Con el objetivo de proteger, salvaguardar y conservar las características esenciales de la información como son: confidencialidad, integridad y disponibilidad, evitando su posible pérdida y robo frente a amenazas internas o externas latentes en el entorno y teniendo en cuenta el Core del negocio, **AFILCO SEGURIDAD LTDA,** Establece los siguientes lineamientos y directrices que se deben cumplir por parte de su personal a nivel nacional y que permita el cumplimiento de los parámetros legales.

Esta política aplica a todos los activos de la información y sus procesos organizacionales, así como a las partes interesadas internas y externas en la prestación de los servicios naturaleza de **AFILCO SEGURIDAD LTDA.**

AFILCO SEGURIDAD LTDA y sus directivas establecen los siguientes lineamientos generales:

- Definir, implementar, operar y mejorar de forma continua la gestión de seguridad de la información, soportado en lineamientos claros alineados a las necesidades de la compañía, y a los requerimientos legales que le aplican al Core del negocio.
- Establecer los parámetros necesarios para asegurar la confidencialidad de la información que se genera en el desarrollo del Core del negocio y en el relacionamiento con clientes, trabajadores, proveedores y demás partes interesadas.
- Proteger la información generada, procesada o resguardada por los procesos de negocio, su infraestructura tecnológica y activos del riesgo que se genera de los accesos otorgados a terceros, (ej.: proveedores o clientes).
- Fortalecer la cultura de seguridad de la información en los colaboradores, terceros, contratistas, practicantes y clientes de la organización.
- Asegurar y controlar el acceso a la información, sistemas y recursos de red de la organización.
- Implementar la mejora continua de la seguridad y privacidad de la información a través de una adecuada gestión de los eventos de seguridad y las debilidades asociadas
- Asegurar la disponibilidad de sus procesos de negocio y la continuidad de su operación basada en el impacto que pueden generar los eventos de seguridad de la información
- Cumplir las obligaciones legales, regulatorias y contractuales establecidas.
  Proporcionar los recursos y herramientas necesarias para el cumplimiento de la presente política.

A continuación, se establecen los lineamientos puntuales que permitirán cumplir el objetivo de la presente política:

Lineamientos uso de dispositivos móviles y trabajo remoto:

- ✓ Proporcionar a los colaboradores todos los recursos tecnológicos necesarios para que puedan desempeñar las funciones para las cuales fueron contratados, por tal motivo salvo autorización dada por el proceso responsable, no se permite conectar a la red o instalar dispositivos fijos o móviles, tales como: computadores portátiles, tabletas, enrutadores, agendas electrónicas, celulares inteligentes, etc.

- ✓ Garantizar la seguridad de la información cuando se utiliza computación móvil e instalaciones de trabajo remoto.
- ✓ Se autoriza el uso de WhatsApp únicamente en dispositivos suministrados por la compañía, no se permite por esta aplicación, el envío de fotografías, audios, y videos y cualquier otro tipo de archivo clasificados como información confidencial y/o sensible.
- ✓ Los dispositivos móviles asignados por AFILCO SEGURIDAD LTDA deben tener la configuración realizada por Logística, así mismo solo podrá configurarse únicamente las cuentas de correo electrónico asignadas al usuario por la organización.
- ✓ Los usuarios responsables de la información de AFILCO SEGURIDAD LTDA, 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.
- ✓ Las conexiones remotas solo se podrán realizar al personal autorizado por la Gerencia en la ejecución de trabajo remoto, adicional las conexiones solo se realizarán a través de los aplicativos autorizados por la organización.
- ✓ Los dispositivos móviles deben tener contraseña de ingreso y bloqueo del equipo de manera automática y manual.
- ✓ Los dispositivos móviles corporativos 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 organización.
- ✓ Ante la pérdida del equipo, ya sea por extravío o hurto, deberá informar de manera inmediata al proceso de Logística, y continuar con el procedimiento administrativo por pérdida de elementos establecido por la compañía.
- ✓ Es responsabilidad del usuario hacer buen uso del dispositivo suministrado por el AFILCO SEGURIDAD LTDA con el fin de realizar actividades propias de su cargo o funciones asignadas en la entidad.
- ✓ Los usuarios no están autorizados a cambiar la configuración, ni a la desinstalación de software de los equipos móviles corporativos posterior a su recibo; únicamente se deben aceptar y aplicar las actualizaciones.
- ✓ Los usuarios de dispositivos móviles asignados por la compañía deben evitar hacer uso de lugares con algún riesgo de seguridad, evitando el extravío o hurto del equipo.
- ✓ Los usuarios de dispositivos móviles corporativos no deben conectarlos en computadores y/o puertos USB de uso público (Restaurantes, café internet, aeropuertos, etc.).
- ✓ Los usuarios de dispositivos móviles corporativos NO deben hacer uso de redes inalámbricas públicas.
- ✓ Todo correo enviado desde una cuenta corporativa debe llevar la firma del remitente para su identificación. En caso de gestionar el correo desde equipos que no son propiedad de la compañía, se debe configurar la firma institucional para su uso.
- ✓ Toda información gestionada por el AFILCO SEGURIDAD LTDA y que sea accedida remotamente debe ser utilizada solamente para el cumplimiento de las funciones del cargo o de las obligaciones contractuales con el compañía.

