1. OBJETIVO GENERAL

Establecer un marco de referencia formal para la gestión de la seguridad de la información y la protección de datos personales en CONFIAR SEGURIDAD LTDA, con el fin de proteger sus activos de información contra todas las amenazas, internas o externas, deliberadas o accidentales. Esta política busca asegurar la Confidencialidad, Integridad y Disponibilidad (CID) de la información, cumpliendo con los requisitos de negocio, los compromisos contractuales con los clientes y las exigencias de la legislación colombiana.

2. OBJETIVOS ESPECÍFICOS

- Alinear la estrategia de seguridad de la información con los objetivos de negocio de la compañía, especialmente en la prestación de servicios de seguridad y la operación del Centro de Operaciones (COS).
- Proteger los activos de información contra accesos no autorizados, divulgación, modificación o destrucción.
- Cumplir de manera rigurosa con el marco legal colombiano, incluyendo la Ley 1581 de 2011 (Habeas Data), Ley 1273 de 2009 (Delitos Informáticos) y los estándares internacionales de la familia ISO 27001:2022.
- Gestionar proactivamente los riesgos de seguridad de la información, reduciendo su probabilidad e impacto.
- Fomentar una cultura de seguridad en todos los empleados, contratistas y terceros, asegurando que comprendan sus responsabilidades.

3. ALCANCE

Esta política es de cumplimiento obligatorio y aplica a:

- Toda la información propiedad de CONFIAR SEGURIDAD LTDA o custodiada por esta (perteneciente a clientes, empleados y terceros), independientemente de su forma (digital, física, verbal).
- Todos los activos de información que la procesan, almacenan o transmiten (software, hardware, redes, bases de datos, sistemas en el COS, servidores, portátiles).
- Todo el personal (empleados directos, directivos, contratistas, temporales y terceros) que, en el ejercicio de sus funciones, tenga acceso a dichos activos e información.

4. DEFINICIONES CLAVE (ISO 27001 / LEY 1581)

- Activo de Información: Cualquier información o recurso (hardware/software) que tenga valor para la organización.

- Confidencialidad: Propiedad de que la información no se pone a disposición ni se revela a individuos, entidades o procesos no autorizados.
- Integridad: Propiedad de salvaguardar la exactitud y completitud de la información y los métodos de procesamiento.
- Disponibilidad: Propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada.
- Dato Personal: Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables.
- Dato Sensible: Datos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación (ej. origen racial, orientación política, datos biométricos, datos de salud).
- Tratamiento de Datos: Cualquier operación sobre datos personales (recolección, almacenamiento, uso, circulación, supresión).
- Titular: Persona natural cuyos datos personales sean objeto de Tratamiento.
- Responsable del Tratamiento: (En este caso, CONFIAR SEGURIDAD LTDA) Persona que decide sobre la base de datos y/o el Tratamiento de los datos.

5. ROLES Y RESPONSABILIDADES

- Gerencia General (Alta Dirección): Liderar, aprobar y asignar los recursos necesarios para el Sistema de Gestión de Seguridad de la Información (SGSI). Es el máximo responsable de velar por su cumplimiento.
- Oficial de Seguridad de la Información (Designado): (Rol clave faltante en el procedimiento actual) Designar a un responsable (ej. Director de Operaciones o Jefe de TI) de supervisar la implementación, cumplimiento y auditoría de esta política.
- Directores y Jefes de Área (Lideres del Proceso): Implementar y hacer cumplir esta política en sus respectivos equipos. Son responsables de clasificar la información que manejan y de gestionar los accesos de su personal.
- Área de Tecnología (TI): Implementar, gestionar y mantener los controles técnicos (firewalls, antivirus, backups, VPNs, gestión de accesos) que soportan esta política.
- Área de Gestión Humana: Asegurar que la seguridad de la información sea parte de la inducción y reentrenamiento. Administrar el acuerdo de confidencialidad y el proceso disciplinario en caso de incumplimiento.

- Todos los Empleados y Contratistas: Es su obligación conocer, entender y cumplir esta política, el acuerdo de confidencialidad firmado y reportar cualquier incidente de seguridad.

