SIG.Pol.010-v2
23/02/2025
POLÌTICA DE SEGURIDAD DE LA INFORMACIÒN

Proceso SIG

VIGILADO Super Vigilancia Res 20204100009567 de 27/12/2020

1. DECLARACIÓN DE LA ALTA DIRECCIÓN

SEGURIDAD APOLO LTDA., empresa dedicada a la prestación de servicios de vigilancia y seguridad privada, se compromete a proteger la Confidencialidad, Integridad y Disponibilidad (CID) de todos sus activos de información y de las bases de datos personales bajo su custodia (clientes, colaboradores operativos y administrativos, candidatos, proveedores y visitantes).

En estricto cumplimiento de la Ley Estatutaria 1581 de 2012, el Decreto Único 1074 de 2015, las directrices de la Superintendencia de Industria y Comercio (SIC) —incluyendo las disposiciones de la Resolución No. 67785 del 31 de octubre de 2023— y en articulación con los sistemas ISO 9001, ISO 18788, SARLAFT y PTEE, la Alta Dirección establece la presente Política de Seguridad de la Información bajo el principio de Responsabilidad Demostrada y mejora continua.

2. OBJETIVO

Establecer los lineamientos y controles administrativos, humanos y técnicos (físicos y lógicos) necesarios para prevenir el acceso no autorizado, adulteración, pérdida, consulta, uso o circulación fraudulenta de la información y de los datos personales tratados por SEGURIDAD APOLO LTDA.,

3. ALCANCE

Esta política es de obligatorio cumplimiento para todos los niveles de la organización: Representantes Legales, directores y Líderes de Proceso, personal administrativo, personal operativo (vigilantes, supervisores, operadores de medios tecnológicos), así como contratistas, proveedores y encargados del tratamiento que tengan acceso físico o digital a las instalaciones, plataformas (como SharePoint, Monday.com, correo corporativo y servidores) o archivos físicos de SEGURIDAD APOLO LTDA.

4. PILARES DE LA SEGURIDAD DE LA INFORMACIÓN

- **Confidencialidad:** Garantizar que la información (especialmente datos sensibles como huellas biométricas, historias clínicas ocupacionales, estudios de seguridad, antecedentes y registros fílmicos) sea accesible únicamente por el personal estrictamente autorizado según su rol.

- **Integridad:** Asegurar la exactitud, veracidad y completitud de la información y los métodos de procesamiento, evitando modificaciones no autorizadas.
- **Disponibilidad:** Garantizar que los usuarios autorizados tengan acceso oportuno a la información y a las bases de datos cuando lo requieran para la operación del servicio y el cumplimiento de requerimientos legales.

5. MEDIDAS Y CONTROLES DE SEGURIDAD IMPLEMENTADOS

Para dar cumplimiento a los estándares exigidos por la SIC se implementa y audita de forma permanente los siguientes controles:

5.1. Controles Administrativos (Gobernanza y Procesos)

1. **Clasificación de la Información:** Toda información generada o recibida se clasifica en: *Pública, de Uso Interno, Confidencial* y *Restringida (Datos Sensibles)*.
2. **Debida Diligencia y Terceros:** En articulación con **SARLAFT y PTEE**, todo proveedor o encargado que acceda a bases de datos debe suscribir cláusulas de confidencialidad y transmisión/encargo de tratamiento de datos personales.
3. **Ciclo de Vida del Dato:** La recolección de datos cuenta siempre con Autorización Previa, Expresa e Informada del titular (física o digital), conservándose en los expedientes físicos y en el repositorio digital (SharePoint).

5.2. Controles Humanos (Gestión del Talento Humano)

1. **Selección y Vinculación Segura:** Verificación rigurosa de antecedentes y estudios de seguridad antes de otorgar acceso a sistemas o archivos (conforme al Procedimiento de Selección de Personal).
2. **Acuerdos de Confidencialidad:** Todo colaborador firma al momento de su ingreso un compromiso de confidencialidad y reserva de la información, cuyas obligaciones subsisten aún después de finalizado el vínculo laboral.
3. **Capacitación y Sensibilización Continua:** Ejecución periódica de jornadas de formación obligatoria sobre Protección de Datos Personales, Seguridad de la Información, dejando registro documental de asistencia y evaluación de eficacia.
4. **Retiro o Cambio de Rol:** Revocación inmediata de credenciales de acceso (correo, SharePoint, Monday.com, software contable/nómina) y entrega formal de activos al finalizar el contrato laboral.

