POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

PSI — Documento Maestro de Seguridad

Razón Social	**[Nombre del estudio o empresa]**
CUIT	**[CUIT del estudio]**
Versión	1.0 — Primera emisión
Fecha de emisión	**[DD/MM/AAAA]**
Próxima revisión	**[DD/MM/AAAA — recomendado: 12 meses]**
Responsable	**[Nombre y cargo del responsable de seguridad]**
Aprobado por	**[Nombre y cargo del socio/director que aprueba]**

Control del Documento

Rol	Nombre	Firma	Fecha
Elaborado por	[Nombre]		[Fecha]
Revisado por	[Nombre]		[Fecha]
Aprobado por	[Nombre]		[Fecha]

Historial de Versiones

Versión	Fecha	Descripción del cambio	Autor
1.0	[Fecha]	Primera emisión del documento	[Nombre]

1. Introducción y Propósito

Este documento establece la Política de Seguridad de la Información (PSI) de

Este documento establece la Política de Seguridad de la Información (PSI) de **[Nombre del estudio / empresa]**. Representa el compromiso formal de la dirección con la protección de los activos de información propios y de terceros que el estudio administra en el ejercicio de su actividad profesional.

Los estudios contables y jurídicos manejan información de alta sensibilidad: datos fiscales, claves de AFIP, información patrimonial de clientes, legajos laborales y documentación con valor legal. La pérdida, alteración o divulgación no autorizada de esta información puede generar daño patrimonial, responsabilidad legal y pérdida de confianza irreparable.

Esta política aplica a todas las personas que acceden o procesan información del estudio, incluyendo socios, empleados, pasantes y proveedores de servicios externos.

2. Alcance

Esta política aplica a:

- Todo el personal del estudio, independientemente de su relación contractual (socio, empleado en relación de dependencia, pasante, colaborador externo).
- Todos los sistemas de información utilizados para procesar datos del estudio y de sus clientes, incluyendo software contable, plataformas de AFIP, correo electrónico, sistemas de gestión documental y almacenamiento en la nube.
- Todos los activos tecnológicos: computadoras de escritorio, laptops, teléfonos inteligentes, impresoras, escáneres y dispositivos de almacenamiento externo.
- Los proveedores y terceros que accedan, procesen o almacenen información del estudio en nombre de este.
- Toda la documentación física y digital generada o recibida en el ejercicio de la actividad profesional.

3. Marco Normativo de Referencia

Esta política se elaboró considerando el siguiente marco normativo y estándares aplicables:

- Ley 25.326 — Ley de Protección de Datos Personales (LPDP) y sus decretos reglamentarios.

- Resoluciones de la Agencia de Acceso a la Información Pública (AAIP) sobre seguridad de bases de datos personales.
- Secreto profesional según Código de Ética del CPCE (Consejo Profesional de Ciencias Económicas) aplicable.
- Norma ISO/IEC 27001 — Sistema de Gestión de Seguridad de la Información (referencia de buenas prácticas).
- CIS Controls v8 — Controles de Seguridad del Center for Internet Security (referencia técnica adaptada a pymes).
- Regulaciones de AFIP sobre acceso y custodia de información fiscal de terceros.

Normativa interna adicional aplicable: [Indicar convenios colectivos, acuerdos sectoriales u otras normas internas relevantes]

4. Principios Rectores de Seguridad

Toda decisión de seguridad en el estudio se basa en los siguientes principios:

🔒 **Confidencialidad**	La información sólo es accesible para las personas autorizadas según su función. Ningún empleado accede a información de clientes fuera del ámbito de su tarea asignada.
✔ **Integridad**	La información es exacta, completa y no ha sido alterada por personas no autorizadas. Los registros contables y legales tienen mecanismos de control de modificaciones.
⚡ **Disponibilidad**	Los sistemas y la información están disponibles cuando son necesarios. Los backups y los planes de continuidad garantizan la operación ante fallos.
📋 **Responsabilidad**	Toda acción sobre la información es trazable. Cada acceso, modificación o envío queda registrado y puede ser auditado en caso de incidente.
🔑 **Menor privilegio**	Cada persona accede únicamente a la información que necesita para cumplir su función. Los accesos se revisan y revocan ante cualquier cambio de rol.

5. Responsabilidades

5.1 Dirección / Socios

- Aprobar formalmente esta política y sus revisiones periódicas.

- Asignar los recursos necesarios para implementar los controles de seguridad.
- Designar al Responsable de Seguridad de la Información del estudio.
- Promover la cultura de seguridad con el ejemplo.

5.2 Responsable de Seguridad de la Información

Cargo designado: [Nombre y cargo] | Contacto: **[Email / interno]**

- Mantener actualizada esta política y todos los documentos del sistema de seguridad.
- Coordinar la respuesta ante incidentes de seguridad.
- Gestionar el alta, baja y modificación de accesos a sistemas.
- Organizar las capacitaciones periódicas al personal.
- Reportar a la dirección el estado de la seguridad trimestralmente.

5.3 Todo el Personal

- Leer, comprender y cumplir esta política y los procedimientos asociados.
- Reportar inmediatamente cualquier incidente o sospecha de incidente de seguridad.
- No compartir credenciales de acceso bajo ninguna circunstancia.
- Proteger la información de clientes con el mismo cuidado que la información propia.
- Completar las capacitaciones de seguridad en los plazos establecidos.

5.4 Proveedores y Terceros

- Cumplir con los requisitos de seguridad establecidos en el contrato de servicios.
- Firmar el Acuerdo de Confidencialidad (NDA) antes de acceder a cualquier información del estudio.
- Reportar al Responsable de Seguridad cualquier incidente que afecte datos del estudio.

6. Áreas Principales de Control

Esta política se implementa a través de los siguientes documentos específicos, cada uno con sus procedimientos detallados:

#	Documento / Procedimiento	Objetivo principal
02	Política de Uso Aceptable	Definir el uso permitido de sistemas, correo e internet
03	Acuerdo de Confidencialidad (NDA)	Proteger datos de clientes y del estudio ante terceros
04	Política de Privacidad y Datos (LPDP)	Cumplimiento de la Ley 25.326
05	Clasificación de la Información	Definir niveles de sensibilidad y manejo correcto
06	Política de Contraseñas y MFA	Controles de autenticación seguros
07	Control de Acceso	Alta/baja de usuarios y principio de menor privilegio

08	Inventario de Activos	Registro de hardware, software y licencias
09	Escritorio Limpio y Pantalla Bloqueada	Protección física de información visible
10	Trabajo Remoto	Seguridad fuera de la oficina
11	BYOD	Dispositivos personales en el entorno laboral
12	Política de Backups	Respaldo y recuperación de datos
13	Plan de Continuidad (BCP)	Operación ante interrupciones graves
14	Plan de Recuperación (DRP)	Restauración técnica tras desastre
15	Protocolo de Respuesta a Incidentes	Acción inmediata ante un ataque o fallo
16	Matriz de Riesgos	Identificación y tratamiento de amenazas
17	Seguridad con Proveedores	Requisitos para terceros con acceso a datos
18	Bitácora de Mantenimiento	Registro de parches, actualizaciones y auditorías
19	Plan de Capacitación	Cronograma de formación del personal
20	Registro de Incidentes	Historial de eventos de seguridad

7. Principales Riesgos y Controles

La siguiente tabla resume los riesgos más críticos para un estudio contable/jurídico y el control principal asignado a cada uno. El análisis completo se documenta en la Matriz de Riesgos (Documento 16).

Amenaza principal	Prob.	Impacto	Control aplicado
Ransomware / cifrado de archivos	Alta	Crítico	Backups diarios aislados + antivirus activo + parches al día
Phishing a empleados o socios	Alta	Alto	Capacitación trimestral + MFA obligatorio en cuentas críticas
Acceso no autorizado a legajos	Media	Alto	Control de acceso por rol + registro de accesos
Pérdida de dispositivo (laptop/celular)	Media	Alto	Cifrado de disco + política de pantalla bloqueada
Fallo de proveedor de software contable	Baja	Alto	Cláusula de seguridad en contrato + backup propio
Error humano (borrado accidental)	Alta	Medio	Backups con retención de 30 días + confirmación en borrado masivo

8. Incumplimiento y Sanciones

El incumplimiento de esta política puede resultar en las siguientes consecuencias, según la gravedad de la infracción:

Gravedad	Ejemplo de infracción	Consecuencia posible
⚠ Leve	No bloquear pantalla al alejarse del escritorio	Apercibimiento verbal y capacitación adicional
⛔ Grave	Compartir credenciales de AFIP o del sistema contable	Sumario disciplinario + posible acción legal por incumplimiento del deber de confidencialidad
🚨 Crítico	Divulgación deliberada de datos de clientes a terceros	Desvinculación + denuncia ante AAIP + posible acción penal (Ley 25.326)

9. Revisión y Actualización

Esta política debe revisarse como mínimo una vez al año, o ante cualquiera de los siguientes eventos:

- Cambio significativo en la estructura del estudio (incorporación de socios, fusión, apertura de nueva sede).
- Incorporación de nuevos sistemas o plataformas de software.
- Ocurrencia de un incidente de seguridad grave.
- Cambio en la normativa legal aplicable (LPDP, regulaciones de AFIP, etc.).
- Indicación del Responsable de Seguridad ante nuevas amenazas detectadas.

La revisión debe ser aprobada por la dirección del estudio y registrada en el Historial de Versiones de este documento.

10. Declaración de Compromiso de la Dirección

La dirección de **[Nombre del estudio]** declara formalmente su compromiso con la seguridad de la información como prioridad estratégica del negocio. Este compromiso incluye la asignación de recursos, la capacitación del personal, el cumplimiento de la normativa vigente y la mejora continua del sistema de gestión de seguridad.

Esta política es de cumplimiento obligatorio para todas las personas indicadas en la sección de Alcance, con vigencia a partir de la fecha de aprobación indicada en la carátula.

Firma del/la Socio/a o Director/a **[Nombre y cargo]** **[Fecha]**	Firma del Responsable de Seguridad **[Nombre y cargo]** **[Fecha]**

Anexo A — Glosario de Términos

Término	Definición
Activo de información	Cualquier dato, sistema, software o dispositivo que tiene valor para el estudio y debe ser protegido.
Autenticación de doble factor (MFA)	Método de verificación de identidad que requiere dos elementos: algo que se sabe (contraseña) y algo que se tiene (código de aplicación).
Backup / Respaldo	Copia de seguridad de la información almacenada en un lugar separado del original, para recuperación ante pérdidas.
BYOD	"Bring Your Own Device": política que permite o regula el uso de dispositivos personales para trabajo.
Clave fiscal AFIP	Credencial de acceso a los servicios web de la Administración Federal de Ingresos Públicos. De máxima confidencialidad.
Confidencialidad	Garantía de que la información sólo es accesible para personas autorizadas.
Incidente de seguridad	Cualquier evento que ponga en riesgo la confidencialidad, integridad o disponibilidad de la información.
LPDP	Ley 25.326 — Ley de Protección de Datos Personales de la República Argentina.
Menor privilegio	Principio por el cual cada usuario accede únicamente a la información necesaria para cumplir su función.
MFA	Ver "Autenticación de doble factor".
NDA	"Non-Disclosure Agreement" o Acuerdo de Confidencialidad: contrato que obliga a guardar reserva sobre información confidencial.
Phishing	Ataque por correo electrónico o mensaje que simula ser una entidad confiable para robar credenciales o datos.
PSI	Política de Seguridad de la Información: este documento.
Ransomware	Malware que cifra los archivos de la víctima y exige un rescate económico para restaurar el acceso.
Responsable de Seguridad	Persona designada por la dirección para gestionar y coordinar la seguridad de la información del estudio.
VPN	"Virtual Private Network": red privada virtual que cifra el tráfico de internet para conexiones remotas seguras.

— Fin del Documento —