MATRIZ DE RIESGOS

DE SEGURIDAD DE LA INFORMACIÓN

Identificación · Evaluación · Tratamiento · Seguimiento

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

DOCUMENTO CONFIDENCIAL — USO INTERNO EXCLUSIVO

1. Propósito

La Matriz de Riesgos es el instrumento que permite al Estudio tomar decisiones informadas sobre qué proteger primero, cuánto invertir en seguridad y dónde concentrar los esfuerzos preventivos. Sin una evaluación de riesgos, la seguridad se gestiona por intuición o por reacción ante incidentes pasados, en lugar de por priorización basada en evidencia.

Este documento identifica las amenazas más relevantes para un estudio contable o jurídico en Argentina, evalúa su probabilidad e impacto, y define los controles de tratamiento para cada riesgo. Debe revisarse anualmente y después de cualquier cambio significativo en el entorno tecnológico o normativo.

> **i** Esta matriz representa una evaluación inicial basada en amenazas típicas del sector. El Estudio debe ajustar las puntuaciones de probabilidad e impacto según su contexto específico: tamaño, clientes, herramientas tecnológicas y experiencia previa con incidentes.

2. Metodología de Evaluación

El riesgo se calcula como el producto de la Probabilidad por el Impacto:

PROBABILIDAD (P) — Escala 1 a 5	IMPACTO (I) — Escala 1 a 5
• 5 — Casi Seguro: ocurrirá en los próximos 12 meses (>90%) • 4 — Probable: ocurrirá probablemente (50-90%) • 3 — Posible: podría ocurrir (20-50%) • 2 — Improbable: ocurriría en circunstancias excepcionales (5-20%) • 1 — Raro: ocurriría solo en circunstancias extraordinarias (<5%)	• 5 — Catastrófico: pérdida irreversible de datos de clientes, cierre del Estudio, responsabilidad penal • 4 — Mayor: pérdida de datos críticos, daño reputacional grave, pérdida de clientes significativa • 3 — Moderado: interrupción operativa significativa (días), daño reputacional moderado • 2 — Menor: interrupción operativa corta (horas), daño reputacional bajo, pérdida económica menor • 1 — Insignificante: impacto mínimo, resuelto internamente sin consecuencias externas

Puntuación (P × I)	15-25 → 🔴 CRÍTICO	8-14 → 🟠 ALTO	4-7 → 🟡 MEDIO | 1-3 → 🟢 BAJO

3. Mapa de Calor de Riesgos

El siguiente mapa muestra la combinación de probabilidad e impacto y el nivel de riesgo resultante (puntuación = P × I):

PROBABILIDAD \ IMPACTO	1 Insignif.	2 Menor	3 Moderado	4 Mayor	5 Catastrófico
5 — Casi Seguro (>90%)	5	10	15	20	25
4 — Probable (50-90%)	4	8	12	16	20
3 — Posible (20-50%)	3	6	9	12	15
2 — Improbable (5-20%)	2	4	6	8	10
1 — Raro (<5%)	1	2	3	4	5

🔴 CRÍTICO (15-25)Acción inmediata	🟠 ALTO (8-14)Plan en 30 días	🟡 MEDIO (4-7)Plan en 90 días	🟢 BAJO (1-3)Monitorear

4. Criterios de Tratamiento del Riesgo

Nivel de riesgo	Acción requerida	Tratamiento y plazo
🔴 CRÍTICO	Acción INMEDIATA. No puede aceptarse. El riesgo debe reducirse antes de continuar la operación normal.	Reducir (implementar controles) o Transferir (seguro de ciberseguridad). Plazo: acción inmediata, plan completo en 7 días.
🟠 ALTO	Acción urgente. El riesgo es inaceptable a largo plazo. Requiere plan de acción formal aprobado por la dirección.	Reducir (controles adicionales) o Transferir (seguro). Plazo: plan aprobado en 15 días, implementación en 30 días.
🟡 MEDIO	Acción planificada. El riesgo es manejable con controles adicionales moderados.	Reducir o Aceptar con controles de monitoreo. Plazo: plan en 30 días, implementación en 90 días.
🟢 BAJO	Monitorear. El riesgo es aceptable con los controles actuales.	Aceptar con monitoreo periódico. Documentar la decisión de aceptación. Revisar en la evaluación anual.

5. Matriz de Riesgos del Estudio

La siguiente tabla lista los riesgos identificados para el Estudio, evaluados con la metodología de la Sección 2. Las puntuaciones de probabilidad e impacto deben ajustarse según la realidad del Estudio.

📋 Los riesgos están ordenados de mayor a menor puntuación. Comenzar el tratamiento por los riesgos críticos y altos. Ajustar la columna 'P' (Probabilidad) según la experiencia real del Estudio con cada amenaza.

