

ESTRATEGIA DIGITAL • EXECUTIVE BRIEFING

CRISIS COMMAND PACK

Protocolo estructurado de contención en 60 minutos ante fallas operacionales críticas, alucinaciones de IA y amenazas reputacionales de Directorio.

REGLA FUNDAMENTAL DE LA HORA CERO:

En incidentes de tecnología y fallas de IA, el desenlace no se define en la conferencia de prensa del día siguiente, sino en las decisiones tomadas durante los primeros 60 minutos. Congelar la hemorragia de datos, aislar canales comprometidos y preservar evidencia forense para proteger la responsabilidad fiduciaria del Directorio.

AUTOR PRINCIPAL

Gustavo Papasergio

Socio Director | Estrategia Digital

AUDIENCIA OBJETIVO

Directorio, CEO, CISO & Legal

Comités de Crisis Corporativos

MARCO DE APLICACIÓN

Edición Anual 2026

Cumplimiento SLA, D&O y PII

El Protocolo de los Primeros 60 Minutos

Secuencia estricta cronometrada de respuesta inmediata. Diseñada para aislar el daño técnico y reputacional antes de que escale al escrutinio público o litigios regulatorios.

Fase 1: Aislamiento Técnico y Preservación de Telemetría

MINUTO 00 A 15

El impulso reactivo suele ser apagar servidores o borrar publicaciones; esto destruye la evidencia necesaria para defensa jurídica, aseguradoras de Cyber y auditoría forense.

- **Desconexión segura de agentes autónomos:** Desviar tráfico de bots y modelos a respuestas estáticas de mantenimiento preventivo.
- **Congelamiento forense de logs y prompts:** Preservar registros transaccionales, prompts e IPs de inferencia antes de aplicar parches.
- **Rotación de credenciales:** Revocar tokens y accesos a modelos fundacionales ante sospecha de exfiltración.

Fase 2: Convocatoria del Comité y Supresión de Ruido

MINUTO 15 A 30

El comité debe restringirse a tomadores de decisión reales (CEO, Legal, CISO, PR). Eliminar cualquier interacción pública no supervisada.

- **Suspensión de automatizaciones:** Silenciar campañas de anuncios, emails masivos y posts programados en redes sociales.
- **Vocería única institucional:** Prohibición explícita a empleados y mandos medios de opinar en LinkedIn o foros técnicos.
- **Perímetro del incidente:** Determinar técnicamente si existió compromiso de PII/contraseñas o solo denegación de servicio.

Fase 3: Evaluación de Riesgo Legal, Regulatorio y SLA

MINUTO 30 A 45

Calcular el reloj de cumplimiento normativo y activar las defensas contractuales frente a clientes estratégicos.

- **Plazos de notificación mandatoria:** Verificar si el incidente exige aviso formal en 24h a 72h ante reguladores de datos o sectoriales.
- **Impacto en SLAs de cuentas Tier 1:** Identificar penalidades contractuales activas con clientes de alto valor de vida (LTV).
- **Notificación a pólizas Cyber y D&O:** Alertar al broker de seguros de forma oportuna para no anular la cobertura directiva.

Fase 4: Comunicación Controlada y Protección del LTV

MINUTO 45 A 60

Emitir postura oficial comprobada y contener las relaciones estratégicas prioritarias de la compañía.

- **Principio de certeza técnica:** Declarar exclusivamente hechos comprobados; nunca comprometer horarios de restablecimiento no certeros.
- **Llamada 1 a 1 con Top 20 Clientes:** Contacto personal del CEO/Directorio antes de que los trascendidos alcancen la prensa.
- **Escucha digital de señales débiles:** Medir velocidad de propagación para detectar menciones de abogados litigantes o periodistas.



PRINCIPIOS FIDUCIARIOS DE DIRECTORIO EN LA HORA CERO

1. No Destruir Evidencia

La premura por corregir el bot o apagar el cluster suele purgar la telemetría que exige la aseguradora de Cyber para liberar pagos de indemnización.

2. Blindaje Contractual Tier 1

La llamada personal y confidencial del CEO retiene contratos millonarios con mucha mayor eficacia que un frío comunicado corporativo masivo.

