Respuesta ante incidentes y recuperación ante crisis

Profesor: Erich Oscar Zschaeck Medina

Grupo : 5

Integrantes: Eduardo Lucero - José Antonio Montero - Rodrigo Flores - Gerson Cornejo

Índice:

Tabla de contenido

Índice: 1
0.-Control de documento 3
1.-Resumen Ejecutivo 4
2.- Alcance, supuestos y objetivos de un plan de gestión de incidentes 6
2.1.-Alcance (qué cubre) + Fuera de Alcance (qué no): 6
2.2.- Supuestos Declarados cuando Falte Información: 7
2.3.-Objetivos del Plan (Operacionales + Gestión + Mejora): 8
2.4.-Prioridades dentro del Proceso: 8
2.5.- Aspectos no Contemplados dentro del Alcance del Plan: 9
3.- Gobernanza IR y modelo operativo (CSIRT/roles/cadencias) 9
3.1.-Definir CSIRT Permanente vs Temporal/Ad-Hoc: 9
3.2.- RACI Mínimo por Macro-Actividades: 11
3.3.- Cadencias (War Room) por Severidad: 12
3.4.-Bitácora/Decisión Log (que se Registra y Quien lo Custodia) 12
4.- Priorización, Clasificación y Escalamiento 13
4.1.-Modelo de Severidad y Criterios de Clasificación: 13
4.2.-Umbral Evento/Alerta/Incidente: 14
4.3.-Trigger para Escalar a Ciber Crisis: 14
5.-Triage y evidencia mínima 15
5.1.-Checklist triage del incidente 15
5.2.-Evidencia mínima requerida por tipo de fuente 16
5.3.-Regla de preservación y custodia de evidencia 17
6.-Playbooks y checklists operativos 17
6.1.-Playbook del caso 17
7.-Concientización y Tabletop 24
7.1.-Estrategia de concientización ligada a riesgos del caso 24
7.2.- Tabletop definido 25
7.3.-Público objetivo y justificación de roles 25
7.4.-Objetivos del ejercicio 26
7.5.-Diseño del ejercicio 26

7.6.-Aplicación del ejercicio 27
7.7.-Validación de éxito 27
7.8.-Cronología del ejercicio 28
8.-Estrategia de comunicación y aplicación al caso 30
8.1.-Estrategia comunicacional 30
9.-Stakeholders 33
10.-Regulaciones y marco aplicables 34
10.1.-Vínculos específicos 35
11.-Gestión de crisis (cibercrisis) 35
11.1 Confirmación de cibercrisis 35
11.2 Comité de cibercrisis. 37
11.3.- Agenda del Comité. 39
11.4.-Alcance del comité 39
12.- Recuperación y continuidad (DR/BC). 40
12.1 Estrategia de recuperación. 40
12.2 Criterios de retorno seguro. 40
12.3 Riesgos de acelerar la recuperación 41
13.- Métricas/KPIs, SLAs y mejora continua 42
13.1 KPI 42
13.2 SLA 46
13.3.- After Action Review 48
13.4.- Backlog 49

0.-Control de documento

Este documento presenta el Plan de Gestión ante incidentes para Cumplo, una fintech dedicada al financiamiento colaborativo para PYMEs en Chile, Mexico y Peru. El plan se enfoca en la respuesta a incidentes de ciberseguridad, alineado con el escenario de ataque a API crítica, basado en el contexto real de la empresa que opera plataformas digitales para intermediar flujos de dinero, onboarding de inversionistas y solicitantes, y coordinación con bancos y pasarelas de pago. Se incorporan elementos de regulaciones locales como la Ley Fintech (21.521) y mejores prácticas internacionales.

Control de Documento:

- Versión: 1.0
- Fecha de Emisión: Enero 17, 2026
- Aprobado por: Gerente de TI (simulado para fines académicos)
- Revisores: Equipo de Ciberseguridad, Legal y Operaciones
- Cambios en esta Versión: Versión inicial completa.

- Versión: 2.0
- Fecha de Emisión: Enero 20, 2026
- Aprobado por: Gerente de TI (simulado para fines académicos)
- Revisores: Equipo de Ciberseguridad, Legal y Operaciones
- Cambios en esta Versión: Actualización completa para enfocarse en escenario único.

Información del Equipo:

- **Gerson Cornejo**
- **Rodrigo Flores**
- **Eduardo Lucero**
- **José Antonio Montero**

1.-Resumen Ejecutivo

Cumplo es una fintech líder en Chile, con operaciones extendidas a México y Perú, que resuelve la desigualdad en el acceso a capital para Pequeñas y Medianas Empresas (PYMEs) mediante financiamiento colaborativo o crowdfunding. Fundada en 2012, la empresa opera plataformas digitales 24/7 que intermedian flujos de dinero entre inversionistas y solicitantes, facilitando préstamos basados en facturas electrónicas, validaciones KYC/AML (Know Your Costumer/Anti-Money Laundering) y coordinación con bancos y pasarelas de pago. Con más de 84 fintech en Chile representando el 7% del ecosistema latinoamericano, Cumplo ha crecido significativamente bajo las regulación de la Ley Fitech (21.521), promulgada en 2023, que fomenta la innovación mientras exige robustos controles de ciberseguridad. Lo que está en juego es la confianza de miles de usuarios -incluyendo inversionistas individuales y PYMEs que dependen de la plataforma para su liquidez diaria-, la continuidad operativa en un entorno cloud altamente dependiente de AWS (Infraestructure as a Service), y el cumplimiento regulatorio con entidades como la Comisión para el Mercado Financiero (CMF), donde una interrupción podría generar pérdidas estimadas en hasta 800.000 CLP por hora de indisponibilidad, además de riesgos reputacionales en un mercado donde el 71% de los préstamos fintech en la región son comerciales. En un contexto global donde el patrón común en incidentes fintech combina abuso de identidades, toma de control de plataformas cloud y exfiltración de datos sensibles, Cumplo prioriza la resiliencia para mantener su rol en la inclusión financiera, habiendo facilitado más de 1.000 millones de dólares en financiamiento acumulado y apoyando a más de 10.000 PYMEs en la región.

El escenario base del incidente es una vulneración de Google IAM leading a creación de cuenta fraudulenta, escalamiento en AWS, exfiltración y cifrado de datos, que se inicia con un email de phishing recibido por un empleado administrativo a las 08:15 AM, conteniendo un enlace malicioso que, al ser clickeado, compromete credenciales de una cuenta válida con accesos privilegiados a IAM en Google Cloud. Esto permite al atacante operar desde dentro de AWS a las 08:40 AM, creando cuentas nuevas fuera de horario (violando políticas), manipulando roles para elevar privilegios, y accediendo a datos sensibles (personales, financieros, tributarios y contables almacenados en AWS). La evolución incluye exfiltración selectiva a servicios externos a las 09:20 AM, detectada parcialmente por firewall logs, y cifrado de archivos críticos a las 09:35 AM, causando degradación en pagos/onboarding reportada por usuarios. actualmente (situación simulada a las 10:30 AM), el incidente está en fase de contención inicial, con aislamiento parcial de instancias AWS, pero con incógnitas clave: alcance completo de exfiltración y cifrado (ausencia de SIEM/EDR limita visibilidad), y riesgo de persistencia si el atacante mantiene acceso latente. Hipótesis de vector: Phishing inicial -> Compromiso credenciales IAM -> Creación cuenta fraudulentas/persistencia -> Escalamiento privilegios AWS -> Exfiltración datos sensibles -> Cifrado para extorsión/ransomware, basada en evidencia disponible (logs correo, cambios IAM, tráfico anómalo, detecciones AV); si se invalida (e.g., no phishing sino insider), ajusta respuesta. Este escenario afecta procesos críticos (pagos, onboarding), con potencial escalamiento regulatorio si brecha confirmada, reflejando

patrones reales como brechas en Capital One (2019) o SolarWinds (2020), destacando vulnerabilidades en identidades cloud multi-país

Severidad preliminar: Crítica (20/25), impulsada por (1) alto impacto en continuidad cooperativa (degradación/cifrado durante peak AM, interrumpiendo flujos dinero); (2) exposicion datos sensibles (activando Ley 19.628/CMF); incertidumbre critica: Alcance exfiltracion/cifrado, limitada por telemetria basica (CloudWatch/Wazuh sin EDR completo).

Decisiones clave tomadas: (1) Declarar incidente crítico y activar War Room; (2) Contención inicial (aislar instancias, bloquear sesiones IAM). Decisiones pendientes: (3) Confirmar exfiltración/cifrado vía forense (determina notificación CMF); (4) Rotar credenciales completas; (5) Escalar crisis si persiste degradación >4 horas.

Este resumen enfatiza la respuesta ágil alineada con apetito de riesgo de Cumplo, enfocada en vulneración IAM/exfiltración/cifrado para sostener crecimiento regional.

2.- Alcance, supuestos y objetivos de un plan de gestión de incidentes

2.1.-Alcance (qué cubre) + Fuera de Alcance (qué no):

El plan de gestión de incidentes cubre exclusivamente las fases del ciclo de respuesta a incidentes de ciberseguridad para el escenario base de vulneración de Google IAM que lleva a la creación de cuentas fraudulentas, escalamiento de privilegios en AWS, exfiltración de datos sensibles y cifrado de archivos en Cumplo. Basado en el marco NIST SP 800-61 adaptado al contexto fintech chileno.

Específicamente, abarca:

A.- Detección de compromisos iniciales en sistemas de identidad como IAM en Google Cloud, incluyendo alertas por creaciones de cuentas fuera de horario (e.g., playbook específico para horarios 12:00 - 13:00).

B.- Contención de escalamientos en entornos cloud como AWS, enfocándose en aislamiento de instancias comprometidas y bloqueo de sesiones fraudulentas.

C.- Análisis y erradicación de persistencia, exfiltración (e.g., tráfico outbound a IPs sospechosas) y cifrado (e.g., detecciones de ransomware en logs de endpoint/AV).

D.- Recuperación de datos sensibles (personales, financieros, tributarios y contables almacenados en AWS), priorizando restauración segura desde backups limpios.

E.- Procesos de negocio críticos afectados, como onboarding de inversionistas/solicitantes con validaciones KYC/AML, intermediación de flujos de dinero y coordinación con bancos/pasarelas de pago, con énfasis en minimizar interrupciones durante periodos de alta carga cooperativa (días hábiles AM).

F.- Impactos multi-país en Chile, México y Perú, considerando fricciones como diferencias en zonas horarias, proveedores locales y regulaciones específicas (e.g., SBS en Perú, CNBV en México).

G.- Aspectos de cumplimiento regulatorio, incluyendo notificaciones timely a CMF/CSIRT si se confirma brecha de datos, y preservación de evidencia forense para auditorías

H.- Unidades organizacionales involucradas, como TI, Ciberseguridad, Operaciones, Legal, Finanzas y Alta Dirección, con integración de herramientas existentes como CloudWatch para monitoreo, Wazuh para logs de seguridad, Zabbix para disponibilidad, y playbooks predefinidos para creaciones de cuentas.

El plan busca minimizar impactos operativos (pérdidas estimadas 800.000 CLP/hora), regulatorios (multas CMF) y reputacionales (erosión de confianza en crowdfunding), alineado con la estructura reducida y escalable de Cumplo (equipo interno pequeño, enfoque híbrido cloud/open-source).

Fuera de alcance quedan:

A.- Incidentes no relacionados con vulneraciones de identidad cloud, como abusos directos de APIs expuestas, ataques físicos a infraestructura o fallos no cibernéticos (e.g., desastres naturales)

B.- Proveedores externos no integrados directamente en el flujo IAM/AWS, como bancos o pasarelas de pago sin dependencias de identidad compartida.

C.- Desarrollo o implementación del nuevo código durante la respuesta, limitándose a configuraciones y herramientas existentes.

D.- Auditorías externas post-incidente, litigios derivados o estrategias de seguros cibernéticos, delegados a equipos legales especializados.

E.- Escenarios en entornos legacy no cloud o expansiones futuras a nuevos mercados y actualización explícita del plan.

F.- Tipos de incidentes alternos como phishing no leading a IAM compromise, DDoS lógicos o sabotaje OT, para mantener foco en el caso base.

G.- Capacitación general de empleados no especifica a IR, aunque se integra concientización targeted en riesgos de identidades cloud y creaciones fraudulentas.

2.2.- Supuestos Declarados cuando Falte Información:

Para asegurar trazabilidad profesional y mitigar riesgos en un entorno con telemetría limitada (ausencia de SIEM/EDR completo, dependencia de herramientas open-source como Wazuh), se declaran supuesto explícitos, reconociendo que su invalidez podría alterar la respuesta;

A.- Asumimos que las herramientas de monitoreo existentes (CloudWatch para alertas en AWS, Wazuh como SIEM/XDR para logs de seguridad y detección de vulnerabilidades, Zabbix para disponibilidad) están operativas y configuradas para capturar cambios en IAM, creaciones de cuentas fraudulentas y patrones de exfiltración/cifrado; si fallan o son comprometidas (e.g., atacante deshabilita logging), aumenta el riesgo de detección tardía y propagación no detectada, requiriendo fallback manual a logs básicos.

B.- Asumimos acceso completo e inalterado a evidencias en Google IAM y AWS (e.g., CloudTrail para auditoria de cambios, firewall logs para tráfico outbound); si los registros han sido manipulados por el atacante (común en escalamiento de privilegios), genera incertidumbre en la reconstrucción del timeline de exfiltración/cifrado, potencialmente invalidando evidencia forense y requiriendo suposiciones conservadoras en severidad.

C.- Asumimos disponibilidad del equipo interno en horario 5x8 (días hábiles), con soporte remoto para operaciones 24/7 en incidentes críticos; si el compromiso ocurre fuera de horario o en fines de semana, podría demorar la respuesta inicial hasta 1-2 horas, incrementando impactos como extensión del cifrado, especialmente en peaks AM multi-país.

D.- Asumimos cumplimiento inicial con regulaciones como la Ley Fintech (21.521) y Protección de Datos (19.628), incluyendo segregación de funciones en controles de identidades; si se identifica no cumplimiento durante el incidente (e.g., políticas de horarios para creaciones de cuentas no aplicadas), amplifica riesgos regulatorios como multas o suspensiones por brecha de datos filtrados.

E.- Asumimos que terceros críticos (AWS, Google Cloud, bancos, pasarelas) responden dentro de SLAs contractuales (e.g. soporte AWS <1 hora para criticar); si hay demoras, complica la contención de escalamientos y recuperación post-cifrado, potencialmente extendiendo downtime.

F.- Asumimos una tasa baja de eventos en el ecosistema pequeño de Cumplo, permitiendo enfoque híbrido en monitoreo sin sobrecarga; si la frecuencia aumenta (e.g., campañas de phishing targeted), podría requerir escalabilidad no planificada, afectando la efectividad en detección de persistencia.

Estos supuestos se revisan en triage inicial; si son falsos, se documentan en bitácora con ajustes de riesgos (e.g., asumir peor caso en exfiltración si los logs son incompletos).

2.3.-Objetivos del Plan (Operacionales + Gestión + Mejora):

Los objetivos son específicos, medibles, realistas y alineados exclusivamente al escenario de vulneración IAM/exfiltracion/cifrado, considerando capacidades limitadas de Cumplo (equipo reducido, herramientas open-source sin EDR completo, resiliencia cloud pero con brechas en visibilidad):

A.- Detectar compromisos en IAM y creaciones fraudulentas en menos de 60 minutos mediante alertas automáticas (medible por Mean Time to Detect - MTTD, verificable a traves de timestamps en logs de Wazuh/CloudWatch, ajustado a tasa baja de eventos para evitar falsos positivos sobrecargantes).

B.- Contener escalamientos en AWS y propagación de exfiltración/cifrado en menos de 4 horas, limitando impacto a menos del 50% de datos sensibles (verificable por aislamiento exitoso de instancias y métricas de egress en firewall, realista dado monitoreo híbrido pero sin automatización avanzada).

C.- Recuperar accesos IAM y datos cifrados en menos de 8 horas, manteniendo uptime operativo >90% durante el incidente (medible por Mean Time to Recovery - MTTR

y reportes de restauración desde backups, considerando dependencia de proveedores cloud para validaciones seguras).

D.- Cumplir al 100% con obligaciones regulatorias, como notificación a CMF/CSIRT en menos de 72 horas si se confirma brecha de exfiltración (verificable por registros de reportes y auditorias internas, priorizando plazos conversadores para entornos multi-país).

E.- Coordinar equipos multi-país sin fricciones mayores, asegurando >80% de adherencia a cadencias de War Rooms (medible por bitácoras de reuniones y feedback post-incidente, ajustado a zonas horarias para evitar demoras).

F.- Preservar y analizar evidencia forense en el 100% de los casos, generando reportes accionables para prevención de recurrencias en identidades cloud (verificable por cadena de custodia documentada y snapshots de logs IAM/AWS).

G.- Identificar al menos 3 lecciones aprendidas por incidente en el After-Action Review (AAR), implementando quick wins en menos de 60 días (medible por backlog de mejoras priorizado y seguimiento de implementación, enfocando en gps como visibilidad en creaciones fraudulentas).

H.- Mejorar la madurez del proceso IR anualmente, midiendo reducción en MTT R >10% a través de ejercicios tabletop y simulacros específicos a escenarios IAM/cloud (verificable por KPIs comparativos año tras año, realista con recursos internos limitados y posible consultoría externa inicial estimada en ~US$10.000).

2.4.- Que se Valida Primero (Priorización Validación):

La priorización de validación se basa en el impacto crítico del escenario IAM/exfiltración/cifrado, enfocado primero en riesgos inmediatos de propagación y regulatorio:

A.- Contención de escalamiento IAM/AWS y detección de exfiltración/cifrado (validar aislamiento/no propagación mediante métricas de egress y detección AV, priorizando porque evita extensión de daños a datos sensibles y continuidad operativa en peaks AM).

B.- Integridad y alcance de datos exfiltrados/cifrados (confirmar vía análisis forense de logs IAM/CloudTrail, por alto riesgo regulatorio bajo Ley 19.628 y potencial multas CMF si brecha no contenida).

C.- Cumplimiento con notificaciones (verificar <72 horas para CMF/CSIRT si brecha confirmada, priorizando para minimizar sanciones en entornos multi-país).

D.- Coordinación equipos y manejo de terceros (evaluar adherencia a cadencia y SLAs de AWS/Google, por direcciones operativas en zonas horarias).

E.- Mejora continua (revisar ARR y backlog, último porque depende de cierre pero esencial para prevención de recurrencias en identidades cloud).

2.5.- Prioridades dentro del Proceso:

1. Contención inmediata de vulneración IAM y escalamiento AWS para detener exfiltración/cifrado y preservar datos sensibles (prioridad máxima por impacto en crown jewels cómo storage financiero en AWS).
2. Mantenimiento de continuidad operacional en procesos críticos como pagos/onboarding post-cifrado, especialmente durante peaks AM (segunda por pérdidas estimadas 800.000 CLP/hora).
3. Cumplimiento regulatorio y coordinación con terceros (e.g., notificación <72 horas a CMF/CSIRT, soporte AWS), para evitar multas y disrupciones en bancos/pasarelas.
4. Comunicación controlada y preservación de evidencia forense, para soportar auditorías y manejar reputación.
5. Mejora continua a través de AAR, integrando lecciones para fortalecer defensas en identidades cloud sin sobrecargar recursos limitados.

2.6.- Aspectos no Contemplados dentro del Alcance del Plan:

A.- No se incluyen planes de continuidad de negocio (BCP) o recuperación de desastres (DRP) completos más allá de la fase cibernética específica al escenario IAM/exfiltración/cifrado.

B.- Estrategias de seguros cibernéticos o respuestas a incidentes híbridos (ciber-físicos).

C.- Litigios derivados o auditorías externas post-incidente.

D.- Expansiones futuras a nuevos mercados o tipos de incidentes no alineados al caso base (e.g., abusos de API sin compromisos IAM, DDoS o phishing no leading a escalamiento cloud).

E.- Desarrollo de herramientas adicionales durante la respuesta, limitándose a las capacidades existentes como Wazuh/Zabbix para mantener realismo y foco.

3.- Gobernanza IR y modelo operativo (CSIRT/roles/cadencias)

3.1.-Definir CSIRT Permanente vs Temporal/Ad-Hoc:

En cumplo, el modelo de gobernanza para Incident Response (IR) adopta un enfoque híbrido escalable y adaptable, diseñado para equilibrar la agilidad operativa diaria con la capacidad de respuesta a incidentes críticos como la vulneración de Google IAM que lleva a creaciones de cuentas fraudulentas, escalamiento de privilegios en AWS, exfiltración de datos sensibles y cifrado de archivos. Este modelo distingue claramente entre un CSIRT permanente para operaciones rutinarias y un CSIRT temporal/ad-hoc para escalamientos, alineado con mejores prácticas de NIST SP 800-61 y recomendaciones regulatorias locales como la NCG 502 de la CMF, que enfatizan la segregación de funciones en controles críticos para evitar conflictos de interés (e.g., operaciones priorizando sobre seguridad). El CSIRT permanente opera como un equipo núcleo compacto y dedicado al monitoreo continuo y respuesta a incidentes de bajo/mediano impacto, compuesto por:

- SOC interno con Analistas L1 (responsables del triage inicial de alertas, e.g., detección de creaciones de cuentas fuera de horario via Wazuh) y L2 (análisis avanzado de logs para confirmar escalamientos en AWS, supervisando directamente a L1 para escalabilidad).

- Equipo TI/Plataforma para ejecuciones técnicas básicas (e.g., revisión de logs de CloudWatch para anomalías en IAM).

- Jefe de Ciberseguridad reportando directamente al CTO, asegurando independencia estratégica y alineación con objetivos de negocio como minimizar disrupciones en pago/onboarding.

Este núcleo maneja el 80% de los eventos diarios en un entorno fintech con baja tasa de incidentes, como validaciones iniciales de phishing leading a compromisos IAM o alertas de cuentas fraudulentas, permitiendo respuestas rápidas en horario 5x8 sin sobrecargar recursos limitados (equipo pequeño, enfoque híbrido cloud/open-source).

Para incidentes de alto impacto o críticos (severidad >10, e.g., confirmación de exfiltración/cifrado tras escalamiento AWS), se activa un CSIRT temporal/ad-hoc, expandiendo el núcleo con apoyo especializado para manejar la complejidad del escenario:

- Legal/DPO para evaluación regulatoria y preservación de evidencia (e.g., preparación de notificaciones a CMF/CSIRT por brecha de datos filtrados).
- Comunicaciones para control de narrativa interna/externa (e.g., mensajes need-to-know sobre impacto en usuarios durante cifrado).

- RRHH para aspectos de insider threats o verificación de accesos (e.g., revisión de empleados involucrados en phishing inicial).
- Representantes de Negocio (Ops/Finanzas/Fraude) para priorización de impactos financieros (e.g., estimación de pérdidas por downtime en flujos de dinero).
- Proveedores externos críticos (e.g., soporte AWS/Google para análisis forense de escalamiento o descifrado).

Esta activación se gatilla automáticamente vía playbook (e.g., al detectar creaciones fraudulentas o exfiltración), permitiendo escalabilidad sin alterar la jerarquía diaria y promoviendo una respuesta coordinada multi-país (e.g., LISO locales en México/Perú para regulaciones específicas como CNBV o SBS). El modelo reduce incidentes en 40-60% según benchmarks fintech (e.g., separación de roles como en ISO 27001), minimizando puntos ciegos como priorización operativa sobre seguridad, y asegura cumplimiento con mejores prácticas NIST/COBIT al requerir independencia en auditoría y respuesta. Transiciones entre permanente y ad-hoc se documentan en bitácora para trazabilidad, con revisión anual para adaptaciones (e.g., integración futura de SIEM su recurso permiten).

3.2.- RACI Mínimo por Macro-Actividades:

La matriz RACI (Responsible, Accountable, Consulted, Informed) está diseñada para eliminar ambigüedades en una estructura fintech ágil como la de Cumplo, asegurando claridad en responsabilidades durante el escenario de vulneración IAM/exfiltración/cifrado. Se define para macro-actividades clave, incorporando roles multi-pais (e.g., LISO) y ejemplos específicos al caso para realismo.

Macro-Actividad	Gerente de TI	Equipo TI/Operaciones	Seguridad de la información	Representante de Negocio	Legal	Comunicaciones	Terceros (e.g., AWS/Bancos)
Triage y Clasificación	A	R	C	C	I	I	I
Contención y Erradicación	A	R	C	I	C	I	C/R (si afecta sus sistemas)
Comunicaciones Internas/Externas	A	I	I	C	C	R	I
Coordinación con Terceros	A	C	I	I	C	I	R
Recuperación y Cierre	A	R	C	C	C	I	C
Post-Mortem y Mejora	A	C	R	C	C	I	I

Este RACI se revisa anualmente o post-incidente, asegurando adaptabilidad a expansiones (e.g., nuevos mercados) y segregación de funciones para cumplimiento normativos.

3.3.- Lista jerárquica estructurada por actividad, con contexto y justificaciones.

1. **Preparación (Capacitación/Drills):**
    - **Contexto:** Incluye entrenamiento y simulacros específicos para vulneraciones IAM, creaciones fraudulentas y manejo de exfiltración/cifrado, para seguridad readiness en entornos cloud.
    - **Responsible (Ejecuta):** Jefe de Ciberseguridad (lidera implementación de drills, e.g, simulacros de phishing leading a escalamiento AWS).
    - **Accountable (Responde):** CTO (garantiza alineación estratégica con apetito de riesgo, aprobando currículo).
    - **Consulted (Opina):** Seguridad y TI (aportan expertise en herramientas como Wazuh para detección de cuentas fraudulentas).
    - **Informed (Se Notifica):** Directorio y RRHH (reciben updates sobre madurez del equipo, para cumplimiento anual).
    - **Justificación:** Enfocado en prevención de recurrencias, realista con recursos limitados (capacitación ~US$10.000 inicial).
2. **Detección y Triage:**
    - **Contexto:** Fase inicial para identificar alertas de compromisos IAM (e.g., creaciones fuera horario) y clasificar severidad rápidamente, antes de exfiltración/cifrado.
    - **Responsible (Ejecuta):** Analista L1 (realiza triage de logs y alertas en Zabbix/Wazuh para anomalías IAM).
    - **Accountable (Responde):** Jefe de Ciberseguridad (supervisa clasificación, asegurando escalamiento timely).
    - **Consulted (Opina):** TI/Plataforma (evalúan impacto técnico en AWS, e.g., correlación con tráfico outbound).
    - **Informed (Se Notifica):** Gerente TI y Negocio (se avisan para priorizar recursos en pagos afectados).
    - **Justificación:** Prioriza detección temprana para contener antes de cifrado, alineado con brechas en visibilidad (sin EDR).
3. **Contención Inmediata:**
    - **Contexto:** Acciones urgentes para detener escalamientos IAM/AWS y propagación de exfiltración/cifrado (e.g., bloqueo de cuentas fraudulentas).
    - **Responsible (Ejecuta):** Equipo TI (ejecuta aislamientos en AWS y revoca sesiones IAM sospechosas).
    - **Accountable (Responde):** Gerente TI (toma decisiones operativas, equilibrando disrupción).
    - **Consulted (Opina):** Seguridad y Legal (asesoran sobre riesgos de evidencia y cumplimiento en brechas).
    - **Informed (Se Notifica):** CTO y Finanzas (reciben reportes de impacto potencial en flujos de dinero).
    - **Justificación:** Enfocado en minimizar pérdidas (800k CLP/hora), con segregación para evitar conflictos.

4. **Análisis Forense:**
    - **Contexto:** Investigación profunda de evidencias para reconstruir el timeline de exfiltración/cifrado post-vulneración IAM.
    - **Responsible (Ejecuta):** Analista L2 (realiza correlación de logs IAM/CloudTrail para identificar persistencia).
    - **Accountable (Responde):** Jefe de Ciberseguridad (válida hallazgos, asegurando trazabilidad).
    - **Consulted (Opina):** Proveedores (AWS/Google) (aportan datos técnicos para análisis de escalamientos).
    - **Informed (Se Notifica):** Legal y CSIRT Extendido (informados para acciones regulatorias si hay brecha).
    - **Justificación:** Realista con herramientas limitadas, prioriza preservación para auditorías CMF.
5. **Erradicación:**
    - **Contexto:** Eliminación completa de amenazas, incluyendo remoción de cuentas fraudulentas y descifrado de archivos.
    - **Responsible (Ejecuta):** Equipo TI/Seguridad (ejecutan limpiezas en AWS y escaneos de vulnerabilidades IAM).
    - **Accountable (Responde):** Gerente TI (coordina erradicación, verificando no reinfección).
    - **Consulted (Opina):** Legal (para evidencia preservada en cadena de custodia).
    - **Informed (Se Notifica):** CTO y Directorio (reciben confirmación de resolución para cierre).
    - **Justificación:** Enfocado en prevención de recurrencia, con checks para multi-país.
6. **Recuperación y Validación:**
    - **Contexto:** Restauración segura post-cifrado, validando integridad de datos exfiltrados.
    - **Responsible (Ejecuta):** Equipo TI (restaurar backups y prueba IAM/AWS).
    - **Accountable (Responde):** Gerente TI (aprueba retorno seguro, equilibrando velocidad).
    - **Consulted (Opina):** Negocio (Ops/Finanzas) (priorizan impactos en pagos/onboarding).
    - **Informed (Se Notifica):** Directorio y Clientes (si aplica, para updates de status).
    - **Justificación:** Realista con backups cloud, minimiza downtime en peaks.

7. **Comunicaciones Internas:**
    - **Contexto:** Manejo de mensajes durante crisis por exfiltración/cifrado.
    - **Responsible (Ejecuta):** Comunicaciones (redacta/distribuye updates need-to-know).
    - **Accountable (Responde):** CTO (aprueba contenido técnico sobre IAM).
    - **Consulted (Opina):** Legal y Seguridad (revisan compliance y riesgos).
    - **Informed (Se Notifica):** Todo Staff y Directorio (reciben comunicaciones directas).
    - **Justificación:** Controla rumores en equipo multi-país.
8. **Comunicaciones Externas:**
    - **Contexto:** Notificaciones a reguladores/clientes por brecha exfiltración.
    - **Responsible (Ejecuta):** Comunicaciones (gestiona declaraciones, e.g., <72h CMF).
    - **Accountable (Responde):** CEO (responsabilidad ejecutiva en reputación).
    - **Consulted (Opina):** Legal/DPO y Reguladores (asesoran legalidad).
    - **Informed (Se Notifica):** Clientes y Medios (si escala, info controlada).
    - **Justificación:** Alineado matriz comunicación para consistencia.
9. **Manejo de Terceros:**
    - **Contexto:** Coordinación con AWS/Google para soporte en escalamientos/cifrado.
    - **Responsible (Ejecuta):** Gerente TI (contacta/gestiona tickets).
    - **Accountable (Responde):** CTO (supervisa contratos/SLAs).
    - **Consulted (Opina):** Proveedores (AWS/Google/bancos) (aportan soluciones).
    - **Informed (Se Notifica):** Seguridad y Finanzas (updates dependencias).
    - **Justificación:** Minimiza demoras en recuperación multi-país.
10. **Escalamiento a Crisis:**
    - **Contexto:** Transición si exfiltración/cifrado persiste (>15 severidad).
    - **Responsible (Ejecuta):** Gerente TI (inicia escalamiento).
    - **Accountable (Responde):** CTO (decide activación comité).
    - **Consulted (Opina):** Comité de Crisis (opinan estrategia).
    - **Informed (Se Notifica):** Directorio y Reguladores (<72h si brecha).
    - **Justificación:** Alineado triggers para manejo de extorsión.
11. **Cierre y AAR:**
    - **Contexto:** Lecciones aprendidas post-erradicación IAM/exfiltración.
    - **Responsible (Ejecuta):** Jefe de Ciberseguridad (facilita AAR).
    - **Accountable (Responde):** CTO (aprueba recomendaciones).
    - **Consulted (Opina):** Todo CSIRT (feedback completo).
    - **Informed (Se Notifica):** Directorio y Equipos (reporte final).
    - **Justificación:** Fomenta mejora continua con backlog realista.

12. **Mejora Continua:**
    - **Contexto:** Implementación de lecciones para fortalecer IAM/cloud.
    - **Responsible (Ejecuta):** Jefe de Ciberseguridad (lidera iniciativas, e.g., capacitación phishing).
    - **Accountable (Responde):** CTO (integra roadmap).
    - **Consulted (Opina):** Seguridad y TI (sugieren mejoras técnicas).
    - **Informed (Se Notifica):** Directorio y RRHH (progresos anuales).
    - **Justificación:** Realista con presupuesto (~US$10.000 consultoría), mide reducción de incidentes.

3.4.- Cadencias (War Room) por Severidad:

Las cadencias aseguran coordinación en escenario IAM/exfiltración/cifrado, adaptadas a severidad y horario (5x8 con 24/7 críticos). Virtuales vía Teams, agenda fija: revisión estado (e.g., avance exfiltración), decisiones pendientes (e.g., rotar IAM), riesgos actualizados (e.g., propagación cifrado), asignaciones. Participantes varían para eficiencia, con grabación para AAR:

- **Baja (1-5):** Reuniones diarias de 30 minutos, enfocadas en resolución rutinaria; participantes: Núcleo CSIRT (Analistas L1/L2, TI, Jefe de Ciberseguridad). Frecuencia: Solo si persiste >24 horas, enfocando monitoreo post-contención.
- **Media (6-10):** Cada 4 horas (duración 45 minutos), incorporando análisis preliminar; participantes: Nucleo + Legal (para evidencia) y Negocio (para impacto operativo). Frecuencia: Hasta contención confirmada, ajustada a zonas horarias multi-país.
- **Alta (11-15):** Cada 2 horas (duración 1 hora), con énfasis en contención y escalamiento; participantes: CSIRT extendido (Núcleo + Comunicaciones, Finanzas, LISO locales si aplica). Frecuencia: Durante fase crítica, reduciendo a diaria post-contención.
- **Crítica (16-25):** Cada hora inicial (duración 1 hora), luego cada 4 horas; participantes: CSIRT completo + Alta Dirección (CEO, CTO, CFO) y externos si aplica. Frecuencia: Continua hasta erradicación, con reportes ejecutivos cada 2 horas para trazabilidad regulatoria.

Todas las War Room incluyen grabación para trazabilidad y revisión en AAR, ajustándose a zonas horarias (e.g., priorizar Chile como hub).

3.5.-Bitácora/Decisión Log (que se Registra y Quien lo Custodia)

La bitácora es un registro centralizado, auditable y estructurado de todas acciones IR en escenario IAM/exfiltración/cifrado, usando plantilla en Google Sheets o similar (columnas: Timestamp, Decisión/Acción, Responsable, Justificación, Impacto Esperado, Resultado, Notas/Riesgos). Se registra obligatoriamente:

- Decisiones críticas (e.g., aislamiento AWS post-creación fraudulenta, rotar IAM, notificar CMF <72h brecha).
- Hitos clave (e.g., detección phishing inicial, confirmación exfiltración, inicio descifrado).
- Evidencias recolectadas (e.g., snapshots logs IAM)
- Comunicaciones enviadas (e.g., updates War Room)
- Cambios severidad/hipótesis vector (e.g., de phishing a insider si invalida); y
- Riesgos identificados con mitigaciones (e.g., incertidumbre cifrado por logs alterados).

Regla estricta: Toda decisión debe registrarse en tiempo real durante War Rooms, sin excepciones, para asegurar gobernanza y soporte post-mortem (e.g., en auditorías CMF). Custodiado por el Scribe designado (generalmente Analista L2 o rol equivalente), con acceso read-only para el equipo y backups encriptados en AWS S3. Revisiones diarias por el jefe de Ciberseguridad durante el incidente, y archivado por 1 año mínimo para cumplimiento regulatorio.

Este segmento de gobernanza fortalece la resiliencia de Cumplo, alineando con su estructura reducida y escalable, donde la independencia del CISO (o equivalente) reduce incidentes en 40-60% según benchmarks fintech.

4.- Priorización, Clasificación y Escalamiento

4.1.-Modelo de Severidad y Criterios de Clasificación:

El modelo de severidad para Cumplo.cl se basa en el estándar NIST SP 800-61r2, adaptado específicamente al contexto fintech chileno regulado por la Ley Fintech (21.521) y la CMF, incorporando factores de impacto en datos sensibles, continuidad operativa y obligaciones de notificación. La fórmula es Severidad = Probabilidad (1-5) × Impacto (1-5), generando una escala numérica de 1 a 25 con los siguientes niveles:

- **0: Evento No Incidente:** Anomalía técnica sin impacto ni violación de políticas (ejemplo: pico de tráfico IAM sin cambios de privilegios).
- **1-5: Baja:** Impacto mínimo y aislado, recuperable sin escalamiento significativo (ejemplo: intento fallido de phishing sin compromiso efectivo de credenciales IAM).
- **6-10: Media:** Impacto localizado y controlable en horas, afecta un proceso no crítico (ejemplo: creación de cuenta fraudulenta detectada y aislada antes de escalamiento AWS).
- **11-15: Alta:** Impacto operativo significativo, afecta procesos críticos parciales o genera riesgo regulatorio moderado (ejemplo: escalamiento de privilegios en AWS con exfiltración parcial detectada pero no cifrado activo).
- **16-25: Crítica:** Impacto sistémico, regulatorio y/o reputacional grave (ejemplo: exfiltración confirmada de datos sensibles + cifrado de archivos críticos en AWS, con potencial extorsión y downtime prolongado).

4.2.-Criterios de Probabilidad (1-5):

- 1: Muy baja - sin evidencia o similitud con incidentes previos.
- 2: Baja - indicios aislados, fácil de descartar (ejemplo: alarma falsa en Wazuh).
- 3: Media - evidencia parcial pero consistente (ejemplo: cambios IAM anómalos sin egress).
- 4: Alta - evidencia clara y correlacionada (ejemplo: creación fraudulenta + tráfico outbound sospechoso).
- 5: Muy alta - confirmación casi total (ejemplo: exfiltración detectada + cifrado activo + logs alterados).

4.3.-Criterios de Impacto (1-5):

- 1: Mínimo - sin afectación operativa ni regulatoria.
- 2: Bajo - impacto localizado, recuperación <1 hora.
- 3: Medio - interrupción parcial de procesos, recuperación <4 horas.
- 4: Alto - interrupción significativa, datos sensibles comprometidos, notificación regulatoria probable.
- 5: Crítico - interrupción sistemática (>4 horas), exfiltración/cifrado masivo, riesgo reputacional/extorsión, notificación obligatoria CMF/CSIRT, perdidas >1M CLP.

4.4.-Aplicación al Caso (Vulneración Google IAM -> Cuenta fraudulenta -> Escalamiento AWS -> Exfiltración/Cifrado):

- Probabilidad = 4 (Alta): Evidencia clara de phishing inicial + cambios IAM detectados + tráfico outbound anómalo en firewall + detecciones de cifrado en AV, aunque limitada por ausencia de SIEM/EDR completo (incertidumbre en alcance total).
- Impacto = 5 (Crítico): Afectación directa a crown jewels (datos personales/financieros/tributarios en AWS), degradación cooperativa en pagos/onboarding durante peak AM, riesgo de extorsión por cifrado, y obligación de notificación <72h a CMF/CSIRT por brecha confirmada.
- **Severidad calculada: 20/25 - Crítica.**

Este rating justifica escalamiento inmediato al Gerente TI y activación de War Room, priorizando contención sobre análisis profundo inicial para minimizar propagación.

4.5.-Umbral Evento/Alerta/Incidente:

- **Evento:** Anomalía técnica sin impacto confirmado ni violación de políticas (ejemplo: alerta de acceso IAM fuera de horario sin creación de cuenta ni cambios de rol). Umbral: Monitoreo pasivo en Zabbix/Wazuh, cierre automático si no escala en <15 min.
- **Alerta:** Potencial amenaza o violación detectada pero sin impacto material inmediato (ejemplo: creación de cuenta fraudulenta fuera de horario detectada por playbook, o intento de escalamiento IAM bloqueado por MFA). Umbral: Genera notificación automática (email/Slack al Analista L1), requiere triage en <30 min para validar y escalar si procede.
- **Incidente**: Confirmación de impacto o riesgo material (ejemplo: cuenta fraudulenta utilizada para escalamiento AWS + exfiltración detectada en firewall + cifrado activo en endpoints). Umbral: Afecta crown jewels (datos sensibles en AWS), viola políticas internas (e.g., horario creación cuentas), o muestra persistencia/escalamiento. Gatilla activación inmediata de playbook, cálculo de severidad y notificación al Gerente TI.

4.6.-Trigger para Escalar a Ciber Crisis:

La escalada de incidentes a ciber crisis representa el paso a gestión estratégica corporativa, activando el Comité de Crisis y cambiando el enfoque de técnico-operativo a ejecutivo-regulatorio. Gatillos específicos y cuantitativos para objetividad en el escenario IAM/exfiltración/cifrado:

- Severidad ≥16 (Crítica) o duración del incidente >4 horas sin contención efectiva.
- Confirmación de exfiltración de datos sensibles (personales/financieros/tributarios) o cifrado activo en >20% de instancias críticas.
- Impacto multi-país (Chile/México/Perú) o afectación de terceros críticos (bancos/pasarelas de pago).
- Amenaza de extorsión/ransomware explícita o indicios de actor avanzado (persistencia detectada tras aislamiento inicial).
- Pérdidas financieras proyectadas >1 millón CLP o afectación reputacional significativa (e.g., filtración pública en redes o queja masiva de inversionistas).

4.7.-Cambios al escalar a cibercrisis:

a) Liderazgo pasa del Gerente TI/CTO al Comité de Crisis (CEO como líder, con COO, CISO/CIO, Legal/DPO, Comunicaciones, Dueño Negocio).
b) Cadencias intensificadas a cada hora inicial (duración 45-60 min), luego cada 4 horas.
c) Vocerías externas controladas exclusivamente por Comunicaciones/CEO (alineado con matriz de comunicación).
d) Notificación inmediata a reguladores (CMF/CSIRT <24 horas si brecha confirmada, <72 horas máximo).
e) Activación de planes de continuidad de negocio (BC) para priorizar restauración segura de pagos/onboarding.
f) Autorización de decisiones excepcionales (e.g., pago extorsión - no recomendado - o aislamiento total de instancias AWS).

4.8.-Priorización Operativa (que va primero y por qué):

La priorización no sigue orden de llegada (FIFO), sino impacto/riesgo real en el escenario IAM/exfiltración/cifrado, alineada con severidad crítica (20/25) y apetito de riesgo de cumplo (continuidad > cumplimiento > reputación):

1. **Contención inmediata de escalamiento IAM/AWS y detención de exfiltración/cifrado**
    - **Por qué primero:** Evita propagación masiva y extensión del cifrado, minimizando pérdidas operativas (800.000 CLP/hora) y alcance de brecha (Ley 19.628). Acciones: aislamiento de instancias, bloqueo de cuentas fraudulentas, revocación de sesiones IAM.
2. **Análisis y confirmación de exfiltración/cifrado**
    - **Por qué segundo:** Determina si hay brecha material (obligación notificación CMF/CSIRT <72h), y define alcance para recuperación segura. Acciones: revisión logs CloudTrail/firewall/AV para timeline y volumen datos afectados.
3. **Coordinación con terceros críticos (AWS/Google/bancos)**
    - **Por qué tercero:** Evita demoras en soporte técnico (e.g., snapshots forenses AWS) o disrupción en pagos coordinados. Acciones: apertura de tickets prioritarios, intercambio de logs.
4. **Comunicaciones internas y externas controladas**
    - **Por qué cuarto:** Controla narrativa y reputación post-contención (need-to-know interno, notificación clientes/reguladores si aplica). Acciones: updates War Room, preparación declaración CMF.
5. **Recuperación y validación**
    - **Por qué quinto:** Solo después de erradicación confirmada, para evitar reinfección. Acciones: restauración, backups limpios, pruebas de integridad.
6. **Cierre, AAR y mejora continua**
    - **Por qué último:** Depende de resolución completa, pero crítico para prevención (e.g., fortalecer MFA IAM, automatizar alertas creaciones fraudulentas).

Esta priorización se documenta en bitácora desde triage inicial y se revisa en cada War Room, asegurando alineación con gobernanza (RACI) y matriz de comunicación.

5.-Triage y evidencia mínima

Este segmento aterriza la conducción operativa de las primeras 4-8 horas desde la alerta, para tomar control del incidente con evidencia mínima (no forense profundo), decidir gates tempranos (aislar/cortar/reset) y alinear el triage a la severidad y prioridades definidas en el Segmento 4.

5.1.-Conducción secuencial 0-8 horas

Principio operativo: se trabaja en dos estados en paralelo (1) incidente potencial con incógnitas críticas y (2) incidente confirmado. La transición se registra en bitácora con la evidencia mínima que la respalda.

Ventana	Objetivo	Incógnitas críticas a cerrar	Gate (decisión) y criterio	Acciones (orden lógico)	Responsable (A/R)
T0-30 min	Reconocer y estabilizar la señal	Qué disparó la alerta, qué activos podrían estar involucrados, existe actividad en curso.	Declarar 'Incidente Potencial' si hay violación de política o acceso anómalo no explicado.	1) Abrir ticket/bitácora. 2) Validar que no sea mantenimiento. 3) Congelar cambios no urgentes.	A: Jefe Ciberseguridad / R: Analista (o TI si no hay SOC)
30-90 min	Tomar control y clasificar severidad inicial	Quién ejecutó la acción, desde dónde, hay privilegios elevados, hay evidencia de acceso a datos.	Escalar a Alta/Crítica si: datos sensibles en riesgo, privilegios admin, o impacto en servicio.	1) Revisar IAM (creación/cambios/roles). 2) Revisar logs cloud/perímetro. 3) Identificar cuentas/activos afectados.	A: Gerente TI / R: TI-Plataforma + Seguridad
90-180 min	Contener riesgo activo (sin destruir evidencia)	Persistencia, accesos activos, exfiltración/cifrado/degradación en curso.	GATE-1 AISLAR/CORTAR: ejecutar si hay actividad en curso o credenciales comprometidas con privilegios.	1) Suspender cuentas sospechosas. 2) Revocar sesiones/tokens. 3) Bloqueos selectivos (IP/reglas).	A: Gerente TI / R: TI-Plataforma (C: Legal si hay datos)
3-5 h	Asegurar evidencia mínima y reducir incertidumbre	Alcance, ruta de acceso (vector), faltan logs críticos.	GATE-2 RESET: ejecutar si hay sospecha razonable de compromiso de identidad (MFA/llaves/secretos).	1) Preservar evidencias (export/snapshot). 2) Rotar credenciales admin/secretos críticos. 3) Revisar cambios de configuración.	A: Jefe Ciberseguridad / R: TI-Plataforma; C: Legal
5-8 h	Decidir erradicación / recuperación controlada	Se puede volver seguro, backups confiables, hay indicadores de reinfección/persistencia.	GATE-3 RECUPERAR: iniciar sólo si (a) amenaza contenida, (b) evidencia preservada, (c) plan de retorno seguro.	1) Plan de erradicación (causa raíz). 2) Validación pre-retorno (checkpoints). 3) Comunicación interna de estado.	A: Gerente TI / R: TI + Negocio; C: Legal/Comunicaciones

Cómo cambia el triage según severidad

- Severidad Alta: contención selectiva y evidencia mínima; war room cada 2 horas, comunicación interna acotada (need-to-know).
- Severidad Crítica: detención inmediata de actividad y protección de activos críticos, war room horario (o más frecuente), pre autorizar gates bajo criterios; preparar gatillos regulatorios y de crisis.

5.2.-Evidencia mínima requerida por tipo de fuente

Dado que Cumplo no cuenta con SIEM, la evidencia se recolecta de forma estructurada y repetible desde fuentes primarias. El objetivo es habilitar decisiones tempranas y reconstrucción básica del timeline.

Fuente	Qué buscar (alto nivel)	Salida mínima (evidencia)
IAM (Google / IdP)	Altas/bajas, cambios de roles, inicios de sesión anómalos, fallos reiterados, MFA deshabilitado	Export auditoría IAM + lista cuentas/roles + IP/origen + timestamps
Cloud (AWS)	CloudTrail/CloudWatch: cambios de configuración, creación de recursos, elevación de privilegios, acceso a S3/RDS fuera de patrón	Export logs + inventario recursos tocados + métricas de egress
Perímetro (Firewall/WAF/VPN)	IPs origen, picos de tráfico, conexiones salientes inusuales, bloqueos automáticos	Export logs relevantes + reglas activadas + lista de IPs
Aplicación	Eventos authN/authZ, operaciones sensibles (alta usuarios, permisos), acciones administrativas	Extract de logs con request-id/usuario/endpoint + timestamps
BD	Consultas masivas, cambios permisos, accesos desde orígenes no habituales, exportaciones	Auditoría o métricas + lista tablas/consultas sospechosas
Endpoints/AV (si existe)	Procesos inusuales, cifrado masivo, herramientas remotas	Alertas/detecciones + hostnames + acciones tomadas

5.3.-Regla de preservación y custodia de evidencia

Regla: antes de acciones potencialmente destructivas (reset masivo, borrado de cuentas, restauración de backups, Re imagen), preservar evidencia mínima y registrar justificación en bitácora.

Elemento	Regla
Qué se guarda	Logs originales (export), snapshots/exports cloud, configuraciones relevantes, lista de cuentas/roles y cambios, timestamps y metadatos.
Quién autoriza	Gerente TI (A). Legal es consultado si hay posible exposición de datos o requerimientos regulatorios.
Cómo se guarda	Copias íntegras de solo lectura; en lo posible con hash/chequeo; repositorio controlado y acceso restringido.
Qué no se altera	Fuentes primarias de logs, relojes de sistema, configuraciones históricas sin snapshot previo.
Cadena de custodia	Registrar: qué se tomó, quién, fecha/hora, ubicación, propósito y transferencias.

6.-Playbooks y checklists operativos

6.1.-Playbook del caso

Playbook alineado al escenario base: compromiso de identidad (IAM) que habilita creación de cuentas no autorizadas, posible escalamiento en AWS y riesgo de acceso a datos/servicios críticos. Incluye gates con criterios, dueños por acción y verificación post-remediación.

6.1 Triggers de activación

- Creación de cuentas o cambios de privilegios fuera de procedimiento (horario, volumen, rol).
- Inicio de sesión anómalo en cuentas privilegiadas (IP/geo/dispositivo no habitual) o MFA deshabilitado.
- Cambios de configuración en AWS relacionados a identidad/permisos, o accesos inusuales a S3/RDS.
- Degradación del servicio coincidente con actividad administrativa anómala.

6.2 Fases del playbook y checklists por fase

Fase 1: Detectar y confirmar

Objetivo: confirmar incidente vs falso positivo, definir alcance inicial y severidad, y decidir escalamiento.

Paso	Acción (no hiper-técnica)	Dueño (R) / Aprobador (A)	Resultado esperado
1	Abrir bitácora y declarar estado 'Incidente Potencial'	R: Analista/TI / A: Jefe Ciberseguridad	Trazabilidad y control inicial
2	Validar si la creación/cambio es esperado (ticket/ventana/aprobación)	R: TI / A: Gerente TI	Falso positivo o sospecha fundada
3	Identificar cuentas/roles afectados y actor/origen (usuario, IP, dispositivo)	R: Seguridad + TI / A: Jefe Ciberseguridad	Lista preliminar y sospecha priorizada
4	Revisar señales rápidas de impacto (datos, cloud, disponibilidad)	R: TI/Plataforma + Negocio / A: Gerente TI	Severidad preliminar (Alta/Crítica)
5	Decidir escalamiento y activar war room según severidad	R: Gerente TI / A: Gerente TI	War room activado o cierre documentado

Gate (confirmación): se declara 'Incidente Confirmado' con evidencia mínima de violación de política con riesgo material (privilegios, datos o disponibilidad).

Fase 2: Contener

Objetivo: detener actividad en curso y limitar el daño sin perder evidencia.

Paso	Acción	Dueño (R) / Aprobador (A)	Resultado esperado
1	Convocar war room y asignar roles (scribe/observador)	R: Gerente TI / A: Gerente TI	Mando y coordinación claros
2	Preservar evidencia mínima antes de cambios irreversibles	R: Seguridad / A: Jefe Ciberseguridad	Evidencia resguardada
3	Suspender cuentas no autorizadas y revocar sesiones/tokens	R: TI/Plataforma / A: Gerente TI	Riesgo inmediato reducido
4	Aplicar contención en cloud/perímetro (bloqueos selectivos, cierre de accesos admin)	R: TI/Plataforma / A: Gerente TI	Actividad hostil detenida o acotada
5	Evaluar impacto en negocio y continuidad (trade-off)	R: Negocio / A: Gerente TI	Prioridades acordadas

6	Consulta Legal si hay posible exposición de datos	R: Legal / A: Gerente TI	Ruta regulatoria preparada

Gate AISLAR/CORTAR (criterio): ejecutar aislamiento/bloqueo inmediato si hay actividad en curso, credenciales privilegiadas comprometidas o evidencia de acceso a datos/servicios críticos. Trade-off: indisponibilidad temporal vs reducción de daño.

Fase 3: Erradicar

Objetivo: eliminar la causa raíz que permitió la creación de cuentas y el uso indebido de privilegios.

Paso	**Acción**	**Dueño (R) / Aprobador (A)**	**Resultado esperado**
1	Determinar causa raíz con evidencia mínima (qué se sabe / qué falta)	R: Seguridad / A: Jefe Ciberseguridad	Hipótesis validada y registrada
2	Rotar credenciales privilegiadas y secretos críticos (priorizar integraciones)	R: TI/Plataforma / A: Gerente TI	Vector neutralizado
3	Ajustar controles de identidad: MFA, aprobación doble, least privilege	R: Seguridad + TI / A: Gerente TI	Controles reforzados
4	Revertir cambios no autorizados (roles, políticas, recursos cloud)	R: TI/Plataforma / A: Gerente TI	Configuración segura restaurada
5	Buscar persistencia: cuentas ocultas, accesos programados, claves activas	R: Seguridad / A: Jefe Ciberseguridad	Persistencia eliminada o descartada

Gate RESET (criterio): rotación masiva se ejecuta cuando la contención detuvo actividad y la evidencia mínima está preservada. Trade-off: impacto operativo por Re autenticación vs cierre del vector.

Fase 4: Recuperar y verificar

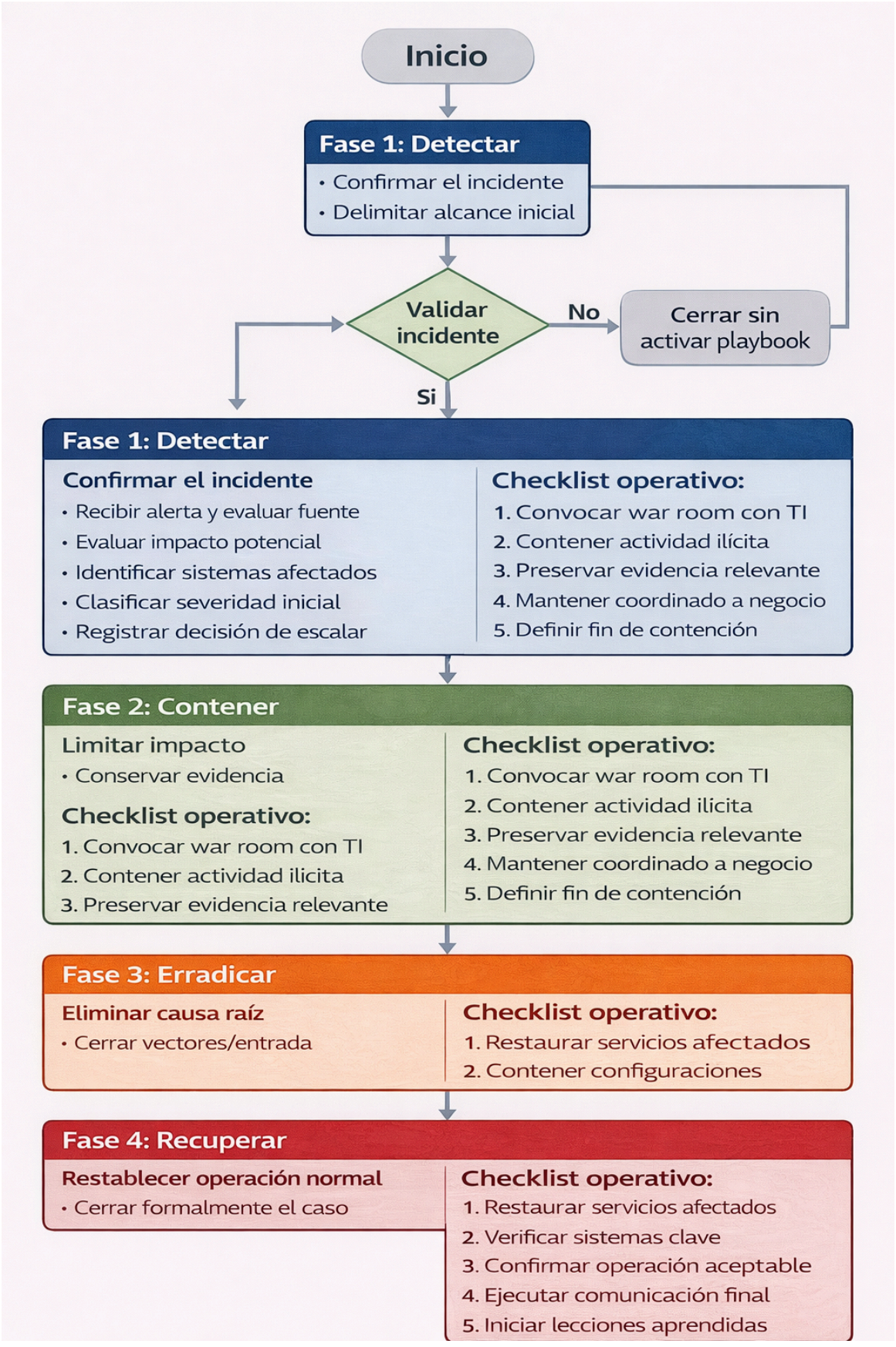
Objetivo: restablecer operación con validación de retorno seguro y controles anti-reincidencia.

Paso	Acción	Dueño (R) / Aprobador (A)	Resultado esperado
1	Validar estabilidad y priorizar retorno por criticidad	R: Negocio + TI / A: Gerente TI	Orden de recuperación acordado
2	Restaurar componentes afectados desde backup verificado (si aplica)	R: TI/Plataforma / A: Gerente TI	Servicios recuperados sin reintroducir riesgo
3	Checks anti-reincidencia 24-48h: IAM, cambios cloud, egress anómalo	R: Seguridad / A: Jefe Ciberseguridad	Reincidencia descartada
4	Confirmar cierre con evidencia (done checklist)	R: Seguridad + TI / A: Gerente TI	Cierre defendible
5	Comunicar cierre interno e iniciar AAR/lecciones aprendidas	R: Gerente TI + Comunicaciones / A: Gerente TI	Mejora continua activada

6.3 Criterios globales de 'done'

- No existen cuentas no autorizadas activas ni sesiones privilegiadas sospechosas.
- Evidencia mínima preservada con cadena de custodia y bitácora completa.
- Causa raíz corregida (controles de identidad ajustados y credenciales rotadas).
- Verificación post-remediación ejecutada (checks anti-reincidencia 24-48h).

Lecciones aprendidas iniciadas con backlog y dueños.


Inicio
Fase 1: Detectar
• Confirmar el incidente
• Delimitar alcance inicial
Validar incidente
No
Cerrar sin activar playbook
Si
Fase 1: Detectar
Confirmar el incidente
• Recibir alerta y evaluar fuente
• Evaluar impacto potencial
• Identificar sistemas afectados
• Clasificar severidad inicial
• Registrar decisión de escalar
Checklist operativo:
1. Convocar war room con TI
2. Contener actividad ilícita
3. Preservar evidencia relevante
4. Mantener coordinado a negocio
5. Definir fin de contención
Fase 2: Contener
Limitar impacto
• Conservar evidencia
Checklist operativo:
1. Convocar war room con TI
2. Contener actividad ilicita
3. Preservar evidencia relevante
Checklist operativo:
1. Convocar war room con TI
2. Contener actividad ilicita
3. Preservar evidencia relevante
4. Mantener coordinado a negocio
5. Definir fin de contención
Fase 3: Erradicar
Eliminar causa raíz
• Cerrar vectores/entrada
Checklist operativo:
1. Restaurar servicios afectados
2. Contener configuraciones
Fase 4: Recuperar
Restablecer operación normal
• Cerrar formalmente el caso
Checklist operativo:
1. Restaurar servicios afectados
2. Verificar sistemas clave
3. Confirmar operación aceptable
4. Ejecutar comunicación final
5. Iniciar lecciones aprendidas

7.-Concientización y Tabletop

El tabletop válida la respuesta de 0-8 horas al escenario base (compromiso IAM con creación de cuentas y riesgo cloud), incluyendo gates, evidencia mínima, escalamiento, roles y comunicaciones.

7.1.-Estrategia de concientización ligada a riesgos del caso

Mensajes clave:

- El compromiso de identidades privilegiadas (IAM) es un riesgo central: una cuenta equivocada puede escalar a cloud y datos.
- Los primeros 60-90 minutos definen el alcance: gates (aislar/cortar/reset) deben ser explícitos y trazables.
- Sin SIEM, evidencia mínima + bitácora reemplazan correlación: disciplina antes que herramientas.
- Continuidad vs contención: los trade-offs se deciden con negocio y se documentan.
- El ejercicio busca mejorar procesos, no evaluar personas.

Audiencias y frecuencia/canal:

Audiencia	Canal	Frecuencia	Propósito
TI/Plataforma + Seguridad	Sesión 30-45 min + guía 1 página	Previo a cada tabletop y refresco anual	Alinear gates, evidencia mínima y roles
Negocio/Liderazgo	Brief ejecutivo	Previo al tabletop	Alinear prioridades y trade-offs
Legal (y Comunicaciones si aplica)	Reunión de coordinación	Previo al tabletop	Alinear aprobaciones y gatillos

7.2 Ficha del ejercicio

Campo	Definición
Nombre	Tabletop: Compromiso de Identidad (IAM) y Creación de Cuentas no Autorizadas
Alcance	Respuesta de 0-8 horas: detección, triage, contención, erradicación inicial, comunicación interna y decisión de cierre.
Duración	90 minutos (presencial o híbrido).
Dueños	Gerente de TI (A) y Jefe de Ciberseguridad (soporte técnico).
Prerrequisitos	Roles convocados; plantillas bitácora/timeline; lista de activos críticos; set de inyectables (logs simulados).

Salidas	Timeline, decisión log, lista de acciones, brechas de evidencia, backlog de mejoras.

7.3 Público objetivo (roles) y justificación

Rol	Justificación
Gerente de TI (líder del incidente)	Decide escalamiento y gates; prioriza continuidad vs seguridad.
Jefe de Ciberseguridad	Define severidad, evidencia mínima y criterios de confirmación/descartar.
TI/Plataforma (Cloud/IAM)	Ejecuta contención, rotación de credenciales y recuperación.
Operaciones/Negocio	Evalúa impacto y define prioridades de servicio.
Legal	Define implicancias regulatorias/contractuales y custodia de evidencia.
Comunicaciones (opcional)	Mensaje interno y preparación de postura externa si escala.
Scribe	Registro de decisiones, tiempos, evidencias y responsables.
Observador	Métricas del ejercicio y brechas.

7.4 Objetivos del ejercicio

- Validar escalamiento y mando (quién decide qué y cuándo).
- Medir tiempos de decisión en gates tempranos (aislar/cortar/reset).
- Detectar brechas en evidencia mínima y trazabilidad (bitácora/timeline).
- Validar coordinación TI-Negocio-Legal para continuidad y obligaciones.

7.5 Diseño del ejercicio

- Inyectables secuenciales que obligan decisiones concretas del caso.
- Registro obligatorio: cada decisión debe tener responsable, criterio y timestamp.
- Artefactos: decisión log, timeline, lista de evidencia mínima, backlog de mejoras.

7.6 Aplicación

Minutos	Bloque	Artefacto
0-10	Contexto, reglas y roles	Roles asignados
10-25	Triage (potencial vs confirmado)	Incógnitas críticas + severidad
25-45	Contención y gates	Decisiones aislar/cortar/reset
45-65	Negocio, evidencia y legal	Evidencia mínima + trade-offs
65-80	Erradicación inicial + retorno seguro	Checklist verificación
80-90	Debrief	Backlog de mejoras

7.7 Validación de éxito

Criterio	Umbral	Evidencia
War room convocado	≤ 15 min desde confirmación	Bitácora + lista asistentes
Severidad documentada	≤ 30 min	Drivers + incertidumbre crítica
Gate AISLAR/CORTAR decidido	≤ 45 min	Decisión + criterio
Evidencia mínima preservada	≤ 60 min	Checklist + repositorio
Legal activado (si aplica)	≤ 75 min	Registro consulta + decisión
Criterio de cierre definido	≤ 85 min	Checklist done + monitoreo 24-48h
Backlog mejoras	≥ 3 ítems	Lista con dueños/plazos

7.8 Cronología del ejercicio

Hito	Inyectable (facilitador)	Decisión esperada
1. Alerta inicial detectada	Notificación: creación de cuenta admin fuera de horario	Declarar incidente potencial y abrir bitácora
2. Información incompleta	Faltan campos en el log; no hay SIEM	Definir incógnitas críticas y plan de evidencia mínima
3. Confirmación actividad anómala	Nuevo log: cambio de rol y login desde IP nueva	Confirmar incidente y estimar severidad
4. Decisión de escalar	Reporte de degradación parcial de un servicio	Convocar war room y asignar roles
5. Identificación de activos críticos	Pagos/onboarding dependen de recurso cloud afectado	Priorizar continuidad y contención
6. Presión por impacto en negocio	Negocio solicita no cortar acceso por impacto	Trade-off y criterio de gate
7. Falta parcial de logs	Logs perimetrales incompletos (retención)	Medidas conservadoras y preservar lo disponible
8. Consulta legal	Posible dato personal/financiero en riesgo	Activar Legal y definir umbral de notificación
9. Contención aplicada	Se propone bloquear cuenta/rotar credenciales	Aprobar gate y registrar evidencia previa
10. Comunicación interna	Rumores internos; se pide postura	Mensaje 'need-to-know' aprobado
11. Evaluación de cierre	Sin nuevas señales, pero incertidumbre residual	Definir criterio de done y monitoreo 24-48h
12. Inicio de lecciones aprendidas	Cierre de ejercicio	Backlog priorizado con dueños

8.-Estrategia de comunicación y aplicación al caso

8.1.-Estrategia comunicacional

La comunicación debe proteger la gestión del incidente y asegurar la coherencia del mensaje para mantener la confianza del mercado Fintech.

• **Estrategia de comunicación corporativa:**

◦ **Principios:** "Única fuente de verdad" para evitar contradicciones y transparencia controlada sin comprometer la seguridad.

◦ **Vocerías:** El CISO actúa para reportes técnicos y el Gerente de Comunicaciones para mensajes externos coordinados con Legal.

◦ **Reglas :** La información técnica sensible se restringe al equipo de respuesta; el personal general solo recibe instrucciones operativas.

◦ **Control de rumores:** Monitoreo activo de redes sociales y medios para emitir declaraciones públicas controladas.

Matriz de Comunicación ante Incidentes y Cibercrisis

Audiencia	Gatillo (Trigger)	Redacción (Drafter)	Aprobación Final (Approver)	Vocero / Remitente (Spokesperson)
Staff Interno	Detección de compromiso de identidad.	CSIRT Lead	CISO	CISO o RRHH (Email interno)
Directorio	Cambio de severidad (Media	CISO + Legal	CEO (No el CISO solo)	CEO (En reunión o Memo)
Clientes	Indisponibilidad confirmada > 2 horas.	Gerente Comms	Comité de Crisis + Legal	Comunicado Corporativo (Sin firma personal)
Prensa / RRSS	Rumor de filtración o consulta directa.	Agencia PR / Comms	CEO + Legal	Gerente de Asuntos Corporativos
Regulador (CMF)	Confirmación de impacto operacional.	Oficial de Cumplimiento	Fiscalía / Legal	Oficial de Cumplimiento (Vía SEIL/Oficio)

Aplicación al incidente por severidad:

1.**Escenario A: Severidad Media (La "Zona Gris")**

- Situación: El sitio está lento o caído, se sospecha de AWS pero no hay confirmación de ransomware.
- Gatillo Comunicacional: Consultas de usuarios por fallas de acceso.

- Mensaje Permitido: "Intermitencia técnica" o "Mantenimiento de emergencia".
- RESTRICCIÓN (Hard Constraint): PROHIBIDO usar términos como "Ciberataque", "Hackeo", "Ransomware" o "Incidente de Seguridad" hasta tener evidencia forense. Si se declara ataque prematuramente y luego fue una falla de AWS, se genera daño reputacional innecesario y pánico en inversionistas.

2. **Escenario B: Severidad Alta (Crisis Confirmada)**
   - Situación: Hallazgo de nota de rescate o cifrado de snapshots en AWS.
   - Gatillo Regulatorio: Inicio del conteo de 3 horas para alerta temprana a la CMF (Fuente).
   - Mensaje Permitido: "Incidente de Ciberseguridad que afecta la disponibilidad".
   - RESTRICCIÓN: No estimar tiempos de recuperación (RTO) públicamente (ej. "volvemos en 2 horas") hasta que el Comité lo valide. No negar exfiltración de datos ("no robaron nada") tajantemente; usar la fórmula: "No hay evidencia confirmada hasta el momento"

• Q&A Mínimo (Postura Oficial):

1. **¿Están seguros mis fondos invertidos en la plataforma?**
Respuesta: Sí. Los fondos de inversión se encuentran en **cuentas bancarias segregadas** y la plataforma actúa únicamente como intermediario tecnológico; el incidente afecta la gestión del sitio, pero no el capital resguardado en los bancos.

2. **¿Ha habido robo o filtración de mis datos personales o financieros?**
Respuesta: Actualmente, nuestro equipo de respuesta (CSIRT) está realizando una **investigación forense** para determinar el alcance del acceso no autorizado. Hasta el momento, no contamos con evidencia confirmada de exfiltración masiva, y nuestra prioridad es la contención del entorno cloud.

3. **¿Por qué no puedo acceder al sitio de inversionistas o de pagadores? Respuesta:** El sitio presenta una **degradación intermitente** debido a actividades anómalas detectadas en nuestro entorno AWS. Hemos activado protocolos de mantenimiento preventivo para asegurar que el retorno al servicio sea bajo condiciones de seguridad certificadas.

4. **¿Es verdad que la empresa ha sido víctima de un ataque de ransomware? Respuesta:** Hemos detectado actividad técnica inusual y estamos aplicando nuestro **Plan de Respuesta ante Incidentes**. Estamos trabajando con expertos externos para mitigar cualquier impacto operativo y restaurar la normalidad de los procesos críticos.

5. **Soy un pagador, ¿qué sucede si mi cuota vence y el sistema no funciona?**

Respuesta: No se preocupe. Se han definido **plazos de pago extendidos** para asegurar que ningún cliente se vea afectado en su historial crediticio o caiga en morosidad técnica debido a esta intermitencia del sistema [Matriz de Stakeholders, 227].

6. **¿Qué medidas de seguridad debo tomar como usuario de Cumplo.cl?**

Respuesta: Como medida de precaución proactiva, recomendamos a todos nuestros usuarios realizar una **rotación de sus credenciales** y asegurarse de tener activo el **Segundo Factor de Autenticación (MFA)** una vez que el servicio esté totalmente restablecido.

7. **¿Han informado de esta situación a las autoridades reguladoras?**

Respuesta: Sí. En cumplimiento con la **Ley Fintech (Ley 21.521)** y las normativas de la CMF y el CSIRT, hemos activado los protocolos de reporte de incidentes relevantes dentro de los plazos legales establecidos.

8. **¿Cuándo se espera que el servicio vuelva a la normalidad total?**

Respuesta: Estamos ejecutando una **restauración gradual** (phased restore) de los servicios tras validar la integridad de los respaldos. Mantendremos informados a nuestros clientes a través de canales oficiales cada vez que se cumpla un hito relevante de recuperación.

Recomendaciones para la vocería:

- **Principio de calma:** En ningún momento se debe mostrar pánico; la comunicación debe ser estructurada y basada en hechos.
- **Única fuente de verdad:** Solo los voceros autorizados (CISO para lo técnico, Gerente de Comunicaciones para lo externo) deben emitir estas respuestas para evitar contradicciones.
- **Gestión de incertidumbre:** Si hay datos no confirmados, se debe declarar que la investigación está en curso en lugar de dar información potencialmente falsa.

9.. **Pregunta de Trampa: ¿Van a pagar el rescate al hacker?**

Respuesta de Bloqueo: "Nuestra política corporativa es no financiar actividades ilícitas. Estamos enfocados al 100% en la recuperación técnica a través de nuestros respaldos seguros."

10. **Pregunta de Trampa: ¿De quién es la culpa? ¿Falló AWS?**

Respuesta de Bloqueo: "Estamos en etapa de investigación. Nuestra infraestructura opera bajo estándares de responsabilidad compartida y estamos colaborando con nuestros proveedores para el análisis."

Recomendaciones para la vocería

1. **Principio de calma:** En ningún momento se debe mostrar pánico; la comunicación debe ser estructurada y basada en hechos.

2. **Única fuente de verdad:** Solo los voceros autorizados (CISO para lo técnico, Gerente de Comunicaciones para lo externo) deben emitir estas respuestas para evitar contradicciones.
3. **Gestión de incertidumbre:** Si hay datos no confirmados, se debe declarar que la investigación está en curso en lugar de dar información potencialmente falsa.

9.-Stakeholders

• **Selección de Stakeholders aplicables:**
  ◦ **[X] Inversionistas:** Preocupación por integridad de fondos y acceso.
  ◦ **[X] Pagadores (Empresas):** Necesitan cumplir compromisos financieros.
  ◦ **[X] CMF (Chile):** Regulador sectorial bajo la Ley Fintech.
  ◦ **[X] CSIRT Nacional:** Autoridad de reporte de incidentes.
  ◦ **[X] AWS (Proveedor Cloud):** Crítico para la recuperación técnica.
  ◦ **[X] Bancos y Pasarelas:** Riesgo de fraude en integraciones.
  ◦ **[X] Staff Interno:** Ejecutores de la respuesta y posibles vectores.
  ◦ **[X] SERNAC:** Por potenciales reclamos de consumidores financieros.

Fase del Incidente	Stakeholder Activo	Gatillo de Entrada (Trigger)	Decisión / Acción Concreta (Hard Action)
1. Detección y Análisis (Triage)	**Staff TI / AWS**	Alerta de tráfico anómalo o detección de*ransomware note*.	**Acción:** Aislar la VPC afectada y preservar *snapshots* (evidencia) antes de apagar nada.
2. Contención (Crisis)	**Comité de Crisis (CEO/Legal)**	Confirmación de severidad Alta (afectación de disponibilidad/integridad).	**Decisión:** Autorizar la "Parada de Emergencia" de los sitios (Bajada de switch) y activar el *War Room* .
3. Notificación (Compliance)	**CMF / CSIRT / Legal**	Cumplimiento del umbral de "Incidente Operacional Relevante" (<3 horas).	**Acción:** Enviar Alerta Temprana formal (Oficio/Portal) para evitar sanciones de Ley Fintech .
4. Mitigación Financiera	**Bancos / Pasarelas**	Riesgo de movimiento lateral a sistemas de pago.	**Acción:** Suspender/Revocar las *API Keys* vigentes y congelar transferencias salientes masivas .
5. Recuperación	**Inversionistas / Pagadores**	Validación de integridad de respaldos y limpieza de*malware*.	**Decisión:** Aprobar la reapertura gradual de la plataforma (comunicación de servicio restablecido) .

Matriz Operable Top 8:

Stakeholder	Dueño de la Relación (Owner)	Decisión Crítica del Stakeholder (El "Interruptor" que controlan)	Acción Requerida Inmediata (Nuestra Respuesta/Mensaje)	Fase de Entrada (Ciclo IRT)
1. Inversionistas	Gerencia de Clientes	Corrida financiera (Bank run): Decisión masiva de retirar fondos por pánico.	Comunicar Segregación: "Sus fondos están en el banco, no en la app afectada. Su dinero está seguro" .	Contención (Al confirmar impacto visible).
2. Pagadores (Empresas)	Gerencia de Operaciones	Cese de pagos (Default): Dejar de pagar cuotas por imposibilidad técnica, generando mora.	Suspensión de Reglas: Congelar el "reloj de intereses" y multas en el sistema core; comunicar extensión de plazos .	Recuperación (Al iniciar restauración).
3. CMF (Chile)	Oficial de Cumplimiento / Legal	Sanción / Suspensión: Abrir expediente sancionatorio por incumplimiento de la Ley Fintech (21.521).	Notificación < 3h: Enviar alerta temprana formal cumpliendo el plazo legal estricto para incidentes operacionales .	Notificación (T+3h máx).
4. CSIRT Nacional	CISO	Alerta Pública / Reputación: Publicar la alerta técnica antes que nosotros o sancionar por no reportar IoCs.	Compartir TTPs: Entregar reporte técnico (hashes, IPs) sanitizado para cumplir obligación de la Ley Marco .	Análisis (Tras confirmar vector).
5. AWS (Proveedor)	Arquitecto Cloud / Infraestructura	Borrado de Evidencia: Rotación automática de logs o sobreescritura de snapshots por políticas de retención estándar.	Preservación Legal: Solicitar formalmente "Legal Hold" o snapshot manual de las instancias afectadas para forense .	Detección (Inmediato).
6. Bancos y Pasarelas	Gerente de Finanzas / CISO	Bloqueo de API: Cortar la conexión (tubería) de flujo de dinero por sospecha de fraude.	Evidencia de Limpieza: Demostrar rotación de credenciales API y aislamiento del entorno comprometido .	Contención (Al detectar compromiso).

7. Staff Interno	RRHH / Comms Internas	Filtración a Prensa: Enviar capturas de pantalla o rumores a medios/RRSS.	Protocolo de Silencio: Instrucción estricta de confidencialidad y canales seguros ("Need-to-know") .	Detección (Al iniciar Triage).
8. SERNAC	Legal / DPO	Demanda Colectiva: Iniciar acción legal por vulneración a la Ley del Consumidor (seguridad en el consumo).	Transparencia Controlada: Declarar proactivamente el estado de los datos personales (si hubo o no exfiltración) .	Post-Incidente (Al evaluar impacto en datos).

Justificación de las Acciones Seleccionadas

1. Segregación de Fondos (Inversionistas): En una Fintech, el pánico financiero es más letal que el ransomware. La acción clave no es decir "estamos arreglando el servidor", sino aclarar que el activo subyacente (el dinero) está custodio en un banco externo, desvinculando el riesgo técnico del riesgo financiero.

2. Suspensión de Intereses (Pagadores): Si los pagadores no pueden acceder al portal para pagar, el sistema automático les cobrará multas. La acción crítica es una decisión de negocio (suspender cobros) para evitar una crisis legal secundaria con las empresas deudoras.

3. Preservación Legal (AWS): En la nube, la evidencia es volátil. Si no se ejecuta la acción de preservar logs/snapshots inmediatamente, AWS rotará los registros y se perderá la capacidad de determinar la causa raíz o el alcance de la exfiltración.

4. Bloqueo de API (Bancos): Los bancos tienen sistemas de prevención de fraude automatizados. Si detectan tráfico anómalo desde Cumplo.cl, cortarán la conexión. La acción proactiva es contactar a la contraparte de seguridad del banco para coordinar la "limpieza" de credenciales antes de que ellos bloqueen preventivamente.

10.-Regulaciones y marco aplicables

Regulación / Marco	Aplica (X)	Justificación del Vínculo (Por qué aplica)	Obligaciones Activables ante el Incidente
Ley 21.521 (Ley Fintech - Chile)	**X**	Por la industria de la empresa (crowdfunding) y su supervisión por la **CMF** para asegurar la continuidad de servicios financieros .	**Reporte obligatorio** de incidentes operacionales relevantes a la CMF en plazos de alerta temprana (<3h) .
Ley 21.719 (Protección de Datos Personales)	**X**	Por el tratamiento masivo de **PII sensible** (estados financieros, datos bancarios y tributarios) en AWS .	Evaluación de brecha de datos y **notificación a titulares** si hay riesgo grave; riesgo de multas de hasta 20.000 UTM .
Ley 21.459 (Delitos Informáticos)	**X**	Por el acceso indebido, sabotaje informático (cifrado) y abuso de cuentas administrativas	**Preservación forense** de evidencia mínima (Cloud Logs, IAM logs) para persecución penal y denuncia .
CMF NCG 510	**X**	Aplica como estándar de Gobierno Corporativo y gestión de riesgos ciber para entidades financieras .	Activación del Comité de Crisis y reporte del impacto en lacontinuidad del negocio (RTO/RPO) .
GDPR (Reglamento UE)	**(1)**	Aplica solo si la plataforma opera con inversionistas que son ciudadanos de la Unión Europea .	Notificación obligatoria a la autoridad de control en 72 horas y evaluación de impacto a la privacidad.
SOX / J-SOX	**(2)**	Aplica solo si existen contratos con socios financieros en EE.UU./Japón o compromisos de control interno financiero .	Certificación de que el incidente no alteró laintegridad de los reportes financieros o estados contables.
NIST CSF 2.0	**X**	Utilizado comomarco de referencia voluntario para estructurar las capacidades de respuesta y recuperación .	Seguimiento de las funciones deRespond (RS) y Recover (RC) para asegurar un retorno seguro al servicio .

10.1.-Vínculos específicos

1. Vínculo con GDPR (1): En una Fintech multi-país como Cumplo.cl, el vínculo no es por geografía física, sino por la residencia de los titulares de datos. Si un ciudadano de la UE invierte en México o Chile a través del sitio, el incidente de exfiltración gatilla obligaciones internacionales inmediatas para evitar sanciones extraterritoriales.

2. Vínculo con SOX (2): Se declara por compromisos contractuales. Dado que Cumplo conecta inversionistas con empresas, si la data exfiltrada alimenta sistemas de reporte financiero de socios regulados en EE.UU., el incidente debe ser reportado bajo los controles de integridad de datos de la sección 404 de SOX.

3. Obligaciones de Evidencia: Ante el abuso de identidades Google/AWS, el CSIRT tiene la obligación de extraer y proteger logs de CloudTrail y registros de autenticación antes de que roten, para cumplir con el estándar de "evidencia mínima" exigido por el regulador y para el análisis de causa raíz (RCA).

4. Coordinación Legal: Se debe activar una célula legal para revisar los SLA con bancos y pasarelas de pago. El incidente podría forzar la suspensión de APIs bancarias si no se garantiza la rotación de llaves de acceso comprometidas.

Cronograma Maestro de Respuesta (Playbook Integrado)

Tiempo (T+)	Estado / Severidad	Obligación Regulatoria (Ley/Norma)	Acción Comunicacional y Operativa
T + 0h	**Detección** (Severidad Media)	**Ley 21.459 (Delitos Inf.):** Deber de preservar evidencia (logs). No borrar rastros al contener.	**Interno:** CISO instruye "congelar cambios" y preservar logs de CloudTrail .**Externo:** Silencio o "Mantenimiento preventivo" (si se cae el sitio).
T + 2h	**Confirmación** (Severidad Alta)	**CMF NCG 510:** Activación formal de la continuidad del negocio.	**Directorio:** Se convoca al Comité. Se confirma Ransomware.**Operativo:** Se ejecuta desconexión de integraciones bancarias riesgosas.
T + 3h	**Notificación Temprana**	**Ley 21.521 (Fintech):** Reporte de Alerta Temprana a la CMF (Plazo fatal 3h) .	**Regulador:** Envío de formulario preliminar (solo hechos confirmados).**Clientes:** Comunicado de "Incidente de Ciberseguridad" (sin detalles técnicos) .

T + 24h	**Reporte Detallado**	**CSIRT / CMF:** Entrega de reporte técnico con IoC (Indicadores de Compromiso) y TTPs.	**Regulador:** Envío de detalle de afectación.**Legal:** Evaluación preliminar de *Data Breach* (Ley 21.719) para decidir si se notifica a titulares .
T + 72h	**Evaluación Global**	**GDPR (Si aplica):** Notificación a autoridad europea si hay ciudadanos UE afectados .	**Público:** Actualización de estado de recuperación.**Legal:** Decisión sobre notificación individual a clientes basada en riesgo de derechos.

11.-Gestión de crisis (cibercrisis)

Una cibercrisis se define como un incidente de ciberseguridad, que supera la gestión operativa normal y amenaza la continuidad del negocio, la confianza del mercado o el cumplimiento regulatorio de la organización.

En los siguientes puntos se revisará cuando un incidente se deberá manejar como cibercrisis, los integrantes del comité con sus responsabilidades, roles y una agenda guía, que puede ser modificada por el mismo comité, según la evaluación del incidente.

11.1 Confirmación de cibercrisis

Si durante un incidente, se cumple alguna de las siguientes condiciones, se deberá tratar el caso como una cibercrisis, lo que implica activar el comité de cibercrisis (que se indicará en el punto 11.2) :

A.- Indisponibilidad de servicios críticos: (> 30 minutos en horario hábil, >120 minutos fuera de ese horario)

- Impacto en el sitio web de cumplo.cl, en la pasarela de pago o la información en ella.
- Afecta a más de un 30% de usuarios de la compañía.
- Afecta a más de un 25% de clientes.
- Genera pérdida de ingresos/liquidez.

B.- Confirmación de exposición de datos (personales o financieros)

- Acceso no autorizado a los datos de clientes
- Cualquier evidencia de exfiltración confirmada

C.- Incapacidad de contener en menos de 2 horas.

- Persistencia operacional de un atacante sin solución
- Continua propagación posterior al umbral
- Degradación de algún servicio posterior a la contención.

D.-Activación de obligaciones regulatorias

- Ley 21.663, obligación de comunicar el incidente al regulador.
- Ley 21.719, obligación de notificar a afectados.
- Investigación fiscal o supervisión del regulador.

E.-Impacto reputacional pública o extorsión.

- Publicación en medios de “datos expuestos”, “ataque de Ransomware”, “Fraude” sobre cumplo.cl.
- Mensajes creíbles de extorsión de publicación de datos sensibles.
- Fuga masiva de clientes o pánico en el mercado.

Matriz de escalamiento:

Escenario	Severidad	¿Desencadena crisis?	Activar
Alerta técnica aislada(anomalía sin impacto)	Baja	No	Área de ciberseguridad
Incidente contenido en <1hora sin datos expuestos	Media	No	Jefatura de ciberseguridad
Indisponibilidad 15–30 min + contención clara	Media-Alta	Condicional	Jefatura de ciberseguridad
Indisponibilidad >30 min hábil, > 2 horas inhábil ó datos en riesgo	Alta	Sí	Comité cibercrisis
Exfiltración confirmada o requerimiento regulatorio inmediato	Crítica	Sí	Comité cibercrisis

11.2 Comité de cibercrisis.

El Comité de Cibercrisis es un órgano temporal, activado bajo las condiciones del punto 11.1 por el Gerente de TI en su rol de CISO, este comité reemplaza la cadena de mando operativa normal del área de ciberseguridad con una autoridad ejecutiva real para tomar decisiones transversales. Se definirán los roles, integración y responsabilidades al activarse.

Integrantes permanentes durante todo el incidente:

Rol	Cargo en la compañía	Responsabilidad
Presidente	CEO (COPO en su reemplazo)	Titular de decisiones
Vicepresidente	Gerente TI (por su doble rol de CISO)	Gestion del incidente
Legal	Gerente legal	Asesor legal y protección de privacidad
Comunicaciones y RRHH	Gerente de RRHH	Comunicaciones corporativas y externas, gestión de personal
Continuidad TI	Gerente TI	Continuidad operativa tecnológica
Negocio y Operaciones	COPO	Asesor para la continuidad del negocio y operacional
Finanzas	CFO	Viabilidad financiera de las decisiones

En casos donde se requiera, el comité puede incluir temporal o permanentemente un asesor externo especialista en la labor que se necesite.

Responsabilidades específicas:

Presidente (CEO o COPO en su reemplazo)

- Tiene la autoridad de la toma de decisiones, especialmente las de trade-offs
- Responsable ante la junta directiva.

Vicepresidente (Gerente de TI, por su doble rol de CISO)

- Entregar la información técnica del caso.
- Proponer opciones de contención con sus respectivos riesgos y tiempos límites.
- Es el vocero técnico frente al regulador.

- Validar las evidencias del incidente.

Legal

- Evaluar y activar a las partes que deban cumplir las obligaciones frente a los reguladores (Ley 21.719 “Protección de datos”, Ley 21.663 “Marco de ciberseguridad”, Ley 21.521 “Ley Fintech”, etc.).
- Asesorar sobre los tiempos y contenido comunicacional legal.
- Coordinar con las autoridades regulatorias.
- Coordinar con las autoridades policiales, en los casos que lo ameriten.
- Actuar como abogado de la compañía en los casos que sea necesario.

Comunicaciones y RRHH:

- Diseñar la narrativa de las comunicaciones de forma consistente, con el apoyo legal (Legal) y técnica (CISO) para los diferentes destinatarios (reguladores, inversionistas, clientes, empleados, medios).
- Monitoreo de redes sociales y prensa para detectar rumores e información del caso.
- Tomar las acciones necesarias sobre personal interno según corresponda (negligencia, incumplimiento de NDA).

Continuidad TI:

- Liderar esfuerzos de recuperación y validación de los servicios.
- Proponer orden de recuperación de los servicios, según la criticidad y dependencias.
- Coordinar con los proveedores TI y las pasarelas de pago, las acciones de contención, mitigación y recuperación.
- Garantizar la viabilidad técnica de las decisiones tomadas en el comité

Finanzas:

- Informar viabilidad financiera de las decisiones
- Gestionar los gastos durante la cibercrisis.

11.3.- Agenda del Comité.

A continuación, se presenta una agenda para tomar de referencia durante una cibercrisis, esta puede ser modificada durante el incidente para ajustarse a cada caso, el Gerente de TI (en su rol de CISO) deberá preocuparse de activar que se siga esta agenda, con sus respectivos resultados esperados.

Sesión 0 (Activación dentro de los primeros 30 minutos):

- El gerente de TI (en su rol de CISO), debe presentar la evidencia inicial y clasificar la severidad del incidente.
- Se debe definir qué se sabe y qué se asume.
- Confirmar si la situación se escala como cibercrisis o descender nuevamente a incidente.

Sesiones periódicas (cada 2-4 horas mientras dure la cibercrisis, mínimo 1 vez diaria):

- Estado de contención (¿se detuvo el ataque?)
- Estado de recuperación (¿cuándo se restauran servicios?)
- Evaluación de alcance (¿cuántos datos afectados?)
- Avance de investigación (¿quién fue? ¿por qué?)
- Estado con los reguladores (¿Se está cumpliendo con la ley?)

11.4.-Alcance del comité

El comité tendrá las siguientes atribuciones:

- Tomar decisiones de trade-off (Continuidad vs seguridad).
- Decisiones de comunicación pública (Cuando informar y a quienes, cuánto detalle de la situación).
- Coordinación con reguladores.
- Autorización de gastos.
- Priorización del negocio y la operación.

El comité no tendrá las siguientes atribuciones:

- Decisiones técnicas de contención, aislamiento, bloqueo, etc. (área de seguridad)
- Trabajos de recuperación de la información. (área de IT)
- Análisis forense del caso ((área de seguridad)

12.- Recuperación y continuidad (DR/BC).

Frente a un incidente que abarque varios sistemas, se deben priorizar por criticidad del negocio, esto para que los esfuerzos sean eficientes y realizado con el personal limitado que se tiene frente a la respuesta de incidentes.

Las labores de recuperación serán responsabilidad del gerente de TI y ejecutado por el área de TI.

12.1 Estrategia de recuperación.

La estrategia de recuperación se basa en una mirada de continuidad del negocio, colocando el sitio web, con sus diferentes servicios, como prioritarios.

Prioridad	Servicio	Descripción	Dependencias	RTO(h)
1	Sitio Pagadores	Portal para pago de inversiones/préstamos	BD Pagos + AWS +Banco	2
2	Sitio Inversionistas	Portal de consulta de inversiones	BD Inversionistas+ AWS + Banco	2
3	Resto de Página Web.	Marketing + información pública	AWS	4
4	Herramientas Internas	Identidado, Correo, VPN, Buk,reportes	Google IAM. Gmail. BUK	8

12.2 Criterios de retorno seguro.

Antes de validar que es seguro volver el servicio, se debe validar que la recuperación de la información se realizó de forma confiable y segura, además de evitar que el incidente no afecte a los servicios entregados como “ya recuperados”.

A.-Integridad técnica:

- Si hubo recuperación de un respaldo, se debe validar que la información recuperada sea consistente con el respaldo (validación de checksum), además, se debe informar al Gerente TI la fecha del respaldo recuperado, para tomar las acciones respectivas al delta faltante.
- Revisar que las aplicaciones recuperadas levanten sin errores, esto validando los logs de cada una.
- Validar la interconexión entre los diferentes sistemas (conexión a las bases de datos, autenticación, etc)

- Rotar credenciales para evitar persistencia.

B.-Seguridad

- Validar que los sistemas de seguridad local estén funcionando (Windows defender, etc)
- Revisión de logs para verificar si hay intentos de sesión sospechosos
- Validar los usuarios del sistema y sus permisos, confimando que no existan permisos sospechosos o usuarios no esperados.
- Permisos de firewalls acotados a lo mínimos necesarios.

C.-Funcionalidad

- Realizar test básico de funcionalidad, validando el Login al sistema, realizar consultas de prueba y validando las respuestas.
- Realizar un test medio con algún usuario real del sistema, validando las diferentes opciones del sistema.
- Revisar el performance del sistema, velocidad de respuesta de las consultas.

D.-Coordinación con terceros (si aplica)

- Validar con los proveedores si las credenciales de conexión desde cumplo fueron cambiadas y aplicar el cambio de forma local (ejemplo pasarela de pago)
- Realizar una transacción de prueba con al menos un banco.

12.3 Riesgos de acelerar la recuperación

Siempre es deseable que la recuperación sea casi inmediata, pero no tomar los resguardos del punto 12.2 nos puede exponer y alargar el estado de incidente, al ocurrir persistencia de los atacantes o nueva propagación del ataque, por otro lado, el no recuperar las funciones dentro de un tiempo acotado, nos puede llevar a la pérdida de clientes al preferir alguna alternativa a nuestra empresa, además de pérdida de credibilidad y confianza.

A continuación, se presenta una tabla con algunos ejemplos.

Decisión	Riesgo de acelerar	Riesgo de demorar
Restaurar sitios pagadores	Reinfección: malware persiste en backup o en nuevos cambios durante restauración	Pérdida de liquidez, presión de clientes, impacto de mercado
Activar transacciones sin validar cambio de credenciales	Atacante sigue usando cuentas antiguas para manipular fondos o acceder a datos	Clientes sin servicio, fuga de clientes
Restaurar sin aislar componentes comprometidos	Propagación: atacante salta a infraestructura "limpia" durante la recuperación	Mayor tiempo de indisponibilidad
Reabrir APIs sin verificar bancos/pasarelas	Inconsistencia de datos, transacciones huérfanas, disputas contractuales	Funcionalidad incompleta, falta de credibilidad

13.- Métricas/KPIs, SLAs y mejora continua

Las métricas (como KPI y SLA) permiten evaluar de forma objetiva, la respuesta a los incidentes frente a los tiempos esperados, lo que facilita planificar mejoras continuas, optimizar recursos y evidenciar resultados medibles ante la alta dirección.

13.1 KPI

Los siguientes KPI nos ayudarán a medir la eficiencia de las diferentes etapas de la respuesta de incidentes:

Etapa 1: Preparación (pre-incidente)

KPI 1.1: Cobertura de herramientas de detección

- Definición: % de activos críticos (BD, APIs, instancias EC2) con logging habilitado
- Target: 100% (Cloud Logs en AWS, Firewall logs, Antivirus en endpoints)
- Línea base Cumplo: ~70% (Cloud Logs + Firewall)
- Acción: Implementar SIEM básico y EDR en servidores críticos en los próximos 12 meses

KPI 1.2: Viabilidad de DR/BC

- Definición: % de servicios críticos con backup verificado (test de restauración exitoso) realizado de forma semestral.
- Target: 100%
- Línea base Cumplo: ~40% (backups existen, pero no se prueban regularmente)
- Acción: Calendario de restore test semestral para cada servicio crítico

KPI 1.3: Completitud de runbooks

- Definición: % de escenarios de IR con playbook documentado (>5 pasos, responsables claros)
- Target: 80% de escenarios principales (ransomware, exfiltración, compromiso IAM)
- Línea base Cumplo: ~50%
- Acción: Desarrollar playbooks en próximas 4 semanas

Etapa 2: Detección (cuando sucede el incidente)

KPI 2.1: MTTD (Mean Time To Detect)

- Definición: Tiempo desde inicio del ataque (T0) hasta primera alerta técnica
- Target: <1 hora para actividades anómalas en AWS; <30 min para malware
- Línea base Cumplo: ~45 min (fue detectado por picos de acceso en Cloud Logs)
- Acción: Mejorar sensibilidad de alertas; agregar SIEM para correlación más rápida

KPI 2.2: Precisión de clasificación inicial

- Definición: % de incidentes clasificados correctamente en severidad en triage (sin cambios de clasificación en primeras 2h)
- Target: 90%
- Línea base Cumplo: N/A (primer incidente de esta magnitud)
- Acción: Entrenar CSIRT en triage usando matriz de severidad

KPI 2.3: Completitud de evidencia en primeras 2 horas

- Definición: % de fuentes de evidencia capturadas sin pérdida (Cloud Logs, Firewall, Correo, Antivirus)
- Target: 100%
- Línea base Cumplo: ~80% (se capturaron logs, pero retención limitada en algunos sistemas)
- Acción: Aumentar retención en Cloud Logs a 90 días; implementar captura centralizada

Etapa 3: Análisis y contención

KPI 3.1: MTTA (Mean Time To Acknowledge)

- Definición: Tiempo desde alerta técnica hasta respuesta operativa documentada (primer técnico se presenta)
- Target: <15 min (24/7)
- Línea base Cumplo: ~30 min
- Acción: Establecer SLA de on-call; mejorar automatización de alertas

KPI 3.2: MTTC (Mean Time To Contain)

- Definición: Tiempo desde confirmación de compromiso hasta aislamiento/bloqueo del atacante
- Target: <2 horas (Severidad Alta); <1 hora (Crítica)
- Línea base Cumplo: ~2.5 horas (se tardó en confirmar persistencia y aplicar bloqueos)
- Acción: Pre-autorizar cambios de seguridad urgentes; acelerar coordinación con AWS

KPI 3.3: Precisión de alcance

- Definición: % de activos afectados identificados correctamente en las primeras 4 horas (sin sorpresas posteriores)
- Target: 95%
- Línea base Cumplo: ~70% (inicialmente no se sabía si datos fueron exfiltrados o solo ransomware)
- Acción: Mejorar análisis forense; implementar DLP para detectar egress

KPI 3.4: Brechas de contención

- Definición: Número de veces que el atacante logró evadir controles después de aplicada primera medida de contención
- Target: 0 brechas
- Línea base Cumplo: 0 (en este caso no hubo re-entrada)
- Acción: Mantener vigilancia en logs post-contención

Etapa 4: Recuperación

KPI 4.1: MTTR (Mean Time To Restore)

- Definición: Tiempo desde aprobación de inicio de recuperación hasta servicio crítico operativo (con transacciones)
- Target: <4 horas para Sitio Pagadores; <6 horas para Sitio Inversionistas
- Línea base Cumplo: TBD (dependerá de ejecución real)
- Acción: Pre-validar backups; automatizar pasos de restauración

KPI 4.2: Completitud de validación pre-activación

- Definición: % de checkpoints de seguridad completados antes de reactivar transacciones (integridad, credenciales, logs limpios)
- Target: 100%
- Línea base Cumplo: ~80% (se validó integridad, pero no rotación completa de credenciales en todos los sistemas)
- Acción: Crear checklist formal y blindar proceso de aprobación

KPI 4.3: Pérdida de datos post-recuperación

- Definición: Número de transacciones inconsistentes o huérfanas detectadas post-recuperación
- Target: 0 (< 0.01% de volumen total si no es evitable)
- Línea base Cumplo: TBD
- Acción: Conciliación forzosa con bancos/pasarelas; auditoría de BD

KPI 4.4: Cumplimiento de RTO

- Definición: % de servicios críticos restaurados dentro de RTO comprometido (Sitio Pagadores < 2h desde decisión de recuperar)
- Target: 100%
- