Política General de Seguridad de la Información

RIBÓN GRUPO JURÍDICO S.A.S.

Versión	Fecha de aprobación	Elaborado por	Aprobado por	Descripción del cambio
1.0	01 / 01 / 2026	[Completar]	Melissa Ribón	Emisión inicial

1. DECLARACIÓN DE LA DIRECCIÓN

La información es el principal activo de RIBÓN GRUPO JURÍDICO S.A.S. y, en su mayor parte, corresponde a información de nuestros clientes amparada por el secreto profesional. Su protección no es una función técnica delegable: es una obligación legal y deontológica que compromete a la firma en su conjunto.

La Dirección de RIBÓN GRUPO JURÍDICO S.A.S. asume el compromiso de establecer, implementar, mantener y mejorar de manera continua un sistema de gestión de seguridad de la información proporcional al tamaño, la naturaleza y el nivel de riesgo de la firma; de asignar los recursos necesarios para su operación; y de exigir su cumplimiento a todo el personal, contratistas y terceros vinculados.

2. OBJETO

Establecer los principios, directrices y responsabilidades que rigen la protección de la confidencialidad, integridad y disponibilidad de la información gestionada por RIBÓN GRUPO JURÍDICO S.A.S., cualquiera sea su formato, soporte o ubicación.

3. ALCANCE

Esta Política aplica a la totalidad de la información creada, recibida, procesada, almacenada, transmitida o eliminada por la firma, y vincula a:

- Socios, abogados, personal administrativo y de apoyo, practicantes y judicantes.

- Contratistas, abogados corresponsales, peritos y demás terceros que accedan a información de la firma.
- Proveedores de servicios tecnológicos, de nube y de soluciones LegalTech.

Cubre los activos de información en soporte físico y digital, los equipos de cómputo y dispositivos móviles corporativos y personales autorizados, las redes, las aplicaciones, los servicios en la nube y las instalaciones físicas de la firma.

4. MARCO DE REFERENCIA

4.1. Normativo

- Constitución Política de Colombia, artículos 15 y 74 (intimidad, habeas data e inviolabilidad del secreto profesional).
- Ley Estatutaria 1581 de 2012 y Decreto Único Reglamentario 1074 de 2015, en materia de protección de datos personales.
- Ley 1273 de 2009, que tipifica los delitos contra la confidencialidad, integridad y disponibilidad de los datos y de los sistemas informáticos.
- Ley 1123 de 2007, Código Disciplinario del Abogado, en particular los deberes de reserva y lealtad con el cliente.
- Ley 527 de 1999, sobre mensajes de datos y firmas digitales.
- Circular Externa 002 de 2024 de la Superintendencia de Industria y Comercio, sobre tratamiento de datos personales en sistemas de inteligencia artificial.

4.2. Estándares internacionales

- ISO/IEC 27001:2022 e ISO/IEC 27002:2022 — sistemas de gestión de seguridad de la información y controles asociados.
- ISO/IEC 27701 — extensión de privacidad.
- ISO/IEC 42001:2023 — sistemas de gestión de inteligencia artificial.

- NIST Cybersecurity Framework — funciones de gobierno, identificación, protección, detección, respuesta y recuperación.

5. PRINCIPIOS RECTORES

- **Confidencialidad.** La información solo es accesible para quien está autorizado.
- **Integridad.** La información es exacta y completa, y sus métodos de procesamiento son fiables.
- **Disponibilidad.** La información y los sistemas están accesibles cuando se requieren.
- **Secreto profesional reforzado.** La información de clientes recibe el máximo nivel de protección y no se comparte con terceros sin instrucción expresa del cliente u orden de autoridad competente.
- **Mínimo privilegio y necesidad de conocer.** Cada persona accede únicamente a la información indispensable para el desempeño de sus funciones.
- **Privacidad y seguridad desde el diseño y por defecto.** Los controles se incorporan desde la concepción de todo proceso, sistema o servicio.
- **Enfoque basado en riesgos.** Los controles se priorizan según la probabilidad y el impacto de las amenazas identificadas.
- **Defensa en profundidad.** La protección se estructura en capas independientes y complementarias.
- **Responsabilidad demostrada.** La firma documenta y conserva evidencia del cumplimiento de sus obligaciones.
- **Mejora continua.** El sistema se revisa y ajusta periódicamente.

