REGISTRO DE INCIDENTES

DE SEGURIDAD DE LA INFORMACIÓN

Historial · Análisis · Lecciones Aprendidas · Mejora Continua

Razón Social	**[Nombre del estudio o empresa]**
CUIT	**[CUIT del estudio]**
Versión	1.0 — Primera emisión
Fecha de inicio	**[DD/MM/AAAA — desde cuándo se usa este registro]**
Responsable del registro	**[Nombre y cargo del responsable de seguridad]**
Aprobado por	**[Nombre y cargo del socio/director que aprueba]**

🔒 ACCESO RESTRINGIDO: Este registro contiene información sobre vulnerabilidades, incidentes y brechas de seguridad del Estudio. Acceso exclusivo para el Responsable de Seguridad y los socios. No distribuir sin autorización.

CONFIDENCIAL — DISTRIBUCIÓN RESTRINGIDA

1. Propósito

El Registro de Incidentes es la memoria institucional de seguridad del Estudio. Sin un registro consistente, cada incidente se atiende de forma aislada, se pierden las lecciones aprendidas, y el mismo tipo de incidente puede repetirse porque no hay evidencia de qué funcionó y qué no.

Este registro cumple cuatro funciones esenciales: (1) Documentar cada incidente con el nivel de detalle suficiente para aprender de él. (2) Proveer trazabilidad ante auditorías, inspecciones o reclamos de clientes. (3) Alimentar las métricas del programa de seguridad para evaluar su efectividad. (4) Generar evidencia de la diligencia del Estudio en la protección de datos, relevante ante la AAIP o en litigios.

⚖ La obligación de documentar los incidentes no es opcional. La Ley 25.326 (LPDP) y las buenas prácticas de gestión de seguridad requieren que los responsables de datos puedan demostrar qué incidentes ocurrieron, cómo se gestionaron y qué medidas se tomaron para prevenir la recurrencia.

2. Alcance — Qué se Registra

Se registra en este documento todo evento de seguridad que cumpla al menos uno de los siguientes criterios:

- Afectó o pudo haber afectado la confidencialidad, integridad o disponibilidad de datos del Estudio o de sus clientes.
- Requirió una acción de respuesta por parte del Responsable de Seguridad o la dirección.
- Causó una interrupción de los sistemas o servicios del Estudio de más de 30 minutos.
- Involucró acceso no autorizado a sistemas, datos o instalaciones.
- Configuró o pudo haber configurado una brecha de datos personales bajo la LPDP.
- Fue detectado durante un simulacro de phishing y requirió capacitación adicional.

También se registran en este documento los desvíos detectados en las auditorías de accesos, los fallos de backup y las vulnerabilidades críticas identificadas en la Bitácora de Mantenimiento (Documento 18).

3. Clasificación de Incidentes

Los incidentes se clasifican conforme a la Sección 3 del Protocolo de Respuesta (Documento 15). Para referencia rápida:

Nivel	Ejemplos típicos en el Estudio	ID en este registro	Tiempo de respuesta
🔴 **CRÍTICO**	Ransomware, filtración de claves AFIP, acceso no autorizado a datos de clientes, sabotaje.	*INC-001 en adelante (numeración única)*	**Inmediato — < 15 minutos**
🟠 **ALTO**	Phishing exitoso, pérdida de dispositivo con datos de clientes, acceso indebido interno.	*INC-xxx (mismo rango, campo Severidad)*	**30 minutos**
🟡 **MEDIO**	Intento de phishing detectado, fallo de backup, dispositivo perdido sin datos críticos.	*INC-xxx*	**4 horas hábiles**
🔵 **BAJO**	Spam, contraseña olvidada, actividad sospechosa sin confirmar.	*INC-xxx*	**24 horas hábiles**

4. Responsabilidades del Registro

Rol	Responsabilidad
Cualquier empleado	Reportar inmediatamente cualquier incidente o sospecha de incidente al Responsable de Seguridad. No se requiere esperar a tener toda la información: reportar tan pronto se detecta algo anómalo.
Responsable de Seguridad	Documentar todo incidente en este registro dentro de las 24 horas de detectado. Actualizar la ficha a medida que avanza la respuesta. Cerrar formalmente el incidente cuando corresponda. Producir el informe anual de incidentes.
Dirección / Socios	Revisar el registro trimestralmente. Aprobar el cierre formal de incidentes críticos. Ser notificados de incidentes críticos en tiempo real.
Asesor Legal	Ser consultado ante incidentes que puedan configurar responsabilidad legal, especialmente brechas de datos de clientes.