6. POLÍTICAS ESPECÍFICAS (DOMINIOS ISO 27001)

6.1. Política de Clasificación de la Información

Toda la información se clasifica para determinar su nivel de protección:

- Nivel 1: Pública: Información diseñada para divulgación (ej. material de marketing).
- Nivel 2: Uso Interno: Información operativa no sensible (ej. formatos, manuales genéricos).
- Nivel 3: Confidencial: Información sensible cuya divulgación no autorizada causa un daño moderado a la compañía o clientes. (ej. listados de personal, datos de nómina, consignas generales).
- Nivel 4: Restringida: Información crítica cuya divulgación causa un daño grave (legal, financiero, reputacional). Requiere los controles más estrictos.

  Ejemplos: Esquemas de seguridad de clientes, análisis de riesgos, datos personales sensibles (Ley 1581), videos de CCTV de incidentes, informes de investigación, credenciales de administrador, estados financieros estratégicos.

6.2. Política de Control de Acceso

- Principio de Mínimo Privilegio: El acceso a la información y sistemas se concederá basándose estrictamente en el rol y la "Necesidad de Saber".
- Gestión de Cuentas: TI es responsable del ciclo de vida (creación, modificación, eliminación) de las cuentas de usuario. Gestión Humana debe notificar las retiradas inmediatamente para suspender los accesos.
- Uso de Contraseñas: Las contraseñas son personales e intransferibles. Deben tener una robustez mínima (ej. 10 caracteres, alfanuméricos) y cambiarse periódicamente (máx. 90 días).
- Acceso al COS: El Centro de Operaciones (COS) es un área de acceso Restringido. El ingreso de personal no adscrito al COS (incluyendo gerentes, directores y jefes) debe ser autorizado y registrado en bitácora.

6.3. Política de Seguridad Física y del Entorno

- Perímetros Seguros: Las áreas que procesan información Nivel 4 (COS, Servidores, Gestión Humana) deben tener controles de acceso físico (ej. puerta de seguridad, acceso controlado).
- Política de Escritorio y Pantalla Limpia (Mandatorio):
    - Toda información Confidencial/Restringida física (carpetas, informes) debe guardarse bajo llave fuera del horario laboral.
    - Todos los equipos deben ser bloqueados (Win+L) siempre que el usuario se ausente de su puesto.
- Prohibición de Dispositivos en Áreas Críticas: Se prohíbe el ingreso de teléfonos móviles personales y memorias USB no autorizadas al Centro de Operaciones (COS) para evitar la fuga de información sensible.

6.4. Política de Seguridad de las Comunicaciones

- Uso del Correo Corporativo: El correo (@confiarseguridad.com.co) es la herramienta oficial para toda comunicación sensible.
- Prohibición de Canales Inseguros (WhatsApp): Se prohíbe terminantemente la transmisión de información Nivel 3 (Confidencial) y Nivel 4 (Restringida) por medios no corporativos como WhatsApp.

    Ejemplos prohibidos: Fotos de consignas, videos de CCTV de clientes, informes de incidentes, datos personales de guardas.
- Uso de VPN: Todo acceso remoto a los sistemas internos de Confiar (ej. Teletrabajo) debe realizarse obligatoriamente a través de la VPN corporativa.

6.5. Política de Uso Aceptable de Activos

- Los activos (portátiles, software, redes) son propiedad de Confiar Seguridad y se destinan a fines laborales.
- Se prohíbe la instalación de software no licenciado (pirata), el uso de P2P, y el acceso a sitios de contenido inapropiado o ilegal.
- El uso de medios extraíbles (USB) corporativos será controlado y monitoreado.

6.6. Política de Antivirus y Copias de Seguridad

- Antivirus (Endpoint Protection): Todos los equipos deben tener el antivirus corporativo activo y actualizado.

- Copias de Seguridad (Backup): El área de TI mantendrá un procedimiento de copias de seguridad de la información crítica (servidores), validando periódicamente su restauración.

6.7. Política de Seguridad en Dispositivos Móviles y Teletrabajo

- El teletrabajo es un privilegio y requiere que el empleado asegure las mismas condiciones de confidencialidad que en la oficina (ej. conexión segura, pantalla no visible por terceros).
- Los dispositivos móviles corporativos deben tener clave de bloqueo y reporte inmediato en caso de pérdida o robo.

