

PLAN ESTRATÉGICO DE SEGURIDAD DE LA INFORMACIÓN Y POLÍTICAS DE TRATAMIENTO DE DATOS PERSONALES

IBÁÑEZ GRANADOS CONSULTORES LEGALES S.A.S.

CÓDIGO: PSI-25 (VERSIÓN 03)

TABLA DE CONTENIDO

1. INTRODUCCIÓN
2. OBJETIVOS
3. ALCANCE
4. MARCO LEGAL Y REGULATORIO
5. POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN
6. POLÍTICAS ESPECÍFICAS DE SEGURIDAD DE LA INFORMACIÓN
 - 6.1. Política de Estructura de Organización
 - 6.2. Política de Bases de Datos
 - 6.3. Política de Uso de Internet
 - 6.4. Política de Acceso Físico y de Red
 - 6.5. Política de Trabajadores
 - 6.6. Política de Gestión de Incidentes y Riesgos
 - 6.7. Política de Uso Compartido de Redes y Carpetas Virtuales
 - 6.8. Política de Seguridad de los Equipos Tecnológicos
 - 6.9. Política de Redes Sociales y Mensajería Instantánea
 - 6.10. Política de Puesto de Trabajo Limpio
 - 6.11. Política de Protección de Datos y Privacidad
 - 6.12. Política de Software No Autorizado y Antivirus
 - 6.13. Política de Copias de Seguridad (*Backups*)
7. OPERACIONES QUE AFECTAN LA POLÍTICA DE SEGURIDAD
8. RÉGIMEN SANCIONATORIO Y DISCIPLINARIO
9. ACUERDO DE CONFIDENCIALIDAD Y ATENCIÓN DE PQRS
10. MATRIZ DE CONTROL DE CAMBIOS

1. INTRODUCCIÓN

IBÁÑEZ GRANADOS CONSULTORES LEGALES S.A.S., en procura de un mejoramiento sostenido en la prestación de sus servicios jurídicos integrales, prevé la seguridad y protección de la información contra cualquier amenaza que se pueda presentar durante el desarrollo de su objeto social. El propósito es garantizar el correcto uso de los documentos almacenados de manera física, electrónica o virtual, así como de la transmitida por correos, medios tecnológicos o divulgada de forma oral en conversaciones.



Mediante la presente política se disponen las medidas que permiten garantizar la protección íntegra, la disponibilidad y la confidencialidad que corresponden al ciclo de vida de la información. El manual se enfoca en la debida observancia de la normatividad legal colombiana vigente, el régimen general de protección de datos personales y las mejores prácticas de seguridad informática.

2. OBJETIVO

Instituir las políticas de seguridad de la información en **IBÁÑEZ GRANADOS CONSULTORES LEGALES S.A.S.** para presentar de manera diáfana y coherente los elementos que la conforman a todas las personas naturales o jurídicas que tengan relación siquiera sumaria con la Firma. Se propende por el cumplimiento óptimo de los principios de integridad, reserva, disponibilidad, legalidad y confiabilidad, previniendo riesgos operacionales, tecnológicos y estratégicos.

3. ALCANCE

Esta política es de conocimiento obligatorio por parte de todos los miembros de la empresa y resulta aplicable desde el momento de su publicación. Debe ser cumplida y acatada por directivos, accionistas, empleados, clientes, contratistas, proveedores, usuarios, beneficiarios, deudores y terceros vinculados con la Firma, procurando un nivel adecuado de protección de los activos de información.

4. MARCO LEGAL Y REGULATORIO

1. **Constitución Política de Colombia (1991):** Artículo 15 (Derecho Fundamental al *Habeas Data*) y Artículo 20 (Libertad de Información).
2. **Código Penal (Ley 599 de 2000) y Código de Procedimiento Penal (Ley 906 de 2004):** Delitos informáticos y protección de datos.
3. **Ley 23 de 1982:** Propiedad Intelectual y Derechos de Autor.
4. **Ley 527 de 1999:** Acceso y uso de mensajes de datos, comercio electrónico, firmas digitales y entidades de certificación.
5. **Ley 1266 de 2007 / 2008:** Disposiciones generales del *Habeas Data* y manejo de información financiera, crediticia y comercial.
6. **Ley 1328 de 2009:** Estatuto del Consumidor Financiero.
7. **Ley 1273 de 2009:** Delitos informáticos y protección de la información.
8. **Ley 1437 de 2011:** Código de Procedimiento Administrativo y de lo Contencioso Administrativo (CPACA).
9. **Ley 1581 de 2012:** Régimen General para la Protección de Datos Personales.
10. **Decreto 1377 de 2013 y Decreto 1081 de 2015:** Reglamentación parcial de la Ley 1581 de 2012.
11. **Ley 2157 de 2021:** Modificaciones al *Habeas Data* financiero.
12. **Ley 2300 de 2023:** Protección de la intimidad de los consumidores frente a canales y horarios de contacto en cobranzas.
13. **Ley 2573 de 2026:** Por medio del cual se establecen medidas para proteger a las personas del reporte negativo ante operadores de información y el cobro de obligaciones en casos de suplantación



de identidad ante los operadores de telecomunicaciones, las entidades financieras - crediticias y demás establecimientos comerciales con esta competencia y se dictan otras disposiciones

5. POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN

La Firma propugna adecuadamente por la seguridad de la información a través de controles administrativos, técnicos y jurídicos para impedir que personas no autorizadas accedan, distribuyan, compartan, conozcan, publiquen, exporten, operen, modifiquen o alteren la información protegida bajo los principios de confidencialidad, integridad y disponibilidad. Esto se implementa mediante una cultura activa de gestión de riesgos en todos los niveles organizacionales.

6. POLÍTICAS ESPECÍFICAS DE SEGURIDAD DE LA INFORMACIÓN

6.1. Política de Estructura de Organización

- La información debe estar bajo la estricta responsabilidad de la Firma para reducir oportunidades de acceso no autorizado o modificación.
- Se mantendrá contacto con asesores y grupos especializados para capacitar al personal y alinear las labores a las políticas de seguridad.
- El uso de servicios en la nube está permitido bajo estrictos acuerdos de confidencialidad, integridad y disponibilidad.
- Los equipos tecnológicos que hayan cumplido su vida útil o representen vulnerabilidades serán actualizados de manera programada.

6.2. Política de Bases de Datos

- Se prohíbe la divulgación, modificación, retiro o destrucción no autorizada de información almacenada en bases de datos.
- Cualquier acceso físico o virtual requiere autorización expresa del Representante Legal.
- **Prohibición de extracción masiva:** Bajo ninguna eventualidad se entregarán copias de bases de datos o servidores en dispositivos removibles externos (USB, discos duros, CD, DVD), salvo requerimiento legal de autoridad judicial o administrativa.
- **Derecho de Supresión:** El titular puede solicitar la eliminación de sus datos si no son tratados conforme a la ley o transcurridos más de ocho (8) años desde su recolección. La solicitud podrá negarse por deber legal/contractual de permanencia o por necesidad de defensa en actuaciones judiciales o administrativas.

6.3. Política de Uso de Internet

- El uso de internet es estrictamente laboral, manteniéndose sujeto a monitoreo y restricciones corporativas.
- Está prohibido introducir códigos maliciosos, descargar software no autorizado o acceder a redes sociales y correos personales sin justificación y autorización del Representante Legal.



6.4. Política de Acceso Físico y de Red

- El acceso a documentos físicos se encuentra bajo llave y bajo la custodia del Representante Legal. Los empleados deben portar su carnet visible.
- Los visitantes y contratistas externos deben permanecer acompañados de forma permanente. Las contraseñas de red son personales e intransferibles.

6.5. Política de Trabajadores

- Los trabajadores deben autorizar el tratamiento de sus datos personales conforme a la Ley 1581 de 2012 mediante cláusulas contractuales.
- Se prohíbe dejar documentos confidenciales desatendidos en impresoras o escritorios, debiendo reportar de inmediato cualquier incidente de seguridad a la Dirección Jurídica.

6.6. Política de Gestión de Incidentes y Riesgos

- Se definen roles para valorar y priorizar los incidentes de seguridad (altos, medios y bajos). Los trabajadores tienen la obligación de reportar cualquier situación sospechosa.

6.7. Política de Uso Compartido de Redes y Carpetas Virtuales

- Se prohíbe almacenar archivos de audio, video o fotografía de índole personal en las carpetas compartidas. La información no pertinente se depurará en un plazo máximo de seis (6) meses. Queda prohibido almacenar información clasificada en nubes públicas o híbridas.

6.8. Política de Seguridad de los Equipos Tecnológicos

- Los equipos y dispositivos son activos institucionales destinados exclusivamente al objeto social de la Firma. Los portátiles deben mantenerse protegidos con dispositivos de sujeción (guayas).

6.9. Política de Redes Sociales y Mensajería Instantánea

- Toda publicación corporativa en redes sociales debe ser autorizada por el Representante Legal y guardar un rigor técnico y jurídico. Se prohíbe vincular cuentas de correo personales a perfiles o seudónimos institucionales.

6.10. Política de Puesto de Trabajo Limpio

- Los trabajadores deben conservar sus escritorios libres de información confidencial al ausentarse o finalizar la jornada. Es obligatorio bloquear la sesión de pantalla ante cualquier ausencia.

6.11. Política de Protección de Datos y Privacidad



- En cumplimiento de la Ley 1581 de 2012, la Firma protege la información personal de titulares, empleados y terceros, exigiendo a terceros comisionados estándares rigurosos de seguridad.

6.12. Política de Software No Autorizado y Antivirus

- Todos los equipos informáticos deben contar con software antivirus activo y actualizado. Se prohíbe desactivar o modificar las herramientas de seguridad configuradas.