3. Responsabilidad Personal D&O

La omisión en la notificación formal de brechas en plazos legales expone a los directores a demandas de responsabilidad civil y penal personal.

Triage Forense de Falla de IA & Matriz RACI

Mapeo visual para clasificar la severidad de incidentes en los primeros 10 minutos y asignar responsabilidades ineludibles por rol.

ÁRBOL DE DECISIÓN RÁPIDA: INCIDENTE EN MODELOS / AGENTES AUTÓNOMOS

Detección Inicial: Agente de IA emite alucinación lesiva, transacciona fuera de guardrails o se sospecha exfiltración.

¿Compromiso de PII, saldos o datos protegidos?

→ **RUTA CRÍTICA REGULATORIA:** Congelar checkpoints, activar póliza Cyber/D&O y redactar aviso obligatorio a 72h. Activar Holding Statement A y B.

¿Falla de inferencia / interrupción funcional sin fuga?

→ **RUTA OPERATIVA:** Revertir a mensaje de mantenimiento estático, parchear RAG/prompts en staging y monitorear sin emitir comunicados públicos masivos.

¿Trascendió a redes o medios masivos?

→ Vocería única del Directorio. Llamadas privadas del CEO al Top 20 de clientes antes de declaraciones en prensa.

¿Incidente confinado internamente?

→ Memorando de confidencialidad al personal. Escucha digital silenciosa sin despertar alarmas innecesarias.

MATRIZ DE RESPONSABILIDAD EN CRISIS (RACI MATRIX)

Acción Operativa Crítica	CEO	CISO / IT	Legal	PR / Comms	Negocio
Desconexión de agentes y fijación de telemetría	I	R	C	I	I
Convocatoria del Comité y supresión de publicaciones	A	C	C	R	I
Evaluación de impacto en SLAs contractuales	I	C	R	I	A
Notificación a aseguradora Cyber y D&O	A	C	R	I	I
Aprobación de Holding Statement oficial	A	C	C	R	I
Contacto 1 a 1 con 20 principales clientes	R	I	I	C	A

R: Responsable directo | A: Aprueba / Accountable | C: Consultado | I: Informado

UMBRALES DE ESCALAMIENTO INMEDIATO AL DIRECTORIO (BOARD ESCALATION CRITERIA)

Umbral Financiero & SLA

Pérdidas proyectadas superiores al 2% de la facturación mensual recurrente o riesgo inminente de penalizaciones contractuales en cuentas Tier 1.

Umbral Legal & Regulatorio

Filtración confirmada de datos personales (PII), secretos comerciales o claves criptográficas que active plazos de aviso perentorio a 72 horas.

Umbral de Escrutinio Público

Menciones del incidente por medios de comunicación de alcance nacional, analistas de industria o superación de 500 menciones orgánicas/hora en redes.

Checklist del Board & Crisis Communication Kit

Herramienta de control en mesa de crisis y 3 plantillas pre-aprobadas para neutralizar el pánico en clientes, medios y empleados.

CHECKLIST DE 10 PUNTOS PARA LA MESA DE CRISIS DEL DIRECTORIO

- | | |
|---|---|
| ☐ 01 ¿Desconectaron modelos/bots sin destruir logs? | ☐ 02 ¿Silenciaron anuncios y posts automatizados? |
| ☐ 03 ¿Hay un único vocero institucional designado? | ☐ 04 ¿Se evaluó exposición de contraseñas o PII? |
| ☐ 05 ¿Top 20 clientes recibieron contacto directo CEO? | ☐ 06 ¿Legal revisó el borrador antes de emitirlo? |
| ☐ 07 ¿Se notificó al seguro de riesgo Cyber y D&O? | ☐ 08 ¿Personal advertido de no opinar en redes? |
| ☐ 09 ¿Activada escucha digital para medir viralidad? | ☐ 10 ¿Fijada la hora del próximo informe al Board? |

CRISIS COMMUNICATION KIT (HOLDING STATEMENTS QUIRÚRGICOS)

PLANTILLA A: LLAMADA CONFIDENCIAL 1 A 1 PARA CLIENTES TIER 1 (GUIÓN DEL CEO)

"Estimado [Nombre Cliente]: Me comunico personalmente antes de cualquier trascendido público para informarte que hemos detectado una interrupción técnica preventiva en [Servicio]. Tus operaciones críticas y datos se encuentran [aislados / bajo resguardo]. Nuestro equipo forense está verificando la telemetría y te brindaré una actualización directa a las [Hora pactada]."

PLANTILLA B: DECLARACIÓN PÚBLICA DE CONTENCIÓN (PRENSA Y REDES - SIN AUTOINCRIMINACIÓN)

"[Empresa] informa que ha activado una pausa técnica programada sobre su canal [Servicio] para aplicar protocolos preventivos de telemetría y seguridad operativa. Nuestras operaciones centrales continúan con normalidad. Estaremos emitiendo la próxima actualización oficial a través de este único canal antes de las [Hora]."

PLANTILLA C: MEMORANDO INTERNO DE ESTRICTA CONFIDENCIALIDAD (COLABORADORES)

"A todo el personal: Todo colaborador debe abstenerse terminantemente de realizar comentarios, disculpas informales o conjeturas en LinkedIn, Twitter o foros externos. Cualquier contacto de prensa debe ser derivado exclusivamente al canal oficial: [voceria@empresa.com]. Toda filtración será tratada como falta grave de confidencialidad."

REGLAS QUIRÚRGICAS DE VOCERÍA PARA EL CEO & PORTAVOCES

1. Silencio Operativo en Redes

Cero declaraciones individuales o respuestas en hilos de LinkedIn/X. Las respuestas impulsivas se incorporan inmediatamente como prueba en litigios.

2. Regla de los Tres "NO"

No admitir culpabilidad antes del peritaje, no conjeturar sobre causas no verificadas y jamás prometer plazos de restablecimiento sin certeza total.

3. Canal Centralizado

Toda comunicación externa se emite a través de un único canal formal y validado previamente por el Directorio y la asesoría letrada.

Resiliencia Operativa & Tabletop Simulations

Ningún plan de contingencia sobrevive al primer contacto con la crisis real si no ha sido ensayado previamente por los tomadores de decisión.

¿Tu Directorio está preparado para la Hora Cero?

En Estrategia Digital diseñamos y facilitamos **Tabletop Simulations** confidenciales a puerta cerrada. Enfrentamos a Directorios, CEOs, CISOs y Comités de Crisis a escenarios realistas de fallo de IA, fuga de credenciales o extorsión reputacional bajo presión de tiempo real.

Simulación en Tiempo Real

Inyección de eventos dinámicos: filtraciones en X, consultas de periodistas y caídas de SLAs simuladas durante 3 horas intensivas.

Auditoría de Brechas en la Mesa

Identificación de cuellos de botella: retrasos legales, contradicciones de vocería y debilidades fiduciarias antes de que ocurra la crisis.

Gobernanza y Protocolos HITL

Definición de matrices de riesgo operacional para limitar la autonomía de agentes de IA en producción sin supervisión.

Acuerdo de Confidencialidad (NDA)

Garantía absoluta de reserva sobre los hallazgos, vulnerabilidades y dinámicas internas observadas durante el ejercicio.

METODOLOGÍA DE SIMULACIÓN EN 3 FASES (TABLETOP EXERCISE)

FASE 1: HORA CERO

Inyección del Incidente

Aparición repentina de falla no supervisada de IA en producción y detección de anomalía de telemetría.

FASE 2: PRESIÓN EXTERNA

Escalada y Tensión

Llamadas simuladas de clientes Tier 1, presión en redes sociales y vencimiento del reloj de notificación regulatoria.

FASE 3: POST-MORTEM

Dictamen Fiduciario

Evaluación de las decisiones tomadas por el Directorio y entrega del informe confidencial de remediación.

Gustavo Papasergio

Socio Director • Estrategia Digital

Advisory en Crisis Reputacional, Resiliencia Digital y Gobernanza de IA

DIRECTO: contacto@estrategiadigital.com.ar

WEB: estrategiadigital.com.ar

ADVISORY: calendly.com/gustavo-estrategiadigital/30min