7. TRATAMIENTO DE DATOS PERSONALES (LEY 1581 DE 2011)

- Autorización del Titular: No se recolectará ningún dato personal (empleados, clientes, visitantes) sin la autorización previa, expresa e informada del Titular (ej. firma en contrato, aviso de videovigilancia).
- Finalidad: Los datos personales recolectados (ej. hojas de vida, datos biométricos) se usarán únicamente para la finalidad informada al titular (ej. proceso de selección, pago de nómina, control de acceso).
- Custodia de Datos Sensibles: Los datos sensibles (exámenes médicos, polígrafos, huellas dactilares) tendrán el máximo nivel de protección (Nivel 4 - Restringido) y acceso limitado al personal de Gestión Humana o Seguridad autorizado.
- Derechos (ARCO): Se garantizará el derecho de los titulares a Conocer, Actualizar, Rectificar o Suprimir sus datos, a través del canal designado por la compañía.
- Aviso de Privacidad: Se debe publicar el Aviso de Privacidad de Confiar Seguridad en los puntos de recolección de datos (recepción, página web, etc.).

8. GESTIÓN DE INCIDENTES DE SEGURIDAD

- Definición: Un incidente es cualquier evento que comprometa la CID de la información (ej. fuga de datos, ransomware, pérdida de portátil, envío de correo sensible a destinatario erróneo).
- Reporte Obligatorio: Todo empleado debe reportar inmediatamente cualquier sospecha o incidente al Área de TI o a su jefe inmediato. Ocultar un incidente será considerado una falta grave.

9. OBLIGACIONES CLAVE Y REGLAMENTO INTERNO DEL TRABAJO

Por medio de esta política se establecen los lineamentos y directrices para los empleados, clientes y terceros de Confiar Seguridad entiendan sus

responsabilidades; esta sección consolida las obligaciones indelegables del personal y las prohibiciones explícitas:

1. Adherencia: Todo el personal está en la obligación de conocer, entender y cumplir cabalmente esta política y todos los procedimientos de seguridad de la información.
2. Acuerdo de Confidencialidad: Al firmar su contrato laboral, todo empleado debe firmar el Acuerdo de Confidencialidad de la compañía. Esta obligación de confidencialidad persiste incluso después de terminada la relación laboral.
3. Autorización de Tratamiento de Datos: Todo el personal debe dar su autorización para el tratamiento de sus datos personales según la Ley 1581 de 2012, para las finalidades propias de la relación laboral.
4. Capacitación: Es obligación del personal asistir y participar activamente en todas las capacitaciones y sensibilizaciones sobre seguridad de la información y protección de datos que programe la compañía.
5. Prohibiciones Específicas: Se incorporan dentro de las prohibiciones del Reglamento Interno de Trabajo las siguientes, y su incumplimiento será considerado FALTA GRAVE:
    - El uso indebido o destino diferente de los recursos electrónicos e informáticos entregados por el empleador (equipos, software, internet).
    - Hacer copia, extraer o divulgar (ej. por WhatsApp, correo personal) archivos, videos o información de la compañía (Nivel 3 y 4) para fines distintos a los autorizados.
    - El uso, descarga o instalación de software para el cual CONFIAR SEGURIDAD LTDA no cuente con la licencia respectiva (software pirata).
    - No mantener en estricta reserva los programas, análisis, informes de riesgo y esquemas de seguridad de la compañía y sus clientes.

10. SANCIONES (LEY 1273 DE 2009)

El incumplimiento de cualquiera de las disposiciones contenidas en esta política será considerado una falta grave y dará lugar a las acciones disciplinarias estipuladas en el Reglamento Interno de Trabajo, incluyendo la terminación del contrato de trabajo con justa causa, de acuerdo con la legislación laboral vigente.

Lo anterior es sin perjuicio de las acciones civiles o penales que CONFIAR SEGURIDAD LTDA o los clientes afectados puedan emprender contra el infractor. Acciones como el acceso abusivo a un sistema, la violación de datos personales (Ley 1581) o el uso de software malicioso (Ley 1273) constituyen delitos en Colombia.

11. REFERENCIAS

Organización Internacional de Normalización. (2022). Guía de responsabilidad social (ISO 27001). https://www.iso.org/standard/27001

La presente política se actualiza el 15 de octubre del 2025.

JOSE ALEJANDRO HOYOS MOR
REPRESENTANTE LEGAL