5. Índice de Incidentes Registrados

Esta tabla es el índice de todos los incidentes documentados en este registro. Cada incidente tiene una Ficha completa en la Sección 6. El índice permite una visión rápida del historial y facilita la búsqueda.

ID	Fecha	Tipo	Severidad	Estado	Causa raíz identificada

Estados posibles: Abierto · En investigación · Cerrado

Tipos de incidente: Ransomware · Phishing · Malware · Acceso no autorizado · Pérdida de dispositivo · Error humano · Brecha de datos · Fallo de backup · Vulnerabilidad · Otro

6. Fichas de Incidentes

Cada incidente registrado tiene su ficha completa a continuación. Las fichas se agregan en orden cronológico. Se incluyen 3 fichas en blanco como punto de partida.

FICHA DE INCIDENTE — ID: INC-001	
SECCIÓN 1 — DATOS BÁSICOS DEL INCIDENTE	
ID del incidente	**INC-001**
Fecha y hora de detección	**[DD/MM/AAAA — HH:MM]**
Fecha y hora de reporte al Resp. Seguridad	**[DD/MM/AAAA — HH:MM]**
Reportado por	**[Nombre y cargo de quien detectó y reportó]**
Tipo de incidente	( ) Ransomware ( ) Phishing ( ) Malware ( ) Acceso no autorizado( ) Pérdida de dispositivo ( ) Error humano ( ) Brecha de datos ( ) Otro:
Severidad inicial	( ) 🔴 CRÍTICO ( ) 🟠 ALTO ( ) 🟡 MEDIO ( ) 🔵 BAJO
Severidad confirmada (post-evaluación)	( ) 🔴 CRÍTICO ( ) 🟠 ALTO ( ) 🟡 MEDIO ( ) 🔵 BAJO
SECCIÓN 2 — DESCRIPCIÓN DEL INCIDENTE	
¿Qué ocurrió? (descripción detallada)	
Sistemas o datos afectados	
[Listar: sistemas, carpetas, bases de datos, equipos]	
¿Datos de clientes afectados? Indicar qué clientes y qué datos	
( ) No ( ) Sí — especificar:	
¿Sigue activo el incidente al momento del reporte?	

( ) No, ya se detuvo ( ) Sí, todavía en curso — describir:	
SECCIÓN 3 — LÍNEA DE TIEMPO DE LA RESPUESTA	
Detección del incidente	**[DD/MM/AAAA HH:MM — por quién]**
Notificación al Resp. de Seguridad	**[DD/MM/AAAA HH:MM]**
Notificación al Coordinador (BCP)	**[DD/MM/AAAA HH:MM]**
Inicio de la contención	**[DD/MM/AAAA HH:MM — primera acción tomada]**
Incidente contenido (propagación detenida)	**[DD/MM/AAAA HH:MM]**
Inicio de la recuperación (si aplica)	**[DD/MM/AAAA HH:MM]**
Sistemas restaurados / operativos	**[DD/MM/AAAA HH:MM]**
Cierre formal del incidente	**[DD/MM/AAAA HH:MM]**
TIEMPO TOTAL DE INACTIVIDAD	**[X horas Y minutos]**
RTO planificado (del DRP)	**[X horas — ver Documento 14]**
¿Se cumplió el RTO?	( ) Sí ( ) No — motivo:
SECCIÓN 4 — ACCIONES DE RESPUESTA TOMADAS	
Acciones de contención ejecutadas	
Acciones de erradicación ejecutadas	
Acciones de recuperación ejecutadas	
¿Se activó el BCP (Doc. 13)?	( ) Sí ( ) No ( ) Parcialmente

¿Se activó el DRP (Doc. 14)?	( ) Sí ( ) No ( ) Parcialmente
¿Se usó el Protocolo de Incidentes (Doc. 15)?	( ) Sí — Playbook #_____ ( ) No ( ) Proceso ad hoc
SECCIÓN 5 — COMUNICACIONES REALIZADAS	
¿Se notificó a clientes afectados?	( ) No aplica ( ) Sí — Fecha: _____ ( ) No — motivo: _____
¿Se notificó a la AAIP (brecha LPDP)?	( ) No aplica ( ) Sí — Fecha y nro de caso: _____ ( ) No — motivo: _____
¿Se reportó al CERT.ar?	( ) No aplica ( ) Sí — Fecha: _____ ( ) No
¿Se notificó a la compañía de seguros?	( ) No aplica ( ) Sí — Fecha y nro de caso: _____ ( ) No
¿Intervino el asesor legal?	( ) Sí ( ) No
Comunicaciones adicionales relevantes	
SECCIÓN 6 — CAUSA RAÍZ Y LECCIONES APRENDIDAS	
¿Se identificó la causa raíz?	( ) Sí ( ) No — pendiente de investigación
Causa raíz del incidente	
[Describir: ¿qué falló? ¿vulnerabilidad técnica, error humano, proceso inadecuado?]	
Vector de ataque / cómo ocurrió	
[Describir: phishing, vulnerabilidad de software, acceso físico, etc.]	
¿Qué funcionó bien en la respuesta?	
¿Qué puede mejorarse en la respuesta?	