6. ROLES Y RESPONSABILIDADES

Rol	Responsabilidades principales
Máximo órgano social / Dirección	Aprobar la Política, asignar recursos,

Rol	Responsabilidades principales
	designar al Responsable de Seguridad de la Información y revisar anualmente el desempeño del sistema.
Responsable de Seguridad de la Información	Coordinar la implementación de la Política, mantener el inventario de activos y la matriz de riesgos, liderar la atención de incidentes, ejecutar el programa de concientización y reportar a la Dirección.
Responsable de Protección de Datos	Atender consultas y reclamos de titulares, mantener el registro de bases de datos y coordinar la notificación de incidentes a la autoridad y a los titulares.
Líderes de área	Definir los perfiles de acceso de su equipo, clasificar la información bajo su responsabilidad y verificar el cumplimiento de la Política.
Todo el personal	Cumplir la Política, proteger las credenciales asignadas, reportar incidentes y sospechas, y participar en las capacitaciones.
Terceros y proveedores	Cumplir las obligaciones contractuales de confidencialidad y seguridad, y permitir la verificación de sus controles.

7. CLASIFICACIÓN DE LA INFORMACIÓN

Toda la información de la firma se clasifica en uno de los siguientes niveles, que determinan los controles aplicables en su almacenamiento, transmisión, reproducción y eliminación:

Nivel	Descripción	Ejemplos
Pública	Información destinada a difusión abierta.	Contenidos del sitio web, publicaciones, material de mercadeo.
Interna	Información de uso general dentro de la firma, no destinada a terceros.	Procedimientos internos, directorios, comunicaciones administrativas.
Confidencial	Información cuya divulgación causaría un perjuicio a la firma o a terceros.	Datos personales, información laboral, información financiera de la firma.
Confidencial privilegiada	Información de clientes amparada por el secreto profesional.	Expedientes, estrategias procesales, comunicaciones abogado-cliente, información de negociaciones.

La información confidencial privilegiada no se almacena en servicios personales, no se transmite por canales no corporativos y no se reproduce en dispositivos no autorizados.

8. DIRECTRICES DE SEGURIDAD

8.1. Gestión de identidades y control de acceso

- Cada usuario cuenta con credenciales personales e intransferibles. Está prohibido compartir contraseñas o utilizar cuentas de otras personas.
- Se exige autenticación multifactor en el correo corporativo, los servicios en la nube y toda aplicación que contenga información confidencial.

- Las contraseñas cumplen requisitos mínimos de longitud y complejidad y se gestionan preferentemente mediante un administrador de contraseñas aprobado.
- Los accesos se otorgan bajo el principio de mínimo privilegio, se documentan y se revisan al menos semestralmente.
- La desvinculación de cualquier persona conlleva la revocación inmediata de todos sus accesos y la devolución de los activos asignados.
- Se establecen muros éticos que restringen el acceso a expedientes cuando exista o pueda existir un conflicto de interés.

8.2. Uso aceptable de los recursos

- Los recursos tecnológicos de la firma se destinan al ejercicio de las funciones asignadas.
- Está prohibido instalar software no autorizado, desactivar controles de seguridad o conectar dispositivos de almacenamiento externos no aprobados.
- El uso de dispositivos personales para acceder a información de la firma requiere autorización previa y la aplicación de los controles mínimos definidos (bloqueo, cifrado, actualización y capacidad de borrado remoto).
- Se aplican las prácticas de escritorio limpio y pantalla limpia: los documentos físicos se guardan bajo llave y las sesiones se bloquean al abandonar el puesto de trabajo.

8.3. Correo electrónico y comunicaciones

- La correspondencia con clientes se realiza exclusivamente por los canales corporativos.
- Los documentos confidenciales se remiten cifrados o mediante enlaces protegidos con contraseña transmitida por un canal distinto.
- Antes de enviar, se verifica la exactitud de los destinatarios; el envío erróneo de información a un tercero constituye un incidente reportable.

- Todo mensaje sospechoso de suplantación o phishing debe reportarse sin interactuar con enlaces o archivos adjuntos.

8.4. Protección criptográfica

- Los equipos portátiles y dispositivos móviles con acceso a información de la firma mantienen cifrado el disco.
- Las comunicaciones se realizan sobre canales cifrados; el sitio web opera bajo certificado TLS vigente.
- Las llaves y certificados se custodian de forma segura y se renuevan antes de su vencimiento.

8.5. Respaldo, continuidad y recuperación

- Se realizan copias de seguridad periódicas de la información crítica, con al menos una copia almacenada en ubicación o servicio independiente.
- La restauración de las copias se prueba al menos una vez al año y el resultado se documenta.
- Se definen objetivos de punto de recuperación (RPO) y de tiempo de recuperación (RTO) para los sistemas críticos, y se mantiene un plan de continuidad que contempla la indisponibilidad prolongada de proveedores en la nube.

