POLÍTICA DE USO Y MANEJO DE INFORMACIÓN CONFIDENCIAL DE CONFIAR SEGURIDAD LTDA

1. PROPÓSITO:

El propósito de esta política es definir los estándares para salvaguardar la información contra uso no autorizado, divulgación o revelación, modificación, daño o pérdida y para asegurar el cumplimiento de requisitos legales e internos de CONFIAR SEGURIDAD LTDA.

2. ALCANCE:

Esta política aplica a todo el personal incluyendo, pero no limitado a empleados, contratistas, consultores, personal temporero y otro personal o partes interesadas de la compañía CONFIAR SEGURIDAD LTDA.

3. BASE LEGAL O NORMATIVA:

- Ley 1581 de 2012 de Tratamiento de Datos Personales.
- Ley 1273 de 2009 de Delitos Informáticos.
- Estándar 6.0.2. BASC.
- Norma Internacional ISO/IEC 27001 - Sistema de Gestión de Seguridad de la Información.

4. DEFICIONES:

- **Información sensitiva:** Esta información debe estar disponible a los empleados de CONFIAR SEGURIDAD LTDA, pero no disponible al público, Ejemplo: Directorios telefónicos internos, manuales de procedimientos operativos no críticos, listados de personal.
- **Información restringida:** Acceso a esta información debe estar limitada a una audiencia restringida, determinada por la Administración.
- Ejemplos: Planes de continuidad del negocio (ISO 22301), manuales operativos de seguridad, informes de auditoría interna.
- **Información confidencial:** Esta información debe estar solamente disponible a personas designadas.

- Ejemplos: Datos financieros no públicos, estrategias de licitación, análisis de riesgos (ISO 31000), expedientes de investigaciones, bases de datos de clientes, información personal sensible (Ley 1581).

5. POLÍTICA:

Dado a la naturaleza de la información que se maneja en CONFIAR SEGURIDAD LTDA, se debe considerar la sensibilidad de los datos que residen en los sistemas de información para el debido control y acceso. Pérdida o mal uso de esta información puede resultar en una variedad de daños, tales como pérdida de confidencialidad e incumplimiento de requisitos legales e internos de la compañía.

5.1 ASPECTOS GENERALES

Todo documento, carpeta, y otros medios de almacenamiento que contienen información sensitiva, restringida o confidencial debe ser ubicada en áreas protegidas. Estos medios de almacenamiento de información nunca deben ser ubicados en un lugar donde visitantes pueda tener acceso a ellos.

Diversos tipos de datos presentan varios riesgos. Preste atención particular a cómo se guarda la información personal: tarjetas de crédito o información financiera, y otros datos sensibles. Si no existe una necesidad legítima de información personalmente identificable, para un proceso específico no la guarde. Si existe una necesidad legítima de negocio de la información, guárdela solamente mientras sea necesario.

Los medios de almacenamiento de información que contienen información sensitiva, restringida o confidencial debe ser guardada en un área segura a final de cada día laborable.

Las computadoras portátiles (“laptops”) y otros dispositivos portátiles (tales como memoria USB / pendrive, etc.) que contiene información de CONFIAR SEGURIDAD LTDA, debe tener instalado software de cifrado (“encryption”) y si no está siendo utilizada o no está en la posesión directa del usuario asignado, debe estar asegurada físicamente.

Toda información de respaldo de datos (“backup”) enviado o almacenado en medios de datos (por ejemplo. disquetes, CD, discos ópticos, etc.) debe ser protegido y debe ser manejado según los procedimientos aplicable de librerías de medios políticas y seguridades vigentes en la compañía.

Las infracciones de esta política pueden tener como resultado acciones disciplinarias conforme a políticas y procedimientos disciplinarios vigentes en CONFIAR SEGURIDAD LTDA.

5.2 PRÁCTICAS EN LAS ÁREAS DE OFICINAS

Todas las computadoras deben ser aseguradas cuando el área de trabajo está desocupada o desatendida (Ej. Bloqueo de sesión con Windows + L). El área de TIC será responsable de aplicar un mecanismo automático para imponer esta práctica (ej. protector de pantalla con contraseña).

Todo documento, carpeta, y otros medios de almacenamiento que contienen información sensitiva, restringida o confidencial debe ser retirada del escritorio y asegurada en archivos de gaveta al final de la jornada de trabajo (Política de Escritorio Limpio). Cada usuario es responsable de asegurar todo documento y medio electrónico de almacenamiento que contenga información sensitiva o confidencial que esta esté ubicada en gavetas o archivos con llave. Las contraseñas no pueden ser dejadas en notas en el escritorio ni en una ubicación accesible.

Los informes impresos que contienen información sensitiva, restringida o confidencial deben ser retirados inmediatamente de las impresoras. 5.2.6 Al momento de desechar, los documentos sensitivos o confidenciales deben ser destruidos en equipos “shredders” (destructoras de papel) para hacerlos ilegibles.

Controles de acceso y monitoreo deben ser aplicados en áreas de oficina e instalaciones de almacenaje donde resida información restringida o confidencial.

Al momento de desechar, los documentos sensitivos o confidenciales deben ser destruidos en equipos “shredders”.

Controles de acceso y monitoreo deben ser aplicados en áreas de oficina e instalaciones de almacenaje donde resida información restringida o confidencial.

Las impresoras y los equipos para facsímil (“Fax”) deben ser localizados en áreas donde el público no pueda ver información sensitiva, restringida o confidencial.

5.3 PRÁCTICAS DE SEGURIDAD DIGITAL Y REMOTA

Correo Electrónico: El correo electrónico corporativo es el medio oficial de comunicación. Se prohíbe el envío de información confidencial o restringida a cuentas de correo personales (Gmail, Hotmail, etc.) o de terceros no autorizados. Use la Copia Oculta (CCO) al enviar correos a múltiples destinatarios externos. Sea escéptico ante correos no solicitados y reporte cualquier sospecha de phishing (suplantación) al área de TIC.

Teletrabajo y Acceso Remoto: El personal que acceda a los sistemas de CONFIAR SEGURIDAD LTDA desde fuera de las instalaciones debe hacerlo exclusivamente

a través de los mecanismos autorizados (ej. VPN). Es responsabilidad del usuario asegurar su red doméstica (ej. Wi-Fi con contraseña robusta) y que los equipos corporativos no sean utilizados por terceros o familiares.

Uso de la Nube: Se prohíbe el almacenamiento de información clasificada (sensitiva, restringida o confidencial) de la compañía en servicios de almacenamiento público no autorizados por la Gerencia y el área de TIC (ej. Dropbox, Google Drive personal, WeTransfer).

Ingeniería Social: Todo el personal debe estar alerta a intentos de ingeniería social (obtener información confidencial mediante engaño, suplantación telefónica o por correo). Nunca divulgue contraseñas ni información confidencial a menos que esté seguro de la identidad del solicitante y su autorización para recibirla.

5.4 PROCESO DE NOTIFICACIÓN

En eventos los cuales información sensitiva, restringida o confidencial es extraviada, robada, divulgada a entidades no autorizadas (intencional o accidentalmente), o si este acontecimiento incluye pérdida de cualquier equipo (computador, celular), medio electrónico (USB) o sospecha de infección por malware (virus, ransomware), se debe notificar inmediatamente al área de TIC.

Bajo ninguna circunstancia el usuario debe intentar solucionar el incidente por sí mismo (ej. conectar un USB infectado en otro equipo, eliminar correos de evidencia, pagar un rescate digital o negociar con un atacante). La prioridad es notificar para contener el incidente.

5.5 NOTIFICACIÓN AL SOCIO

CONFIAR SEGURIDAD LTDA en una base anual, les divulgará a todos sus socios con cuentas activas la política de confidencialidad en la información personal y financiera que estos suministran y es custodiada por la institución.

La divulgación será presentada en formato tabulado y enviado por correo a la última dirección conocida del socio.

Esta divulgación de privacidad, será suministrada de igual forma, a toda persona que así lo solicite.

6.0 MEDIDAS DISCIPLINARIAS

Las sanciones aplicables al personal, de acuerdo con la ocurrencia o severidad de la violación o infracción a esta política se regirá por lo establecido en el Reglamento interno de trabajo.

CONFIAR SEGURIDAD LTDA se reserva la facultad de aplicar la sanción más severa, en este caso el despido, en aquella ocasión en que la gravedad o seriedad de la infracción no amerite permitir que se repita en una futura ocasión.

7.0 VIGENCIA

Esta Política deja sin efecto cualquier circular, carta o política anteriormente emitido sobre los aspectos aquí cubiertos. La Alta dirección puede enmendar esta política en cualquier momento.

La Administración, mediante la implantación de esta política, debe asegurar que la debida diligencia sea ejercitada por todos los individuos involucrados en la operación de los sistemas de información presentes en la CONFIAR SEGURIDAD LTDA.

JOSE ALEJANDRO HOYOS MOR
REPRESENTANTE LEGAL
Última actualización
15/10/2025