Medidas preventivas implementadas para evitar recurrencia

SECCIÓN 7 — CIERRE Y APROBACIÓN	
Estado del incidente	( ) Abierto ( ) En investigación ( ) Cerrado
Fecha de cierre formal	**[DD/MM/AAAA]**
¿Se actualizó el DRP o BCP?	( ) Sí ( ) No aplica ( ) Pendiente
¿Se actualizó el Protocolo de Incidentes?	( ) Sí ( ) No aplica ( ) Pendiente
¿Se realizó reunión de lecciones aprendidas?	( ) Sí — Fecha: _____ ( ) No — motivo: _____
Documentado por	**[Nombre, cargo y fecha]**
Revisado y aprobado por	**[Nombre del socio aprobante y fecha]**

FICHA DE INCIDENTE — ID: INC-002

SECCIÓN 1 — DATOS BÁSICOS DEL INCIDENTE

ID del incidente	**INC-002**
Fecha y hora de detección	**[DD/MM/AAAA — HH:MM]**
Fecha y hora de reporte al Resp. Seguridad	**[DD/MM/AAAA — HH:MM]**
Reportado por	**[Nombre y cargo de quien detectó y reportó]**
Tipo de incidente	( ) Ransomware ( ) Phishing ( ) Malware ( ) Acceso no autorizado( ) Pérdida de dispositivo ( ) Error humano ( ) Brecha de datos ( ) Otro:
Severidad inicial	( ) 🔴 CRÍTICO ( ) 🟠 ALTO ( ) 🟡 MEDIO ( ) 🔵 BAJO
Severidad confirmada (post-evaluación)	( ) 🔴 CRÍTICO ( ) 🟠 ALTO ( ) 🟡 MEDIO ( ) 🔵 BAJO

SECCIÓN 2 — DESCRIPCIÓN DEL INCIDENTE

¿Qué ocurrió? (descripción detallada)

Sistemas o datos afectados

[Listar: sistemas, carpetas, bases de datos, equipos]

¿Datos de clientes afectados? Indicar qué clientes y qué datos

( ) No ( ) Sí — especificar:

¿Sigue activo el incidente al momento del reporte?

( ) No, ya se detuvo ( ) Sí, todavía en curso — describir:

SECCIÓN 3 — LÍNEA DE TIEMPO DE LA RESPUESTA

Detección del incidente	**[DD/MM/AAAA HH:MM — por quién]**
Notificación al Resp. de Seguridad	**[DD/MM/AAAA HH:MM]**
Notificación al Coordinador (BCP)	**[DD/MM/AAAA HH:MM]**
Inicio de la contención	**[DD/MM/AAAA HH:MM — primera acción tomada]**
Incidente contenido (propagación detenida)	**[DD/MM/AAAA HH:MM]**
Inicio de la recuperación (si aplica)	**[DD/MM/AAAA HH:MM]**
Sistemas restaurados / operativos	**[DD/MM/AAAA HH:MM]**
Cierre formal del incidente	**[DD/MM/AAAA HH:MM]**
TIEMPO TOTAL DE INACTIVIDAD	**[X horas Y minutos]**
RTO planificado (del DRP)	**[X horas — ver Documento 14]**
¿Se cumplió el RTO?	( ) Sí ( ) No — motivo:
SECCIÓN 4 — ACCIONES DE RESPUESTA TOMADAS	
Acciones de contención ejecutadas	
Acciones de erradicación ejecutadas	
Acciones de recuperación ejecutadas	
¿Se activó el BCP (Doc. 13)?	( ) Sí ( ) No ( ) Parcialmente
¿Se activó el DRP (Doc. 14)?	( ) Sí ( ) No ( ) Parcialmente
¿Se usó el Protocolo de Incidentes (Doc. 15)?	( ) Sí — Playbook #_____ ( ) No ( ) Proceso ad hoc
SECCIÓN 5 — COMUNICACIONES REALIZADAS	

