éste y debe ser realizado por personal de sistemas. Todas las normas y políticas concernientes al uso del correo electrónico descritas en este manual, se aplican al uso del correo electrónico en los dispositivos móviles. Todo usuario de correo electrónico corporativo debe garantizar la disponibilidad de los correos y toda la información que se responda desde el dispositivo móvil, enviando copia al propio correo para que quede en la bandeja de entrada del correo del pc.

7.28 Políticas específicas para Webmaster

El objetivo de esta política es proteger la integridad de la(s) página(s) Web institucionales, el software y la información contenida.

Estas políticas aplican a los empleados y contratistas actuales y por ingresar y a terceros que se encuentren desempeñando el rol de Webmaster, los cuales serán responsables de todo el contenido de las páginas Web (webmaster), de preparar y depurar la información que será publicada en ésta, las cuáles deben estar acordes con políticas de seguridad de la información de Fundiciones De Lima, consignadas en su mayoría en este documento.

7.29 Políticas de Uso de Mensajería instantánea y redes sociales

El uso de servicios de mensajería instantánea y el acceso a redes sociales corporativos, estarán autorizados para aquellos empleados que las requieran para el desempeño de sus roles o funciones y/o para facilitar los canales de comunicación con las partes interesadas establecidas por Fundiciones De Lima S.A (Ver Planeación estratégica LGR-01).

No se permite el envío de mensajes con contenido que atente contra la integridad de las personas o partes interesadas de la organización o cualquier contenido que represente riesgo de código malicioso.

La información que se publique o divulgue por cualquier medio de internet, de cualquier empleado, contratista u otro colaborador de Fundelima SA, que sea creado a nombre personal, como redes sociales, twitter®, facebook®, youtube®, likedink® o blogs, se considera fuera del alcance.

7.30 Política de Archivos Físicos de Documentos

La Gerencia y Dirección Administrativa son los responsables de la recolección, almacenamiento, organización, identificación, disponibilidad y custodia de los archivos físicos, y deben garantizar, su preservación a largo plazo, y su correcta disposición final cuando sea necesario.

Para ello determinará los espacios físicos para su almacenamiento y las acciones necesarias para su preservación y administración, así como las normas de acceso a estos, según la criticidad de la información que contengan.

Todos los Directores y Jefes de área son responsables de entregar periódicamente a la Dirección Administrativa los documentos físicos que deben reposar en el Archivo Físico de la empresa.

Adicionalmente, todos los documentos que hacen parte del SIG se gestionarán, de acuerdo a los procedimientos e instructivos, que determinan la metodología para la creación, uso, retención, acceso y preservación de la información, independiente de su soporte y medio de creación.

7.31 Política de Transferencia de la Información

Fundiciones De Lima, asegurará la protección de la información en el momento de ser transferida o intercambiada con otras entidades y establecerá Acuerdos de Confidencialidad o de Intercambio de Información con las terceras partes con quienes se realice dicho intercambio. La institución velará por el uso de tecnologías informáticas y de telecomunicaciones para llevar a cabo el intercambio de información; sin embargo, establecerá directrices para el intercambio de información en medio físico.

La Gerencia, con acompañamiento de asesoría Jurídica, debe definir los modelos de Acuerdos de Confidencialidad y de intercambio de información entre la empresa y terceras partes incluyendo los compromisos adquiridos y las penalidades civiles o penales por el incumplimiento de dichos acuerdos.

Entre los aspectos a considerar se debe incluir:

- ✓ La prohibición de divulgar la información entregada por parte de la Fundelima a los terceros con quienes se establecen estos acuerdos.
- ✓ La destrucción de dicha información una vez cumpla su cometido.
- ✓ La oficina Jurídica debe establecer en los contratos que se constituyan con terceras partes, los Acuerdos de Confidencialidad o Acuerdos de intercambio dejando explícitas las responsabilidades y obligaciones legales asignadas a dichos terceros por la divulgación no autorizada de información de la institución que les ha sido entregada.
- ✓ Todo empleado o usuario de Información de Fundelima deben utilizar únicamente los mecanismos y herramientas proporcionadas por FUNDELIMA SA con revisión del Líder de Sistemas para los casos que apliquen, en todo lo relacionado al envío o recepción de información confidencial para la empresa
- ✓ Ningún empleado o usuario de información de Fundelima debe revelar o intercambiar información confidencial de la la empresa por ningún medio, sin contar con la debida autorización.