ID	Categoría	Amenaza	Activo afectado	P	I	P×I	Nivel	Controles actuales	Estado
R01	Cibernético	**Ataque de ransomware que cifra todos los archivos del Estudio incluyendo bases de datos de clientes**	ERP, servidor NAS, archivos de clientes	4	5	20	🔴 CRÍTICO	Backup diario off-site (Doc.12), antivirus, MFA, Protocolo de Respuesta (Doc.15)	
R02	Cibernético	**Phishing exitoso que compromete clave fiscal AFIP del Estudio o de clientes**	Claves AFIP, datos fiscales de clientes	4	5	20	🔴 CRÍTICO	MFA obligatorio en AFIP, capacitación antiphishing, gestor de contraseñas (Doc.06)	
R03	Datos	**Filtración de datos de clientes por ex empleado con acceso no revocado**	Datos de clientes, base de datos ERP	3	5	15	🔴 CRÍTICO	Proceso de baja de usuarios (Doc.07), NDA (Doc.03), auditoría de accesos trimestral	
R04	Cibernético	**Compromiso de contraseña débil o reutilizada en sistema crítico**	ERP, correo, AFIP	5	3	15	🔴 CRÍTICO	Política de contraseñas (Doc.06), gestor de contraseñas obligatorio, MFA	
R05	Continuidad	**Pérdida total de datos por falla de hardware sin backup verificado**	ERP, archivos históricos de clientes	3	5	15	🔴 CRÍTICO	Regla 3-2-1 (Doc.12), prueba de restauración trimestral, NAS + backup en nube	
R06	Físico	**Pérdida o robo de laptop con datos de clientes sin cifrado de disco**	Datos de clientes en laptop	3	4	12	🟠 ALTO	Política de cifrado de disco (Doc.06), inventario de activos (Doc.08), borrado remoto	
R07	Humano	**Error de empleado: envío de datos de un cliente a otro por email**	Datos personales y fiscales de clientes	4	3	12	🟠 ALTO	Verificación manual antes de envío, capacitación (Doc.19), proceso de doble check	
R08	Cibernético	**Acceso no autorizado a sistemas por uso de Wi-Fi público sin VPN**	ERP, AFIP, correo corporativo	4	3	12	🟠 ALTO	Política de trabajo remoto (Doc.10), VPN obligatoria, capacitación	
R09	Proveedor	**Caída o pérdida de datos en el software contable en la nube del proveedor**	Base de datos contable principal	2	5	10	🟠 ALTO	Backup propio independiente del proveedor, SLA contractual (Doc.17)	

R10	Físico	**Incendio o inundación en la oficina que destruye equipos y archivo físico**	Todo el activo físico del Estudio	2	5	10	🟠 ALTO	Backup off-site (Doc.12), BCP (Doc.13), seguro de la oficina, archivo digital	
R11	Humano	**Uso de contraseñas de clientes para fines no autorizados por empleado**	Claves AFIP y datos de clientes	2	5	10	🟠 ALTO	NDA (Doc.03), control de accesos (Doc.07), registro de usos de claves, auditoría	
R12	Legal	**Incumplimiento LPDP por falta de registro de bases de datos ante AAIP**	Cumplimiento legal, reputación del Estudio	3	3	9	🟠 ALTO	Política de privacidad (Doc.04), inscripción ante AAIP, auditoría anual de cumplimiento	
R13	Proveedor	**Vulnerabilidad en software contable no parcheada que permite acceso no autorizado**	Datos de clientes en ERP	3	3	9	🟠 ALTO	Bitácora de mantenimiento (Doc.18), actualización mensual, comunicación con proveedor	
R14	Cibernético	**Malware descargado por empleado desde sitio web no autorizado**	PC del empleado, red del Estudio	3	3	9	🟠 ALTO	Política de uso aceptable (Doc.02), antivirus, filtrado web, capacitación	
R15	Físico	**Pérdida de dispositivo personal (BYOD) con acceso a correo corporativo**	Correo corporativo, datos de contacto	3	2	6	🟡 MEDIO	Política BYOD (Doc.11), borrado remoto, MFA en correo	
R16	Continuidad	**Ausencia imprevista del socio principal sin delegación documentada**	Operación del Estudio, vencimientos AFIP	2	3	6	🟡 MEDIO	BCP sección de personal clave (Doc.13), tabla de reemplazos documentada	
R17	Humano	**Empleado revela información de cliente en conversación en espacio público**	Reputación, secreto profesional	3	2	6	🟡 MEDIO	Capacitación en confidencialidad (Doc.19), NDA (Doc.03), código de conducta	
R18	Físico	**Documentación física confidencial visible para visitantes en recepción**	Datos de clientes en papel	4	1	4	🟡 MEDIO	Política de escritorio limpio (Doc.09), protocolo de visitas, espacio de recepción separado	
R19	Cibernético	**Acceso de proveedor TI a datos de clientes durante soporte técnico**	Datos de clientes en sistemas	2	2	4	🟡 MEDIO	NDA con proveedores (Doc.03), supervisión durante acceso, contratos con cláusulas (Doc.17)	
R20	Continuidad	**Falla de proveedor de internet en momento crítico (vencimiento AFIP)**	Operación y cumplimiento fiscal	3	2	6	🟡 MEDIO	Plan de contingencia: datos móviles como backup, BCP (Doc.13)	
R21	Físico	**Corte de energía prolongado sin UPS**	Equipos locales, continuidad operativa	2	1	2	🟢 BAJO	UPS instalado, trabajo en nube posible desde dispositivos con batería	
R22	Humano	**Pérdida de contraseña maestra del gestor de contraseñas por empleado**	Acceso a sistemas del empleado	2	2	4	🟡 MEDIO	Proceso de recuperación de acceso, Resp. Seguridad puede restablecer acceso corporativo	