¿Se notificó a clientes afectados?	( ) No aplica ( ) Sí — Fecha: _____ ( ) No — motivo: _____
¿Se notificó a la AAIP (brecha LPDP)?	( ) No aplica ( ) Sí — Fecha y nro de caso: _____ ( ) No — motivo: _____
¿Se reportó al CERT.ar?	( ) No aplica ( ) Sí — Fecha: _____ ( ) No
¿Se notificó a la compañía de seguros?	( ) No aplica ( ) Sí — Fecha y nro de caso: _____ ( ) No
¿Intervino el asesor legal?	( ) Sí ( ) No

Comunicaciones adicionales relevantes

SECCIÓN 6 — CAUSA RAÍZ Y LECCIONES APRENDIDAS

¿Se identificó la causa raíz?	( ) Sí ( ) No — pendiente de investigación

Causa raíz del incidente

[Describir: ¿qué falló? ¿vulnerabilidad técnica, error humano, proceso inadecuado?]

Vector de ataque / cómo ocurrió

[Describir: phishing, vulnerabilidad de software, acceso físico, etc.]

¿Qué funcionó bien en la respuesta?

¿Qué puede mejorarse en la respuesta?

Medidas preventivas implementadas para evitar recurrencia

SECCIÓN 7 — CIERRE Y APROBACIÓN

Estado del incidente	( ) Abierto ( ) En investigación ( ) Cerrado
Fecha de cierre formal	**[DD/MM/AAAA]**
¿Se actualizó el DRP o BCP?	( ) Sí ( ) No aplica ( ) Pendiente
¿Se actualizó el Protocolo de Incidentes?	( ) Sí ( ) No aplica ( ) Pendiente
¿Se realizó reunión de lecciones aprendidas?	( ) Sí — Fecha: _____ ( ) No — motivo: _____
Documentado por	**[Nombre, cargo y fecha]**
Revisado y aprobado por	**[Nombre del socio aprobante y fecha]**

FICHA DE INCIDENTE — ID: INC-003

SECCIÓN 1 — DATOS BÁSICOS DEL INCIDENTE

ID del incidente	**INC-003**
Fecha y hora de detección	**[DD/MM/AAAA — HH:MM]**
Fecha y hora de reporte al Resp. Seguridad	**[DD/MM/AAAA — HH:MM]**
Reportado por	**[Nombre y cargo de quien detectó y reportó]**
Tipo de incidente	( ) Ransomware ( ) Phishing ( ) Malware ( ) Acceso no autorizado( ) Pérdida de dispositivo ( ) Error humano ( ) Brecha de datos ( ) Otro:
Severidad inicial	( ) 🔴 CRÍTICO ( ) 🟠 ALTO ( ) 🟡 MEDIO ( ) 🔵 BAJO
Severidad confirmada (post-evaluación)	( ) 🔴 CRÍTICO ( ) 🟠 ALTO ( ) 🟡 MEDIO ( ) 🔵 BAJO

SECCIÓN 2 — DESCRIPCIÓN DEL INCIDENTE

¿Qué ocurrió? (descripción detallada)

Sistemas o datos afectados

[Listar: sistemas, carpetas, bases de datos, equipos]

¿Datos de clientes afectados? Indicar qué clientes y qué datos

( ) No ( ) Sí — especificar:

¿Sigue activo el incidente al momento del reporte?

( ) No, ya se detuvo ( ) Sí, todavía en curso — describir:

SECCIÓN 3 — LÍNEA DE TIEMPO DE LA RESPUESTA

Detección del incidente	**[DD/MM/AAAA HH:MM — por quién]**
Notificación al Resp. de Seguridad	**[DD/MM/AAAA HH:MM]**
Notificación al Coordinador (BCP)	**[DD/MM/AAAA HH:MM]**
Inicio de la contención	**[DD/MM/AAAA HH:MM — primera acción tomada]**
Incidente contenido (propagación detenida)	**[DD/MM/AAAA HH:MM]**
Inicio de la recuperación (si aplica)	**[DD/MM/AAAA HH:MM]**
Sistemas restaurados / operativos	**[DD/MM/AAAA HH:MM]**
Cierre formal del incidente	**[DD/MM/AAAA HH:MM]**
TIEMPO TOTAL DE INACTIVIDAD	**[X horas Y minutos]**
RTO planificado (del DRP)	**[X horas — ver Documento 14]**
¿Se cumplió el RTO?	( ) Sí ( ) No — motivo:
SECCIÓN 4 — ACCIONES DE RESPUESTA TOMADAS	
Acciones de contención ejecutadas	
Acciones de erradicación ejecutadas	
Acciones de recuperación ejecutadas	
¿Se activó el BCP (Doc. 13)?	( ) Sí ( ) No ( ) Parcialmente
¿Se activó el DRP (Doc. 14)?	( ) Sí ( ) No ( ) Parcialmente
¿Se usó el Protocolo de Incidentes (Doc. 15)?	( ) Sí — Playbook #_____ ( ) No ( ) Proceso ad hoc
SECCIÓN 5 — COMUNICACIONES REALIZADAS	

