PLAN DE RECUPERACIÓN ANTE DESASTRES

Disaster Recovery Plan (DRP)

Procedimientos técnicos de restauración de sistemas

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: anual y ante cambios técnicos]**
Responsable técnico (DRP)	**[Nombre y cargo — Responsable de Seguridad o TI]**
Aprobado por	**[Nombre y cargo del socio/director que aprueba]**

🔒 DOCUMENTO DE USO TÉCNICO RESTRINGIDO: Este plan contiene información técnica detallada sobre los sistemas del Estudio. Acceso solo para el Responsable de Seguridad, los socios y el proveedor de soporte TI designado. Guardar una copia impresa junto al BCP (Documento 13) fuera de la oficina.

CONFIDENCIAL — DISTRIBUCIÓN RESTRINGIDA AL PERSONAL TÉCNICO AUTORIZADO

1. DRP vs BCP — Diferencia Clave

BCP — Documento 13	DRP — Este documento
Plan OPERATIVO: cómo seguimos funcionando como negocio durante el incidente. Audiencia: socios, gerentes, todo el personal. Foco: clientes, comunicación, vencimientos, personal. **Pregunta que responde: ¿Cómo seguimos atendiendo a clientes?**	Plan TÉCNICO: cómo restauramos los sistemas de IT después del incidente. Audiencia: Responsable de Seguridad, técnico TI, socios con rol técnico. Foco: sistemas, datos, hardware, red, software. **Pregunta que responde: ¿Cómo levantamos los sistemas?**

En la práctica, ambos se activan en paralelo ante un incidente grave: el BCP gestiona la continuidad del negocio mientras el DRP restaura los sistemas técnicos.

2. Propósito

Este Plan de Recuperación ante Desastres (DRP) documenta los procedimientos técnicos paso a paso para restaurar los sistemas de información del Estudio después de un incidente que cause pérdida, daño o inaccesibilidad de los sistemas críticos.

A diferencia del BCP (que se enfoca en mantener la operación del negocio), el DRP se enfoca en restaurar los sistemas técnicos al estado operativo normal lo antes posible. Ambos planes se complementan y se activan en paralelo.

🔒 Este documento debe estar guardado fuera de los sistemas del Estudio. Si todos los servidores están caídos, este plan debe ser accesible en papel o en un dispositivo externo que no dependa de los sistemas internos.

3. Objetivos de Recuperación

Los siguientes objetivos definen los parámetros de recuperación del Estudio:

Métrica	Definición	Objetivo del Estudio

RTO — Recovery Time Objective	Tiempo máximo tolerable para restaurar un sistema desde que ocurre el incidente.	**[Ej: 4 horas para sistemas críticos (ERP, correo) | 24 horas para el resto]**
RPO — Recovery Point Objective	Pérdida máxima de datos tolerable, expresada en tiempo. Si el RPO es 24h, podemos perder hasta 24h de datos.	**[Ej: 24 horas (un día de datos) para datos de clientes]**
MTTR — Mean Time to Recover	Tiempo promedio real de recuperación. Se mide en los simulacros y se compara con el RTO.	**[Medir en el próximo simulacro anual]**
Nivel de servicio mínimo	El nivel funcional mínimo aceptable al reanudar operaciones (puede ser operación reducida).	70% de funcionalidad: acceso a datos de clientes + AFIP + correo. El 30% restante puede restaurarse después.

4. Inventario de Sistemas Críticos

La siguiente tabla lista todos los sistemas críticos del Estudio con sus parámetros de recuperación. Debe mantenerse actualizada ante cada cambio tecnológico.

Sistema	Proveedor / Solución	Criticidad	RTO	RPO	Procedimiento de recuperación
Software contable / ERP	**[Ej: Tango / Bejerman]**	🔴 Crítico	4 hs	24 hs	Ver Sección 7.1
Acceso a AFIP	AFIP (servicio externo)	🔴 Crítico	1 hs (si es corte del proveedor)	N/A	Ver Sección 7.2
Correo corporativo	**[Ej: Google Workspace]**	🔴 Crítico	2 hs	0 (cloud sync)	Ver Sección 7.3
Almacenamiento en nube	**[Ej: Google Drive / OneDrive]**	🟠 Alto	2 hs	0 (cloud sync)	Restaurar desde versionado del servicio
Servidor NAS local	**[Ej: Synology / QNAP]**	🟠 Alto	4-8 hs	24 hs	Ver Sección 7.4
VPN del Estudio	**[Ej: OpenVPN / WireGuard]**	🟠 Alto	2 hs	N/A (configuración)	Restaurar config desde backup cifrado
PCs y laptops	**[Windows / macOS]**	🔵 Medio	24-48 hs	24 hs	Restaurar desde imagen o reinstalar + datos de backup

Teléfonos corporativos	Android / iOS	🔵 Medio	24 hs	24 hs (backup en nube del OS)	Restaurar desde backup de Google/iCloud corporativo

ℹ RTO = Tiempo máximo para restaurar el sistema. RPO = Máxima pérdida de datos tolerable en tiempo. N/A = No aplica (sistema externo o sin datos locales).

5. Evaluación de Impacto ante Desastre

Ante un incidente, el Responsable Técnico evalúa el impacto antes de iniciar la recuperación:

#	Paso	Detalle técnico
1	**Identificar qué sistemas están afectados**	Listar todos los sistemas inoperativos o degradados. Determinar si el incidente sigue activo (ej: ransomware todavía en la red).
2	**Determinar la causa**	¿Es falla de hardware? ¿Software? ¿Ataque externo? ¿Error humano? La causa determina el procedimiento de recuperación.
3	**Estimar el alcance de los datos afectados**	¿Qué datos se perdieron o comprometieron? ¿Hasta qué fecha están los backups disponibles?
4	**Priorizar la recuperación**	Recuperar primero los sistemas con menor RTO y mayor impacto en la operación del Estudio. Ver tabla de Sección 4.
5	**Notificar al BCP**	Informar al Coordinador del BCP (Documento 13) del alcance técnico para que active los protocolos operativos en paralelo.
6	**Documentar el estado inicial**	Antes de cualquier acción de recuperación, tomar capturas de pantalla o notas del estado de los sistemas afectados. Útil para forensia y seguros.

6. Procedimiento General de Recuperación

Este es el flujo general de recuperación para cualquier desastre tecnológico. Los procedimientos específicos por sistema están en la Sección 7.

Fase	Nombre	Actividades
FASE 1 (0-1 hs)	**Contención y evaluación**	Detener la propagación del daño. Aislar sistemas afectados. Evaluar el alcance. No restaurar nada hasta tener claro el alcance completo.
FASE 2 (1-4 hs)	**Preparación del entorno de recuperación**	Preparar equipos de reemplazo o entorno limpio. Verificar integridad de los backups. Identificar el

		backup adecuado para restaurar. Limpiar sistemas afectados de malware si corresponde.
FASE 3 (4-24 hs)	**Restauración de sistemas críticos**	Restaurar primero los sistemas con RTO más corto: ERP/software contable, acceso a AFIP, correo corporativo. Verificar integridad post-restauración.
FASE 4 (24-72 hs)	**Restauración de sistemas secundarios**	Restaurar NAS local, VPN, sistemas de gestión documental. Verificar la consistencia de todos los datos restaurados.
FASE 5 (72 hs+)	**Normalización y revisión**	Verificar funcionamiento completo de todos los sistemas. Documentar el incidente. Implementar mejoras preventivas. Actualizar el DRP con lecciones aprendidas.

7. Procedimientos de Recuperación por Sistema

⚠ Antes de iniciar cualquier restauración: verificar que el sistema receptor (equipo o entorno donde se va a restaurar) esté LIMPIO y libre de malware. Restaurar sobre un sistema comprometido invalida la recuperación.