7.32 Política de Cumplimiento de Requisitos Legales.

Fundiciones De Lima SA respeta y acata las normas legales existentes relacionadas con seguridad de la información, para lo cual realizará una continua revisión, identificación, documentación y cumplimiento de la legislación y requisitos contractuales aplicables para la entidad, relacionada con la seguridad de la información.
Fundelima debe velar por la protección de derechos de autor y propiedad intelectual, razón por la cual propenderá porque el software instalado en los recursos de la plataforma tecnológica cumpla con los requerimientos legales y de licenciamiento aplicables.

El Área de Sistemas deberá garantizar que todo el software que se ejecute los activos de información de Fundelima SA esté protegido por derechos de autor y requiera licencia de uso o, sea software de libre distribución y uso.

Los usuarios y/o empleados de Fundelima deben cumplir con las leyes de derechos de autor y acuerdos de licenciamiento de software, se recuerda que es ilegal duplicar software, duplicar documentación sin la autorización del propietario bajo los principios de derechos de autor y, la reproducción no autorizada es una violación a la ley.

7.33 Política de Retención y archivo de datos.

La alta dirección, directores de área, responsables de proceso y el personal de sistemas, son responsables de velar por mantener la integridad y disponibilidad de la información y de los servicios de procesamiento de información.

Los lineamientos de retención y archivo de la información se encuentran consignados en Listado Maestro de Documentos FGI-01, Control de Registros FGI-02, o de acuerdo a disposiciones de ley, contractuales, tributarias, jurídicas o de otra índole.

7.34 Política de Gestión de Vulnerabilidades

El personal de Sistemas, realizará pruebas técnicas de vulnerabilidad a intervalos planificados en los sistemas de información y comunicaciones de Fundelima.

Así mismo, implementará un programa de gestión de vulnerabilidades técnicas que incluya el plan de tratamiento de las mismas, el cual deberá ser aprobado por el Comité de Seguridad de la Información.

7.35 Políticas para el Personal y Contratistas del Área de Sistemas.

Todo empleado o contratista del área de Sistemas, debe cumplir con todas las políticas y normas establecidas en el presente manual.

7.36 Política Para Proveedores, Tercerización u Outsoursing.

El Comité de Seguridad de la Información y el Líder de Sistemas, deben velar por 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.

En los casos a los que haya lugar, se deben 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 Fundelima SA, las cuales deben se divulgadas por los funcionarios responsables de la realización y/o firma de contratos o convenios.

Todo proveedor y/o contratista que firme contrato, y que en el desempeño del objeto de este tenga acceso a cualquier tipo de información de Fundiciones De Lima, deberá diligenciar y firmar el formato de ACUERDO DE CONFIDENCIALIDAD PARA PROVEEDORES Y CONTRATISTAS FGR-04.

Los contratistas, oferentes y/o proveedores deben aceptar y firmar el acuerdo de confidencialidad establecido por Fundiciones De Lima.

El Área Sistemas deberá mitigar los riesgos de seguridad con referencia al acceso de los proveedores y/o contratistas a los sistemas de información de Fundelima SA

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.

Los funcionarios de Fundiciones de Lima SA que se desempeñan como Administradores de Contratos (según lo consignado en el Procedimiento de Compras PCA-01), deberán realizar seguimiento, control y revisión de los servicios suministrados por los proveedores y/o contratistas en lo relacionado al cumplimiento de las Políticas de Seguridad de la Información.

7.37 Política de Gestión de los Incidentes de la Seguridad de la Información.

El personal de Sistemas, debe presentar notificar inmediatamente la información a la Dirección Administrativa y Gerencia general todos incidentes relacionado con la seguridad que se presenten en todo el sistema informático de la compañía. De igual manera, gestionará el tratamiento pertinente a los incidentes de seguridad de la información que se presenten, investigando y solucionando los incidentes detectados y/o reportados, tomando las medidas necesarias para evitar su reincidencia y escalando los incidentes de acuerdo con su criticidad.

La Gerencia general, será la única autorizada aprobar el reporte de incidentes de seguridad ante las autoridades; así mismo, de autorizar pronunciamientos oficiales ante entidades externas.