8.6. Seguridad física

- El acceso a la oficina y a las áreas donde se custodian expedientes se encuentra controlado.
- Los archivos físicos confidenciales se guardan bajo llave y su consulta se registra.
- La destrucción de documentos físicos se realiza por medios que impidan su reconstrucción.

8.7. Relación con proveedores y servicios en la nube

- Toda contratación de servicios que implique acceso a información de la firma exige la suscripción previa de acuerdos de confidencialidad y, cuando corresponda, de contratos de transmisión de datos personales.
- Se evalúan las condiciones de seguridad del proveedor, la ubicación de los servidores, los plazos de retención y las condiciones de portabilidad y devolución de la información al terminar el contrato.
- Se mantiene un inventario actualizado de proveedores con acceso a información confidencial y de su nivel de criticidad.

8.8. Inteligencia artificial

- Las herramientas de inteligencia artificial se rigen adicionalmente por el marco de Gobernanza de IA de la firma.
- Está prohibido cargar información de clientes en herramientas de inteligencia artificial públicas, gratuitas o carentes de acuerdo contractual de confidencialidad y no entrenamiento.
- Toda herramienta de inteligencia artificial se incorpora al inventario de activos y se somete a evaluación de riesgo antes de su habilitación.

8.9. Gestión de vulnerabilidades y cambios

- Los sistemas operativos, aplicaciones y complementos del sitio web se mantienen actualizados a la versión soportada por el fabricante.
- Se mantienen activos los mecanismos de protección contra código malicioso.
- Los cambios relevantes en la infraestructura se documentan y se valida su impacto en seguridad antes de su implementación.

8.10. Registro y trazabilidad

- Se habilitan registros de auditoría en los sistemas que contienen información confidencial.

- Los registros se protegen contra alteración y se conservan por el término definido en el procedimiento correspondiente.

9. GESTIÓN DE INCIDENTES DE SEGURIDAD

Se considera incidente de seguridad todo evento que comprometa o pueda comprometer la confidencialidad, integridad o disponibilidad de la información, incluidos los accesos no autorizados, la pérdida o robo de dispositivos, el envío erróneo de información, la infección por código malicioso y la indisponibilidad de servicios críticos.

El procedimiento de atención comprende las siguientes etapas:

- Reporte inmediato al Responsable de Seguridad de la Información por parte de quien detecte el incidente. La omisión del reporte constituye falta disciplinaria.
- Registro, clasificación y evaluación preliminar del impacto.
- Contención, erradicación y recuperación.
- Comunicación a los clientes afectados cuando su información se encuentre comprometida.
- Reporte a la Superintendencia de Industria y Comercio cuando el incidente afecte bases de datos que contengan datos personales, en los términos y plazos previstos en la normativa vigente.
- Denuncia penal cuando existan indicios de conductas tipificadas en la Ley 1273 de 2009.
- Análisis de causa raíz, documentación de lecciones aprendidas y ajuste de controles.

10. CAPACITACIÓN Y CONCIENTIZACIÓN

Todo el personal recibe inducción en seguridad de la información al vincularse y capacitación al menos anual sobre protección de datos, ingeniería social, manejo de información privilegiada, uso responsable de inteligencia artificial y

procedimiento de reporte de incidentes. La asistencia se registra y conserva como evidencia de cumplimiento.

11. CUMPLIMIENTO, AUDITORÍA Y RÉGIMEN DISCIPLINARIO

El cumplimiento de esta Política es obligatorio. Su desconocimiento no exime de responsabilidad. Las infracciones se tramitan conforme al reglamento interno de trabajo y pueden dar lugar a sanciones disciplinarias, a la terminación de la relación laboral o contractual con justa causa, y a las acciones civiles y penales que correspondan.

La Dirección dispondrá revisiones periódicas del cumplimiento y podrá contratar evaluaciones independientes cuando lo considere necesario.

12. EXCEPCIONES

Toda excepción a esta Política debe solicitarse por escrito, justificarse técnicamente, contar con la aprobación del Responsable de Seguridad de la Información y de la Dirección, señalar controles compensatorios y tener una vigencia determinada. Las excepciones vigentes se registran y se revisan al menos anualmente.

13. VIGENCIA Y REVISIÓN

Esta Política rige a partir de su aprobación y se revisa como mínimo una vez al año, y de manera extraordinaria cuando se presenten cambios normativos relevantes, modificaciones significativas en la infraestructura tecnológica o incidentes de seguridad de alto impacto.

Fecha de aprobación: 01 de enero de 2026.