7.1 Software Contable / ERP

#	Paso	Detalle técnico
1	**Preparar el equipo de restauración**	Verificar que el equipo receptor tiene el sistema operativo limpio y actualizado. Si el equipo original fue comprometido por ransomware, formatearlo antes de proceder.
2	**Instalar el software contable**	Descargar el instalador del proveedor. Versión:
3	**Identificar y acceder al backup de la base de datos**	Ubicación del backup: [Indicar ruta exacta en la nube o disco externo]. Verificar que el backup no esté cifrado por ransomware (comparar hash o fecha de modificación).
4	**Restaurar la base de datos**	Ejecutar el proceso de restauración del software contable. Verificar que el proceso complete sin errores.
5	**Verificar la integridad de los datos**	Abrir el sistema y verificar: últimas facturas emitidas, últimas liquidaciones procesadas, que los datos correspondan al período esperado del backup.
6	**Configurar accesos de usuarios**	Verificar que todos los usuarios tienen sus accesos configurados correctamente. Si la base de usuarios también fue comprometida, restaurar desde backup de configuraciones.

7	**Verificar integración con AFIP**	Probar la emisión de facturas electrónicas y la comunicación con los servicios de AFIP antes de dar el sistema como recuperado.

Proveedor del software	**[Nombre y teléfono de soporte técnico]**
Instalador disponible en	**[URL de descarga o ubicación en backup]**
Número de licencia	**[Guardar en gestor de contraseñas — no aquí]**
Tiempo estimado de restauración	**[Completar después del primer simulacro]**

7.2 Acceso a AFIP

AFIP es un servicio externo. Los escenarios posibles son:

- Caída del servicio de AFIP (problema del organismo): verificar en el sitio oficial de AFIP o en redes sociales. Si es problema de AFIP, no hay acción técnica posible: informar a los clientes y esperar. AFIP generalmente extiende plazos en casos de caída masiva del sistema.
- Pérdida de credenciales de acceso (clave fiscal del Estudio): recuperar mediante el proceso de recuperación de clave fiscal de AFIP con CUIT y datos del representante legal del Estudio.
- Pérdida de acceso a claves fiscales de clientes almacenadas localmente: restaurar desde el gestor de contraseñas (backup en nube).

Contacto mesa de ayuda AFIP: 0800-999-2347 | Web de recuperación: www.afip.gob.ar

7.3 Correo Electrónico Corporativo

Los sistemas de correo corporativo en la nube (Google Workspace, Microsoft 365) tienen alta disponibilidad y sus datos son gestionados por el proveedor. Los escenarios y acciones son:

Escenario	Acción de recuperación
Caída del proveedor (Google/Microsoft)	Verificar en status.google.com o status.office.com. Si es incidente del proveedor, esperar. No hay acción técnica local.
Pérdida de contraseña de cuenta de correo	Usar el proceso de recuperación del proveedor. Si el MFA también se perdió, contactar soporte del proveedor con prueba de identidad.
Correos eliminados accidentalmente	Restaurar desde la papelera del servicio (disponible según política de retención del proveedor — generalmente 30 días). Para

	períodos mayores, usar Google Vault o Microsoft 365 Archive si están activos.
Cuenta de correo comprometida (acceso no autorizado)	Cambiar contraseña inmediatamente. Revocar todos los accesos activos en la configuración de seguridad de la cuenta. Revisar reglas de reenvío y firmas modificadas por el atacante.