Los directores o jefes de área como propietarios de los activos de información deben reportar a la Dirección Administrativa los incidentes de seguridad que identifiquen o que reconozcan su posibilidad de materialización

En los casos a los que haya lugar se sigue lo consignado en el Procedimiento de Acciones Correctivas, Preventivas y de Mejoras PGI-03

7.38 Política de Registro y seguimiento de eventos de sistemas e información y comunicaciones

La Dirección Administrativa es responsable de diligenciar el Registro de incidentes de seguridad de la información FGR-05. Así mismo es la responsable de la solicitud a quien corresponda, de la ejecución de las acciones para el tratamiento de dicho incidente y las acciones para mitigar futuros incidentes.

7.39 POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES

Fundiciones de Lima ha dispuesto su Política de Tratamiento de Datos Personales POGR-02.

En Fundiciones de Lima SA toda captura, recolección, uso y almacenamiento de datos personales que realice Fundiciones De Lima SA en el desarrollo de sus actividades, y de aquellas finalidades dispuestas en la Política de Tratamiento de

Datos Personales POGR-02, requiere de los titulares un consentimiento libre, previo, expreso, inequívoco e informado.

Para tal efecto, Fundiciones de Lima SA ha puesto a disposición de los titulares la autorización para el tratamiento de sus datos personales en los diversos escenarios en los cuales realiza la captura del dato, tanto de manera física como digital, a través de coberturas en modelos de autorizaciones o avisos de privacidad en donde se informa al titular sobre la captura de sus datos personales, el tratamiento al cual serán sometidos incluyendo las finalidades, sus derechos, los canales de ejercicio de sus derechos y la información relacionada sobre la Política Tratamiento de Datos Personales

Es importante tener en consideración que en todos los casos Fundiciones de Lima SA debe custodiar las autorizaciones obtenidas para el tratamiento de los datos personales, dado que ésta hace parte de las pruebas exigidas por la Superintendencia de Industria y Comercio. Así las cosas, se deberán guardar los formatos físicos en donde existan autorizaciones, el registro de llamadas o de los formularios web en los cuales se da trazabilidad sobre la aceptación del tratamiento. La retención documental de las autorizaciones estará alineada con las Tablas de Retención Documental de la empresa de acuerdo con el tipo de documento que las contiene o a las cuales están asociadas.

De acuerdo con las disposiciones normativas, los avisos de privacidad y/o autorizaciones de tratamiento de datos personales mediante los cuales se obtiene la autorización de los titulares deben tener los siguientes elementos:

a. Nombre o razón social y datos de contacto del responsable del tratamiento

b. El Tratamiento al cual serán sometidos los datos y la finalidad de este.

c. Los derechos que le asisten al titular.

d. Los mecanismos dispuestos por el responsable para que el titular conozca la política de Tratamiento de la información.

e. En todos los casos, debe informar al Titular cómo acceder o consultar la política de Tratamiento de información.

7.39.1. Autorización en Formatos.

Los modelos de autorización de tratamiento de datos personales deben ser tramitados a través del formato Autorización para el Tratamiento de los Datos Personales FGR-02

7.39.1.1 Autorización en formatos físicos.

Las áreas que lleven a cabo iniciativas que impliquen la recolección de datos personales deberán tener en cuenta los siguientes aspectos:

a. Fundiciones de Lima Sa debe obtener la respectiva autorización para el Tratamiento de los datos personales debidamente firmado por el titular, antes de ingresar la información a cualquiera de sus bases de datos sea física o magnética. En el caso de la base de dato del software contable, debe remitirse al área de contabilidad la respectiva Autorización para el Tratamiento de los Datos Personales firmada por el titular, antes de crear la base de datos en el sistema. El área de contabilidad es responsable de abstenerse a la creación de la base de datos sino recibe la respectiva autorización.
b. Cada jefe de área es responsable del cumplimiento de la Política de Tratamiento de Datos Personales POGR-02 en su área.
c. Debe remitir a la Dirección Administrativa las bases de datos que contengan datos personales y su cantidad.
d. Puede recibir auditorías por parte de la Dir. Administrativa para verificar las bases de datos, autorizaciones y tratamientos.
e. En las autorizaciones de tratamiento de datos personales sólo debe solicitar aquellos datos personales necesarios conforme con la finalidad de la captura.
f. Para que Fundiciones de Lima SA pueda realizar el tratamiento de los datos capturados en el formulario, el titular debe dar la autorización. En el evento en que el titular no haya autorizado, deberá ser analizado de manera independiente.
g. Validar que en la Política de Tratamiento de Datos Personales POGR-02, se encuentren todas las finalidades de tratamiento asociadas a la captura de los datos solicitados.