- ✓ No se debe acceder remotamente a los recursos de la red corporativa de AFILCO SEGURIDAD LTDA desde equipos que no cuenten con antivirus actualizado y funcionando, o que no cuenten con las actualizaciones de seguridad del sistema operativo o que sea de uso público (café Internet, por ejemplo) o que se sospeche que no es seguro.
- ✓ Cuando se acceda remotamente a la información de AFILCO SEGURIDAD LTDA se debe cumplir con las políticas de control de acceso (aplica para el trabajo desde casa).

Lineamientos de Seguridad para Talento Humano:

- ✓ Se debe asegurar que los trabajadores del AFILCO SEGURIDAD LTDA, adopten sus responsabilidades para atender y cumplir las políticas de seguridad de la información de la entidad y actúen de manera consistente frente a las mismas, con el fin de reducir el riesgo de pérdida de integridad, confidencialidad y/o disponibilidad de la información o de los activos de información.
- ✓ Los candidatos, aspirantes, contratistas y proveedores deben dar aprobación para el tratamiento de sus datos personales de acuerdo con la Ley 1581 de 2012, por el cual se dictan disposiciones generales del Habeas Data y se regula el manejo de la información contenida en base de datos personales.
- ✓ A la firma del contrato laboral o posesión del cargo el colaborador debe firmar un acuerdo de confidencialidad para con el AFILCO SEGURIDAD LTDA.
- ✓ Se debe capacitar y sensibilizar a los colaboradores durante la inducción sobre las políticas de seguridad de la información.
- ✓ AFILCO SEGURIDAD LTDA es el dueño de la propiedad intelectual de los avances tecnológicos e intelectuales desarrollados por los funcionarios contratistas de la entidad, derivadas del objeto del cumplimiento de funciones y/o tareas asignadas, como las necesarias para el cumplimiento del objeto del contrato. Así mismo el AFILCO SEGURIDAD LTDA es propietario de los activos de información y los administradores de estos activos son los funcionarios, contratistas o demás colaboradores de la organización (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 de Información (TIC).
- ✓ Los procesos y Lideres de Procesos son responsables de la cadena de custodia la cual se apoya en la aplicación de controles para la protección de la información según su nivel de clasificación y el recurso en donde esta se almacene.

Lineamiento de uso de internet:

- ✓ La infraestructura, servicios y tecnologías usados para acceder a internet son propiedad de AFILCO SEGURIDAD LTDA, por lo tanto, se reserva el derecho de monitorear el tráfico de internet y el acceso a la información.

- ✓ La navegación en Internet debe realizarse de forma razonable y con propósitos laborales.
- ✓ No se debe visitar y/o navegar en sitios o portales web con contenidos contrarios a la ley o a las políticas de la compañía o que representen peligro para la entidad como: pornografía, terrorismo, hacktivismo, segregación racial u otras fuentes definidas por el AFILCO SEGURIDAD LTDA.
- ✓ 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 los lineamientos de uso de internet.
- ✓ Los usuarios de los activos de información de AFILCO SEGURIDAD LTDA tienen prohibido el acceso a redes sociales, sistemas de mensajería instantánea y cuentas de correo no corporativos.