Proveedor de correo corporativo: [Google Workspace / Microsoft 365 / otro] | Panel de administración: [URL del panel admin]

7.4 Servidor NAS Local

#	Paso	Detalle técnico
1	**Evaluar el tipo de falla**	¿Es falla de un disco del RAID? ¿Falla del NAS completo? ¿Corrupción de datos? La acción es diferente para cada caso.
2	**Falla de disco en RAID**	Si el NAS tiene RAID y un disco falla: reemplazar el disco defectuoso. El NAS reconstruirá el RAID automáticamente (puede tardar horas según el tamaño). Durante la reconstrucción, los datos siguen accesibles pero con menor rendimiento.
3	**Falla total del NAS**	Si el NAS completo falló y los discos están íntegros: intentar montar los discos en otro NAS del mismo fabricante. Si los discos también fallaron: restaurar desde el backup en nube (backup off-site de la Regla 3-2-1).
4	**Restaurar desde backup en nube**	Acceder al servicio de backup en nube con las credenciales del gestor de contraseñas. Descargar los datos al nuevo NAS o equipo de reemplazo. Verificar la integridad de los datos restaurados.
5	**Reconectar usuarios y aplicaciones**	Actualizar las rutas de red en los equipos del Estudio para que apunten al NAS restaurado. Verificar que los accesos de cada usuario funcionen correctamente.

Modelo del NAS	**[Marca, modelo y número de serie]**
Configuración de RAID	**[RAID 1 / RAID 5 / RAID 6 / sin RAID]**
Discos instalados	**[Cantidad, tamaño y modelo de cada disco]**
Panel de administración NAS	**[IP local del NAS: ej. 192.168.1.100:5000]**
Manual de recuperación del fabricante	**[URL de documentación del fabricante]**

7.5 Procedimiento Específico ante Ransomware

🚨 El ransomware requiere un procedimiento diferente al de otras fallas. La velocidad de contención en los primeros minutos determina cuántos sistemas son cifrados. Seguir este procedimiento en estricto orden.

#	Paso	Detalle técnico
1	**CONTENER — Desconectar de la red INMEDIATAMENTE**	Desconectar el cable de red de TODOS los equipos que parezcan afectados. Desactivar el Wi-Fi en esos equipos. Si no se puede identificar cuáles están afectados, desconectar el router del Estudio. La velocidad de esta acción determina cuántos sistemas se cifran.
2	**NO apagar los equipos afectados**	Apagar un equipo con ransomware puede eliminar información en memoria RAM que es útil para identificar el tipo de ransomware y potencialmente recuperar la clave de cifrado. Dejar encendido pero desconectado de la red.
3	**Identificar el tipo de ransomware**	Buscar en ID Ransomware (www.id-ransomware.malwarehunterteam.com) el tipo de ransomware cargando un archivo cifrado o la nota de rescate. Algunos ransomwares tienen descifradoras gratuitas disponibles.
4	**NO pagar el rescate**	El pago no garantiza la recuperación. Solo un 50% de quienes pagan recuperan todos los datos. El pago financia futuros ataques y puede tener implicancias legales.
5	**Preparar equipos de reemplazo LIMPIOS**	Usar equipos nuevos o formateados completamente. NO reutilizar equipos potencialmente infectados sin formatearlos.
6	**Verificar el backup pre-infección**	Identificar el backup más reciente anterior al momento de infección. Verificar que ese backup NO fue cifrado por el ransomware (muchos ransomwares atacan también los backups conectados a la red).
7	**Restaurar desde backup off-site**	El backup en nube (off-site de la Regla 3-2-1) debería estar intacto si estaba desconectado de la red local cuando ocurrió el ataque. Restaurar en los equipos limpios.
8	**Reconfigurar la red de forma segura**	Cambiar todas las contraseñas de la red. Actualizar firmware del router. Verificar que no hay puertas traseras instaladas por el atacante antes de reconectar a internet.
9	**Reportar a las autoridades**	Reportar el incidente al CERT.ar (Coordinación de Emergencias en Redes Teleinformáticas — www.cert.ar). Si hay datos de clientes comprometidos, notificar a la AAIP.