7.39.1.2 Custodia de la autorización.

Cada área de Fundiciones De Lima SA que realice un tratamiento activo de datos personales debe garantizar la custodia y almacenamiento de la autorización para el tratamiento de los datos. Así mismo, se deberán poner a disposición de la

Superintendencia de Industria y Comercio o de la Dirección Administrativa en el evento en que éstos lo requieran.

7.39.1.3. Políticas de Información Biométrica.

La información biométrica solo puede ser utilizada para control de acceso, en ningún caso para otro fin.

El personal de gestión Humana es el único con acceso a esta información, por lo tanto, son los directamente responsables del buen uso de la misma.

7.39.1.4. Política de Sistema Cerrado de Televisión.

Fundelima cuenta con Sistema Cerrado de Televisión con fines de seguridad física de las instalaciones y seguimiento a los procesos cuando sea necesario.

Toda persona que labora en Fundelima, autoriza el Uso de esta Tecnología para Implementación de Acciones de Control y Vigilancia.

Así mismo, para el caso de terceros que visiten las instalaciones de la planta, Fundelima debe mantener avisos en las zonas de acceso que informen la existencia de videovigilancia, así como dónde pueden encontrar disponible nuestra Política de Protección de Datos Personales POGR-02, y el canal de acceso para cualquier inquietud, queja o reclamo.

7.39.1.5. Verificación del cumplimiento de las disposiciones sobre datos personales.

La Dirección Administrativa podrá, en cualquier momento, adelantar auditorías de supervisión de cumplimiento de las disposiciones sobre protección de datos personales, con el propósito de garantizar el adecuado cumplimiento de la Política de Tratamiento de Datos Personales POGR-02.

Como resultado de las revisiones pueden levantarse planes de acción para cerrar las brechas encontradas, los cuales tendrán seguimiento en los Comités de Seguridad de la Información.

8. PROCEDIMIENTOS QUE APOYAN LA POLÍTICA DE SEGURIDAD

Los siguientes procedimientos del SIG, apoyan la política de seguridad de la información y se llevan a cabo cuando sea pertinente:

- Procedimiento de Información Documentada PGI-01
- Procedimiento de Acciones Correctivas, Preventivas y de Mejoras. PGI-03

9. SANCIONES PARA LAS VIOLACIONES A LAS POLITICAS DE SEGURIDAD DE LA INFORMACION

Las Políticas de Seguridad de la Información establecidas en este manual, tienen como fin crear y afianzar la cultura de seguridad de la información entre los socios, empleados, clientes, proveedores y demás partes interesadas de la Organización. Por tal razón, es necesario que las violaciones a las Políticas Seguridad de la Información y en general a las Políticas de Seguridad, sean clasificadas, con el objetivo de aplicar medidas correctivas conforme con los niveles de clasificación definidos y mitigar posibles afectaciones contra la seguridad de la información y seguridad en general. Las medidas correctivas pueden considerar desde acciones administrativas, hasta acciones de orden disciplinario o penal, de acuerdo con las circunstancias, si así lo ameritan.

En el Reglamento Interno de Trabajo, están establecidos los procesos disciplinarios a seguir para los empleados que hayan cometido alguna violación de la Política de Seguridad de la Información.

Las investigaciones disciplinarias corresponden a actividades pertenecientes al proceso de Gestión Humana.

Se consideran Violaciones a las Políticas de Seguridad de la Información y en general a las políticas de Seguridad las siguientes:

- No firmar los acuerdos de confidencialidad o de entrega de información o de activos de información.
- No reportar los incidentes de seguridad o las violaciones a las políticas de seguridad, cuando se tenga conocimiento de ello.