Lineamiento de disposición de 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 del uso de medios removibles de almacenamiento, por lo cual se deshabilita la funcionalidad de los puertos USB.
- ✓ El correo electrónico corporativo es exclusivo para envío y recepción de mensajes de datos relacionados con las actividades de AFILCO SEGURIDAD LTDA, no se hará uso de él para fines personales como registros en redes sociales, registros en sitios web con actividades particulares o comerciales o en general entablar comunicaciones en asuntos no relacionados con las funciones y actividades en la compañía.
- ✓ La información transmitida a través de las cuentas de correo electrónico corporativo no se considera correspondencia privada, ya que estas tienen como fin primordial la transmisión de información relacionada con las actividades ordinarias de AFILCO SEGURIDAD LTDA
- ✓ Es prohibido utilizar el correo electrónico corporativo para divulgar información confidencial, reenviar mensajes que falten al respeto o atenten contra la dignidad e intimidad de las personas, difundir propaganda política, comercial, religiosa, racista, sexista o similares, reenviar contenido y anexos que atenten contra la propiedad intelectual.
- ✓ El uso del correo electrónico personal está restringido en el equipo de cómputo asignado y/o celular corporativo.
- ✓ La recepción de correos electrónicos de dudosa procedencia debe estar restringidos por seguridad de la información, no se deben abrir y se deben eliminar automáticamente del equipo. Además, se debe informar al Área logística la situación.

Lineamiento de control de acceso:

- ✓ Todas las cuentas de acceso a los sistemas y recursos de las tecnologías de información son personales e intransferibles, cada empleado y contratista es responsable por las cuentas de acceso asignadas y las transacciones que con ellas se realicen. Se permite su uso única y exclusivamente durante el tiempo que tenga vínculo laboral o contractual con AFILCO SEGURIDAD LTDA
- ✓ Las contraseñas de acceso pueden poseer un mínimo de ocho (8) caracteres y debe contener al menos una letra mayúscula, una letra minúscula, un número y un carácter especial (+-*/@#$%&). No debe contener vocales tildadas, ni eñes, ni espacios.
- ✓ La contraseña inicial de acceso al equipo que le sea asignada debe ser cambiada la primera vez que acceda, además, debe ser cambiada con frecuencia, o cuando se considere necesario debido a alguna vulnerabilidad en los criterios de seguridad
- ✓ Todos los funcionarios deben tener la información de sus computadores de manera organizada, en carpetas, evitando tener archivos en el escritorio del Computador a la vista del personal no autorizado.
- ✓ Se debe mantener con clave el computador, de tal manera al retirarse del escritorio el protector de pantalla será el logo de la empresa y solamente la persona autorizada podrá continuar nuevamente a la sesión de trabajo, esto con el fin de evitar filtración de información.
- ✓ Todo empleado o contratista que se retire de AFILCO SEGURIDAD de forma definitiva o temporal (superior a 2 semana), deberá hacer entrega formal a quien lo reemplace en sus funciones o a su superior inmediato de la claves de acceso de las cuentas asignadas que se requieran, con el fin de garantizar la continuidad de las operaciones a su cargo.
- ✓ Los celulares asignados deben poseer clave numérica para evitar ser vulnerados por personal no autorizado o en caso de pérdida, para reservar la información contenida en los mismos.
- ✓ Impedir el acceso no autorizado a los sistemas de información, bases de datos y servicios de información, mediante el establecimiento de responsabilidades en el manejo de la información de acuerdo con su rol y tipo.
- ✓ Implementar seguridad en los accesos de usuarios por medio de técnicas de autenticación y autorización, basados en perfiles con permisos y usuarios definidos.
- ✓ Concientizar a los usuarios respecto de su responsabilidad frente a la utilización de contraseñas y equipos.
- ✓ Adoptar parámetros de escritorios y pantallas limpias a fin de proteger toda la información confidencial y reducir los riesgos de acceso no autorizado, pérdida y daño de la información, tanto durante el horario normal de trabajo como fuera del mismo.
- ✓ Almacenar bajo llave, cuando corresponda, los documentos en papel y los medios informáticos, en gabinetes y/u otro tipo de mobiliario seguro cuando no están siendo utilizados, especialmente fuera del horario de trabajo.
- ✓ Retirar inmediatamente la información sensible o confidencial, una vez impresa.