7.6 Falla de Hardware (PC / Laptop)

- Si es falla de disco duro: datos en riesgo. Si el disco no está cifrado con BitLocker/FileVault, intentar recuperar datos antes de reemplazar el disco.
- Si es falla de otro componente (placa madre, memoria): el disco puede estar íntegro. Extraerlo y montarlo como disco externo en otro equipo para recuperar datos.

- Configurar el equipo de reemplazo con el mismo software y accesos, usando el backup de configuraciones y los instaladores almacenados en el backup.
- Si el equipo era la única copia de datos no respaldados: contactar un servicio de recuperación de datos antes de descartarlo.

Servicio de recuperación de datos de confianza: [Empresa, teléfono y referencia — evaluar antes de necesitarlo]

8. Recuperación de Datos Específicos

Además de los sistemas completos, pueden ocurrir pérdidas de datos específicos que no requieren recuperación completa del sistema:

Tipo de pérdida	Acción de recuperación
Archivo eliminado accidentalmente (en nube)	Restaurar desde la papelera de reciclaje del servicio de nube. Si fue vaciada, verificar si el versionado del servicio permite recuperar versiones anteriores.
Archivo eliminado en PC local	Verificar la Papelera de Reciclaje local. Si fue vaciada, usar el backup de PCs (si está configurado). Como último recurso, usar herramientas de recuperación de archivos (Recuva, PhotoRec).
Base de datos contable corrompida (sin ransomware)	Restaurar la última versión íntegra del backup de la base de datos. Si el software contable tiene función de reparación de base de datos, probarla primero.
Correos eliminados	Verificar papelera del cliente de correo. Luego verificar papelera del servidor (en el panel de Google/Microsoft). Para correos eliminados hace más de 30 días, verificar si hay archivo activo (Google Vault / Microsoft Archive).
Historial de transacciones contables faltante	Si los datos están en backup pero el rango de fechas faltante no está cubierto: reconstruir desde comprobantes físicos o digitales. Documentar el proceso para la auditoría.

9. Actividades Post-Recuperación

Una vez restaurados los sistemas, las siguientes actividades son obligatorias antes de declarar la recuperación completa:

- **Verificar la integridad de los datos de cada cliente activo en los sistemas restaurados.**
- **Confirmar que los últimos backups ejecutados desde la restauración son exitosos.**

- **Cambiar todas las contraseñas de los sistemas afectados, aunque no haya evidencia de compromiso.**
- Documentar el incidente en el Registro de Incidentes (Documento 20) con todos los detalles técnicos.
- Actualizar este DRP con las lecciones aprendidas, los tiempos reales de recuperación y las mejoras identificadas.
- Informar al Coordinador del BCP que los sistemas están normalizados para que active la comunicación de normalización con clientes.
- Evaluar si el incidente requiere notificación a la AAIP conforme a la LPDP (Documento 04).
- Revisar la causa raíz e implementar medidas preventivas para evitar que el mismo incidente se repita.

🔍 La causa raíz es más importante que la recuperación. Sin entender qué causó el incidente y cómo prevenirlo, el mismo escenario puede repetirse.

10. Herramientas de Recuperación

El Responsable Técnico debe conocer y tener acceso a las siguientes herramientas antes de que ocurra un incidente:

Herramienta	Uso	Dónde obtenerla / cómo acceder
ID Ransomware	Identificar el tipo de ransomware	*id-ransomware.malwarehunterteam.com (web gratuita)*
No More Ransom Project	Descifradoras gratuitas para algunos ransomwares	*www.nomoreransom.org (proyecto internacional)*
Recuva (Windows)	Recuperar archivos eliminados en Windows	*www.piriform.com/recuva (gratuito)*
PhotoRec / TestDisk	Recuperación avanzada de archivos y particiones	*www.cgsecurity.org (código abierto, gratuito)*
CERT.ar	Reportar incidentes de seguridad en Argentina	*www.cert.ar — ar-cert@cert.ar*
Have I Been Pwned	Verificar si credenciales	*haveibeenpwned.com (gratuito)*

	fueron comprometidas	
Malwarebytes (escáner)	Limpiar malware de equipos antes de restaurar	*www.malwarebytes.com (versión gratuita disponible)*

11. Prueba Anual del DRP

El DRP se prueba una vez al año mediante un simulacro completo coordinado con el BCP. El simulacro verifica que los procedimientos son ejecutables en los tiempos definidos y que el equipo técnico está familiarizado con ellos.