- No actualizar la información de los activos de información a su cargo.
- Clasificar y registrar de manera inadecuada la información, desconociendo los estándares establecidos para este fin.
- No guardar de forma segura la información cuando se ausenta de su puesto de trabajo o al terminar la jornada laboral, *"documentos impresos que contengan información pública reservada, información pública clasificada (privada o semiprivada)*".
- No guardar la información digital, producto del procesamiento de la información perteneciente a Fundelima SA.
- Dejar los computadores encendidos en horas no laborables.
- Permitir que personas ajenas a Fundelima SA, deambulen sin acompañamiento, al interior de las instalaciones, o áreas no destinadas al público para evitar la extracción de información por cualquier medio. El colaborador que autorice el ingreso de un tercero a las instalaciones es responsable de la estadía de este tercero dentro de la empresa.
- Almacenar en los discos duros de los computadores personales de los usuarios, la información de la empresa.
- Solicitar cambio de contraseña de otro usuario, sin la debida autorización del titular o su jefe inmediato.
- Hacer uso de la red de datos de la institución, 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.
- Utilización de software no relacionados con la actividad laboral y que pueda degradar el desempeño de la plataforma tecnológica de la empresa
- Recibir o enviar información institucional a través de correos electrónicos personales, diferentes a los asignados por la empresa.
- Enviar información reservada o información clasificada de la empresa por correo, copia impresa o electrónica sin la debida autorización y sin la utilización de los protocolos establecidos para la divulgación.
- Usar dispositivos de almacenamiento externo en los computadores, cuya autorización no haya sido otorgada por la Gerencia o Dirección Administrativa.
- Negligencia en el cuidado de los equipos, dispositivos portátiles o móviles entregados para actividades propias de Fundelima.
- No cumplir con las actividades designadas para la protección de los activos de información de Fundelima.
- Destruir o desechar de forma incorrecta la documentación institucional.
- Descuidar documentación con información reservada o clasificada de la empresa, sin las medidas apropiadas de seguridad que garanticen su protección, así como abandonarlos en lugares públicos o de fácil acceso.
- Almacenar información pública reservada o clasificada, en cualquier dispositivo de almacenamiento que no permanezca a Fundelima o conectar computadores portátiles u otros sistemas eléctricos o electrónicos personales a la red de datos de Fundelima, sin la debida autorización.
- Promoción o mantenimiento de negocios personales, o utilización de los recursos tecnológicos de Fundelima para beneficio personal.

- El que impida u obstaculice el funcionamiento o el acceso normal al sistema informático, los datos informáticos o las redes de telecomunicaciones de Fundelima, sin estar autorizado.
- El que destruya, dañe, borre, deteriore o suprima datos informáticos o un sistema de tratamiento de información de Fundelima.
- El que distribuya, envíe, introduzca de manera intencional software malicioso u otros programas de computación de efectos dañinos en la plataforma tecnológica de Fundelima.
- El que viole datos personales de las bases de datos de Fundelima.
- El que superando las medidas de seguridad informática suplante un usuario ante los sistemas de autenticación y autorización establecidos por Fundelima.
- No mantener la confidencialidad de las contraseñas de acceso a la red de datos, los recursos tecnológicos o los sistemas de información de Fundelima o permitir que otras personas accedan con el usuario y clave del titular a éstos.
- Permitir el acceso u otorgar privilegios de acceso a las redes de datos de Fundelima a personas no autorizadas.
- Llevar a cabo actividades fraudulentas o ilegales, o intentar acceso no autorizado a cualquier computador de Fundelima o de terceros.
- Retirar de las instalaciones de la empresa, estaciones de trabajo o computadores portátiles que contengan información institucional sin la autorización pertinente.
- Entregar, enseñar y divulgar información calificada de Fundelima SA a personas o entidades no autorizadas.
- Realizar cambios no autorizados en la plataforma tecnológica del Fundelima
- Acceder, almacenar o distribuir pornografía infantil.
- Instalar programas o software no autorizados en las estaciones de trabajo o equipos portátiles institucionales, cuyo uso no esté autorizado por el Área de Sistemas o la Gerencia.
- Copiar sin autorización los programas de Fundelima, o violar los derechos de autor o acuerdos de licenciamiento.

10. CONTROL DE CAMBIOS

Versión	Descripción del Cambio	Fecha
1	Edición del Documento	Enero/19
2	Se adicionó al comité de seguridad al Asistente Administrativo y al Analista TIC, y se agregó la periodicidad de reuniones al comité	Marzo/2022

Revisó: **Aprobó:**

Cargo: *Coordinador de Gestión Integral*	***Cargo:*** *Gerente General*