- ✓ La información de los colaboradores será custodiada bajo llave por el proceso de Talento Humano.
- ✓ Es responsabilidad del usuario el manejo apropiado a las claves asignadas de los servicios de red y de acceso a la red. Estas claves de acceso y usuarios son personales e intransferibles.
- ✓ Solo usuarios designados por AFILCO SEGURIDAD LTDA estarán autorizados para instalar software y/o hardware en los equipos, servidores e infraestructura de telecomunicaciones de AFILCO SEGURIDAD LTDA, así como el uso de herramientas que permitan realizar tareas de mantenimiento, revisión de software, recuperar datos perdidos, eliminar software malicioso.
- ✓ Todo trabajo para realizarse en los servidores AFILCO SEGURIDAD LTDA con información de la compañía, por parte de sus colaboradores o contratistas, se debe realizar en las instalaciones, no se podrá realizar ninguna actividad de tipo remoto sin la debida aprobación del proceso de Logística.

Lineamientos de seguridad física:

- ✓ Es responsabilidad de los trabajadores y contratistas velar por la conservación física de los equipos a ellos asignados, haciendo uso adecuado de ellos y en el caso de los equipos portátiles, estos podrán ser retirados de las instalaciones de AFILCO SEGURIDAD LTDA única y exclusivamente por el usuario a cargo y estrictamente para ejercer labores que estén relacionadas con la compañía.
- ✓ En caso de daño, pérdida o robo, se establecerá su responsabilidad a través de la investigación de los hechos y sanciones que se identifiquen de acuerdo con el RIT Los empleados y contratistas deberán reportar de forma inmediata al proceso de programación y logística sobre equipos de cómputo o de comunicaciones, tales como caídas de agua, choques eléctricos, caídas o golpes, peligro de incendio, peligro de robo, entre otros. Así como reportar de algún problema o violación de la seguridad de la información, del cual fueran testigos.
- ✓ Mientras se operan equipos de cómputo, no se deberá consumir alimentos ni ingerir bebidas.
- ✓ El manejo y uso de memorias USB, CELULARES y otros elementos electrónicos que se puedan conectar a los equipos, están prohibidos, evitando así la filtración de información estrictamente confidencial de AFILCO SEGURIDAD LTDA.
- ✓ Se debe evitar colocar objetos encima de los equipos de cómputo que obstruyan las salidas de ventilación del monitor o de la CPU.
- ✓ Los funcionarios de AFILCO SEGURIDAD LTDA, que se les hayan asignados equipos portátiles son responsables de su custodia y seguridad dentro de la compañía y cuando sean retirados de las instalaciones de la empresa.

Lineamiento de Gestión de Incidentes de Seguridad de la Información:

- ✓ AFILCO SEGURIDAD LTDA establece 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 de este.

Como parte de sus términos y condiciones iniciales de contratación, los empleados, firmarán un Compromiso de Confidencialidad o no divulgación, en lo que respecta al tratamiento de la información de **AFILCO SEGURIDAD LTDA, Clientes Y Proveedores**. La copia firmada del Compromiso deberá ser custodiada por el Área de Talento Humano en la carpeta de cada trabajador.

Así mismo, mediante el Compromiso de Confidencialidad el empleado declarará conocer y aceptar la existencia de determinadas actividades que pueden ser objeto de control y monitoreo. Estas actividades deben ser detalladas a fin de no violar el derecho a la privacidad del empleado.

Los datos personales incorporados en la Base de Datos de AFILCO SEGURIDAD LTDA, estarán vigentes desde la fecha en que se cuente con la autorización del Titular y durará durante el plazo necesario para cumplir sus finalidades, de manera indefinida hasta tanto no sea revocada la autorización, para tal efecto remitirse a la PL-GG-04 POLITICA DE TRATAMIENTO DE DATOS PERSONALES.

AFILCO SEGURIDAD LTDA.
GERENCIA

REPRESENTANTE LEGAL
Nombre: FABIO GARZON