6.13. Política de Copias de Seguridad (*Backups*)

- Se implementarán rutinas periódicas de respaldo y almacenamiento seguro de la información crítica, resguardando los soportes en ubicaciones segregadas de las instalaciones principales.

7. OPERACIONES QUE AFECTAN LA POLÍTICA DE SEGURIDAD

Constituyen violaciones graves al manual las siguientes conductas:

1. No reportar incidentes o riesgos de seguridad de la información.
2. Clasificar, registrar o almacenar indebidamente la información.
3. Abandonar documentos privados en escritorios o gavetas abiertas.
4. Permitir la circulación de personas ajenas sin acompañamiento en la sede.
5. Almacenar información institucional en computadores personales no autorizados.
6. Modificar, alterar o publicar datos de las bases de datos sin autorización.
7. Compartir contraseñas o permitir la suplantación de usuarios.
8. Sustraer o abandonar documentos clasificados o equipos fuera de las instalaciones.
9. Instalar software no autorizado o violar acuerdos de licenciamiento.

8. RÉGIMEN SANCIONATORIO Y DISCIPLINARIO

La transgresión de las disposiciones de este manual dará lugar a investigaciones y sanciones gestionadas por la Gerencia de Recursos Humanos. Tratándose de trabajadores, el incumplimiento se califica como **falta gravísima**, constitutiva de justa causa para dar por terminada unilateralmente la relación laboral, sin perjuicio de las acciones legales civiles o penales pertinentes. Tratándose de terceros, se exigirá la indemnización de perjuicios y la respuesta solidaria ante requerimientos administrativos.

9. ACUERDO DE CONFIDENCIALIDAD Y ATENCIÓN DE PQRS

Todos los colaboradores y contratistas están obligados a suscribir el acuerdo de confidencialidad como parte integral de sus contratos.

Las peticiones, quejas, reclamos o consultas sobre habeas data y protección de datos personales deben radicarse a través del correo electrónico institucional: **uac@igconsultoreslegales.com.co**, las cuales serán resueltas de fondo por el Oficial de Protección de Datos.



10. MATRIZ DE CONTROL DE CAMBIOS

Versión	Fecha de Aprobación	Elaboró / Responsable	Descripción Detallada del Cambio / Modificación	Aprobó
01	Enero de 2020	Dirección de Tecnología / Jurídica	Emisión inicial del Plan Estratégico de Seguridad de la Información (Ley 1581 de 2012).	Representante Legal
02	Octubre de 2024	Dirección Jurídica y Cumplimiento	Actualización normativa para incorporar la Ley 2157 de 2021 (Habeas Data financiero) y directrices iniciales de privacidad.	Representante Legal
03	Agosto de 2026	Dirección Jurídica (Daniel Ibáñez Sierra)	Actualización integral: Inclusión de los mandatos de la Ley 2300 de 2023 (canales y horarios de contacto en cobranza), refuerzo de protocolos para trabajo remoto y actualización de canales de atención (PQRS).	Representante Legal / Dirección

Razón Social: IBÁÑEZ GRANADOS CONSULTORES LEGALES S.A.S. (NIT 900.923.315-0)

Dirección: Carrera 7 No 12C-28 Piso 11 (Edificio América), Bogotá D.C.

Contacto Oficial: uac@igconsultoreslegales.com.co | www.igconsultoreslegales.com.co

11. CIERRE Y APROBACIÓN DEL MANUAL

El presente Plan Estratégico de Seguridad de la Información y Políticas de Tratamiento de Datos Personales (PSI-25) entra en vigencia a partir de su publicación y aprobación oficial por la gerencia de la compañía, en plena observancia de las normativas vigentes, incluidas las disposiciones de la **Ley 2157 de 2021** y la **Ley 2573 de 2026**. Su cumplimiento es de carácter estrictamente obligatorio para todos los colaboradores, directivos, contratistas y terceros vinculados con **IBÁÑEZ GRANADOS CONSULTORES LEGALES S.A.S.**

Cualquier duda, solicitud de aclaración o ejercicio de derechos de *Habeas Data* por parte de los titulares de la información deberá ser canalizada a través de los medios institucionales dispuestos por la Firma, garantizando una respuesta oportuna y de fondo por parte del Oficial de Protección de Datos.

APROBACIÓN INSTITUCIONAL:

- **Razón Social:** IBÁÑEZ GRANADOS CONSULTORES LEGALES S.A.S.
- **NIT:** 900.923.315-0
- **Representante Legal:** Dra. Adriana Granados Bautista
- **Domicilio Principal:** Carrera 7 No 12C-28 Piso 11, Edificio América, Bogotá D.C.
- **Canal Oficial de Contacto y PQRS:** uac@igconsultoreslegales.com.co
- **Sitio Web Oficial:** www.igconsultoreslegales.com.co