5.3. Controles Técnicos y Lógicos (Seguridad Digital)

VIGILADO Super Vigilancia Res 20204100009567 de 27/12/2020

1. **Control de Acceso Basado en Roles (RBAC):** Asignación de permisos en el repositorio central (**SharePoint**), tableros de gestión (**Monday.com**) y carpetas compartidas bajo el principio de *mínimo privilegio* (cada cargo accede únicamente a las carpetas de su proceso).
2. **Gestión de Contraseñas y Autenticación:** Uso obligatorio de contraseñas robustas e individuales para cada usuario, bloqueo automático de sesiones por inactividad y prohibición expresa de compartir credenciales.
3. **Seguridad Perimetral y de Endpoints:** Uso de software antivirus/ licenciado y actualizado, bloqueo de puertos o dispositivos de almacenamiento extraíbles no autorizados en equipos críticos y cifrado de comunicaciones.
4. **Copias de Respaldo (Backups):** Ejecución periódica y automatizada de copias de seguridad de las bases de datos y archivos críticos en almacenamiento en la nube seguro, con pruebas periódicas de restauración.
5. **Trazabilidad y Monitoreo:** Registro de bitácoras de acceso y modificación sobre los repositorios digitales de la compañía.

5.4. Controles Físicos y Ambientales (Instalaciones y Archivo)

1. **Control de Acceso a Instalaciones:** Registro de ingreso y salida de personal y visitantes en la sede administrativa y puestos de trabajo, apoyado por circuito cerrado de televisión (CCTV) con avisos visibles de privacidad.

2. **Seguridad del Archivo Físico (Gestión Documental):** Las carpetas físicas de hojas de vida, contratos comerciales y documentación legal reposan en mobiliario bajo llave y en áreas de acceso restringido exclusivo para el personal autorizado de Talento Humano, Calidad y Dirección.

3. **Política de Escritorio y Pantalla Limpia:** Prohibición de dejar documentos con datos personales (cédulas, exámenes médicos, estudios de seguridad, listados de clientes) expuestos sobre los escritorios sin supervisión.

4. **Disposición Final Segura:** Destrucción controlada (triturado de papel o borrado seguro de medios magnéticos) de soportes que contengan datos personales cuya vida útil o tiempo de retención documental haya expirado.

VIGILADO Super Vigilancia Res 20204100009567 de 27/12/2020

6. GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

Cualquier evento sospechoso o confirmado que comprometa la confidencialidad, integridad o disponibilidad de las bases de datos (pérdida de equipos, accesos no autorizados, filtración de archivos, ataques de *ransomware* o extravío de carpetas físicas) deberá ser reportado de forma inmediata a la Dirección de Calidad.

- **Contención y Análisis:** Se activará el protocolo de contención técnica, evaluación de impacto y análisis de causa raíz (metodología PHVA / Salidas No Conformes).

- **Reporte a la SIC:** Cuando el incidente ponga en riesgo significativo los derechos de los titulares, SEGURIDAD APOLO LTDA. realizará el reporte de novedades de incidentes de seguridad a través del RNBD dentro de los quince (15) días hábiles siguientes al momento en que se detecte y sea puesto en conocimiento del área responsable.

7. ROLES Y RESPONSABILIDADES

- **Representante Legal:** Aprobar la presente política, asignar los recursos técnicos, humanos y financieros necesarios para su implementación.

- **Dirección de Calidad y SIG / Oficial de Cumplimiento y Protección de Datos:** Liderar la implementación, monitoreo, auditoría interna y actualización de esta política.

- **Líderes de Proceso (Gestión Humana, Operaciones, Mercadeo, Compras y Financiera):** Garantizar que el personal a su cargo cumpla los controles físicos y lógicos en el manejo diario de expedientes, matrices y bases de datos.
- **Colaboradores y Contratistas:** Cumplir estrictamente las directrices de seguridad, custodiar sus credenciales y reportar cualquier vulnerabilidad o incidente.

8. RÉGIMEN SANCIONATORIO Y AUDITORÍA

El incumplimiento de los lineamientos establecidos en la presente Política será considerado una falta grave a las obligaciones laborales y contractuales, dando lugar a las sanciones previstas en el Reglamento Interno de Trabajo, sin perjuicio de las acciones civiles o penales a que haya lugar.
El cumplimiento de esta política será verificado mediante auditorías internas del Sistema de Gestión Integrado (SIG) al menos una (1) vez al año, registrando los hallazgos y planes de mejora en la matriz correspondiente.

9. VIGENCIA Y APROBACIÓN

VIGILADO Super Vigilancia Res 20204100009567 de 27/12/2020

La presente Política de Seguridad de la Información rige a partir de la fecha de su publicación, actualiza las versiones anteriores y estará disponible para consulta permanente de todos los colaboradores y partes interesadas a través de los canales oficiales y el repositorio documental de **SEGURIDAD APOLO LTDA.**

Elaboró y Revisó:



Aprobó:





VIGILADO Super Vigilancia Res 20204100009567 de 27/12/2020