El simulacro incluye:

- Restauración completa del sistema más crítico (ERP) desde backup en un entorno de prueba aislado.
- Medición del tiempo real de restauración vs. el RTO objetivo.
- Verificación de que todos los contactos del Árbol de Llamadas están actualizados.
- Documentación de los hallazgos y actualización del DRP.

Fecha del último simulacro: [DD/MM/AAAA] | Tiempo de restauración medido: [X horas Y minutos] | ¿RTO cumplido?: [Sí / No — si No, registrar las mejoras implementadas]

Próximo simulacro: [DD/MM/AAAA] | Responsable: [Nombre y cargo]

12. Revisión y Actualización

Este DRP se revisa anualmente y ante cualquiera de los siguientes eventos:

- Cambio de software contable o ERP.
- Cambio de proveedor de backup o de nube.
- Cambio en la infraestructura de red o hardware del Estudio.
- Después de cualquier incidente real de recuperación.
- Después del simulacro anual.

Anexo A — Ficha de Recuperación Rápida (Para Imprimir)

Esta ficha resume los primeros pasos ante los incidentes más frecuentes. Imprimir y guardar junto al BCP fuera de la oficina.

🔧 FICHA DE RECUPERACIÓN RÁPIDA — DRP

🚨 RANSOMWARE:

1. DESCONECTAR de la red (cable + WiFi) TODOS los equipos afectados
2. NO apagar los equipos — NO pagar el rescate
3. Llamar al Responsable de Seguridad
4. Identificar tipo en: id-ransomware.malwarehunterteam.com
5. Restaurar desde backup en NUBE en equipos LIMPIOS (formateados)

💾 FALLA DE SERVIDOR / NAS:

1. Verificar si los datos están en la NUBE (Drive/OneDrive corporativo)
2. Si no: acceder al backup en nube (Backblaze/S3/otro)
3. Restaurar en equipo alternativo
4. Llamar al soporte TI: undefined

📧 CORREO / SISTEMA EN NUBE CAÍDO:

1. Verificar status.google.com o status.office.com
2. Si es problema del proveedor: esperar y notificar a clientes
3. Si es problema de credenciales: recuperar contraseña desde el gestor

CONTACTOS DE EMERGENCIA:

Resp. Seguridad: undefined | Soporte TI: undefined
Backup en nube (acceder desde cualquier equipo): undefined

Anexo B — Registro de Incidentes Técnicos de Recuperación

Completar ante cada incidente técnico que requiera activar el DRP. Este registro se usa para mejorar el plan con lecciones aprendidas.

REGISTRO DE INCIDENTE TÉCNICO — DRP

Fecha y hora de detección del incidente: [Completar]

Tipo de incidente (ransomware / falla de hardware / corrupción de datos / otro): [Completar]

Sistemas afectados: [Completar]

Causa identificada: [Completar]

Fecha y hora de inicio de la recuperación: [Completar]

Procedimiento ejecutado (número de sección del DRP): [Completar]

Backup utilizado (fecha del backup restaurado): [Completar]

Fecha y hora de recuperación completa: [Completar]

Tiempo total de recuperación (RTO real vs. objetivo): [Completar]

Datos perdidos definitivamente (si los hay): [Completar]

Causa raíz confirmada: [Completar]

Mejoras implementadas para evitar recurrencia: [Completar]

¿Requirió notificación a AAIP? (Sí / No — justificar): [Completar]

— Fin del Documento —