Política General de Seguridad de la Información

1. Objetivo.

Establecer los lineamientos estratégicos y operativos que garanticen la protección adecuada de los activos de información de Robles & Asociados, asegurando su confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad, conforme a marcos legales nacionales, estándares internacionales y el compromiso ético de la firma con sus clientes y partes interesadas.

2. Ámbito de aplicación.

Esta política aplica a:

- Todos los colaboradores (administrativos, abogados, practicantes, asesores).
- Contratistas y consultores externos.
- Clientes, aliados estratégicos y proveedores tecnológicos.
- Sistemas de información, archivos físicos y digitales.
- Plataformas web, sistemas cloud, bases de datos y dispositivos móviles.

3. Fundamento normativo.

- Constitución Política de Colombia – Art. 15 (Derecho al habeas data).
- Ley 1581 de 2012 – Protección de Datos Personales.
- Ley 1266 de 2008 – Habeas Data financiero.
- Ley 1273 de 2009 – Delitos Informáticos.
- Decreto 1377 de 2013 – Reglamentación parcial Ley 1581.

4. Principios de seguridad de la información.

Confidencialidad: Solo el personal autorizado puede acceder a la información.
Integridad: La información debe mantenerse completa, precisa y sin alteraciones no autorizadas.
Disponibilidad: Los sistemas y la información estarán disponibles cuando sean requeridos.
Autenticidad: Se garantizará la identidad de los usuarios y la validez de la información.
Trazabilidad: Las acciones sobre los sistemas de información deben poder auditarse.
Legalidad: Todo tratamiento se rige por la normativa nacional y buenas prácticas internacionales.

5. Clasificación de la información.

NIVEL	DESCRIPCIÓN	EJEMPLOS
Pública	Información sin restricciones de acceso	Artículos publicados, boletines
Interna	Información para uso exclusivo del personal	Informes administrativos, manuales
Confidencial	Información jurídica o personal sensible	Casos de clientes, contratos, datos personales
Sensible	Datos cuyo uso indebido puede causar daño o discriminación	Historia clínica, origen étnico, orientación sexual, etc.

6. Gestión de activos de información.

- Identificación y clasificación de activos (documentos, bases de datos, sistemas).
- Asignación de responsables por activo.
- Inventarios actualizados.
- Procedimientos para el ciclo de vida del activo (creación, uso, eliminación segura).

7. Controles de seguridad implementados.

7.1 Administrativos.

- Políticas y procedimientos documentados.
- Acuerdos de confidencialidad.
- Evaluaciones de cumplimiento y auditorías.
- Gestión contractual con cláusulas de protección.

7.2 Técnicos.

- Control de accesos basado en roles.
- Cifrado de datos en tránsito y reposo.
- Firewalls, antivirus.
- Backups automáticos y pruebas de restauración.
- Monitoreo de logs y actividades críticas.

7.3 Físicos.

- Control de acceso a instalaciones.
- Custodia de archivos sensibles.
- Eliminación segura de documentos y discos duros.

8. Gestión de riesgos.

- Se mantiene un Mapa de Riesgos de Seguridad de la Información, actualizado periódicamente.
- Análisis de amenazas y vulnerabilidades.
- Planes de tratamiento de riesgos.
- Aceptación formal de riesgos residuales por la alta dirección.

9. Gestión de incidentes de seguridad

- Procedimiento estructurado para:

1. Reporte y registro inmediato.
2. Comunicación al titular de los datos y/o autoridades si aplica.
3. Mejora de controles para prevenir recurrencias.

- Canal oficial: informacion@robles-y-asociados.com

10. Continuidad del negocio.

- Plan de Continuidad del Negocio y Plan de Recuperación ante Desastres.
- Pruebas periódicas de continuidad y simulacros.
- Procedimientos para mantener operación legal mínima ante eventos adversos.

11. Seguridad en proveedores y terceros.

- Evaluación previa de riesgos del proveedor.
- Firma de Acuerdo de Confidencialidad y Política de Seguridad.
- Limitación de acceso y control de sesiones remotas.
- Auditorías y revisiones de cumplimiento cuando aplique.

12. Concienciación y formación.

- Programas de capacitación anuales en:

1. Ciberseguridad y protección de datos
2. Manejo seguro de la información del cliente
3. Reacción ante incidentes de seguridad

- Materiales de divulgación: boletines, cápsulas educativas, infografías.

13. Auditoría y cumplimiento.

- Auditorías internas anuales.
- Verificaciones de cumplimiento legal, contractual y normativo.
- Informes periódicos a la Alta Dirección.
- Sanciones por incumplimiento de esta política.

14. Mejora continua.

Esta política será revisada mínimo una vez al año, o cada vez que haya cambios normativos, tecnológicos o estructurales relevantes. Las actualizaciones serán publicadas en los canales oficiales y comunicadas a todas las partes interesadas.

15. Aceptación y compromiso.

Todos los colaboradores, aliados y proveedores que accedan a sistemas, datos o infraestructuras de Robles & Asociados, aceptan cumplir esta política y sus anexos como condición indispensable de la relación laboral o contractual.