¿Se notificó a clientes afectados?	( ) No aplica ( ) Sí — Fecha: _____ ( ) No — motivo: _____
¿Se notificó a la AAIP (brecha LPDP)?	( ) No aplica ( ) Sí — Fecha y nro de caso: _____ ( ) No — motivo: _____
¿Se reportó al CERT.ar?	( ) No aplica ( ) Sí — Fecha: _____ ( ) No
¿Se notificó a la compañía de seguros?	( ) No aplica ( ) Sí — Fecha y nro de caso: _____ ( ) No
¿Intervino el asesor legal?	( ) Sí ( ) No

Comunicaciones adicionales relevantes

SECCIÓN 6 — CAUSA RAÍZ Y LECCIONES APRENDIDAS

¿Se identificó la causa raíz?	( ) Sí ( ) No — pendiente de investigación

Causa raíz del incidente

[Describir: ¿qué falló? ¿vulnerabilidad técnica, error humano, proceso inadecuado?]

Vector de ataque / cómo ocurrió

[Describir: phishing, vulnerabilidad de software, acceso físico, etc.]

¿Qué funcionó bien en la respuesta?

¿Qué puede mejorarse en la respuesta?

Medidas preventivas implementadas para evitar recurrencia

SECCIÓN 7 — CIERRE Y APROBACIÓN

Estado del incidente	( ) Abierto ( ) En investigación ( ) Cerrado
Fecha de cierre formal	**[DD/MM/AAAA]**
¿Se actualizó el DRP o BCP?	( ) Sí ( ) No aplica ( ) Pendiente
¿Se actualizó el Protocolo de Incidentes?	( ) Sí ( ) No aplica ( ) Pendiente
¿Se realizó reunión de lecciones aprendidas?	( ) Sí — Fecha: _____ ( ) No — motivo: _____
Documentado por	**[Nombre, cargo y fecha]**
Revisado y aprobado por	**[Nombre del socio aprobante y fecha]**

7. Análisis Anual de Incidentes

Al finalizar cada año, el Responsable de Seguridad completa el análisis anual de incidentes. Este análisis se presenta a la dirección y se usa para ajustar el programa de seguridad del año siguiente.

Período analizado	**[Año AAAA]**
Fecha del análisis	**[DD/MM/AAAA]**
Elaborado por	**[Nombre y cargo del Responsable de Seguridad]**
Aprobado por	**[Nombre del socio]**

7.1 Estadísticas del año

Métrica anual	Año anterior	Año actual	Tendencia / Análisis
Total de incidentes registrados			
Incidentes críticos			
Incidentes altos			
Incidentes medios / bajos			
Incidentes con causa humana			
Incidentes causados por proveedores			
Incidentes con brecha de datos de clientes			
Tiempo promedio de detección (MTTD)			
Tiempo promedio de respuesta (MTTI)			
Tiempo promedio de recuperación (MTTR)			
% incidentes con causa raíz identificada			
% incidentes cerrados sin datos de clientes afectados			

7.2 Análisis de causas raíz

¿Cuáles fueron las causas raíz más frecuentes de los incidentes del año?

Causa raíz	Frecuencia	Medidas tomadas para prevenir recurrencia
Error humano (phishing, envío incorrecto, contraseña débil)		
Vulnerabilidad de software sin parchear		
Acceso indebido (interno o de proveedor)		
Fallo tecnológico (hardware, backup)		
Otras causas		

7.3 Conclusiones y recomendaciones para el año siguiente

Principal aprendizaje del año:

[Describir el hallazgo más importante del análisis anual de incidentes]

Ajustes al programa de seguridad para el año siguiente:

[Listar los cambios de política, proceso o tecnología a implementar]

Presupuesto adicional de seguridad identificado:

[Indicar inversiones necesarias para el próximo año]

8. Revisión del Documento

Este documento es un registro permanente y se actualiza continuamente ante cada nuevo incidente. La estructura (secciones de política y criterios de clasificación) se revisa anualmente.

Próxima revisión de la estructura: [DD/MM/AAAA] | Responsable: [Nombre y cargo]

— Fin del Documento —