6. Resumen Ejecutivo de Riesgos

Nivel de riesgo	Cantidad	IDs	Acción requerida
🔴 CRÍTICO	5	R01 – R05	Implementar o completar controles faltantes de forma inmediata. Prioridad máxima.
🟠 ALTO	9	R06 – R14	Plan de acción formal en 15 días. Implementación completa en 30 días.
🟡 MEDIO	7	R15 – R20, R22	Plan en 30 días, implementación en 90 días.
🟢 BAJO	1	R21	Monitorear y revisar en la evaluación anual.

7. Plan de Acción — Riesgos Críticos y Altos

El siguiente plan de acción detalla las tareas prioritarias para reducir los riesgos críticos y altos identificados en la Sección 5:

ID	Riesgo	Acción de tratamiento	Responsable	Plazo	Estado
R01	🔴	Verificar y completar la Regla 3-2-1: confirmar backup diario + copia off-site + prueba de restauración	[Resp. Seguridad]	30 días	Pendiente
R02	🔴	Activar MFA con token o app autenticadora en todas las claves fiscales AFIP del Estudio y de clientes	[Resp. Seguridad]	15 días	Pendiente
R03	🔴	Implementar proceso formal de baja de usuarios con checklist (Doc.07) y auditoría trimestral de accesos	[Resp. Seguridad]	7 días	Pendiente
R04	🔴	Implementar gestor de contraseñas corporativo para todo el personal	[Resp. Seguridad]	30 días	Pendiente
R05	🔴	Ejecutar primera prueba de restauración desde backup y programar pruebas trimestrales	[Resp. Seguridad]	15 días	Pendiente
R06	🟠	Activar cifrado de disco (BitLocker/FileVault) en todas las laptops del Estudio	[Resp. Seguridad]	15 días	Pendiente

R07	🟠	Implementar protocolo de verificación doble antes de enviar documentos de clientes por correo	[Resp. Seguridad]	7 días	Pendiente
R08	🟠	Instalar y configurar VPN en los equipos de todos los empleados con trabajo remoto	[Resp. Seguridad]	15 días	Pendiente
R09	🟠	Configurar backup independiente de la base de datos del software contable (no depender solo del proveedor)	[Resp. Seguridad]	30 días	Pendiente
R12	🟠	Inscribir las bases de datos del Estudio ante la AAIP conforme al art. 3 de la LPDP	[Resp. Seguridad + Asesor legal]	30 días	Pendiente

8. Registro de Nuevos Riesgos Identificados

Usar esta tabla para agregar nuevos riesgos identificados durante la operación normal o ante cambios en el entorno del Estudio. Evaluarlos con la misma metodología de la Sección 2.

ID	Cat.	Amenaza / Escenario	Activo afectado	P	I	P×I	Nivel	Controles propuestos	Estado

9. Revisión y Mantenimiento

Esta Matriz de Riesgos se revisa anualmente o ante cualquiera de los siguientes eventos:

- Incorporación de nuevos sistemas o herramientas tecnológicas.
- Cambios significativos en el modelo de negocio del Estudio (nuevos servicios, nuevos clientes corporativos).
- Ocurrencia de un incidente de seguridad que no estaba contemplado en la matriz.
- Cambios en la normativa aplicable (nuevas regulaciones de AFIP, LPDP, etc.).
- Incorporación de personal clave nuevo o cambios en las responsabilidades de seguridad.

Fecha	Revisado por	Cambios principales	Próxima revisión

Próxima revisión programada: [DD/MM/AAAA] | Responsable: [Nombre y cargo]

— Fin del Documento —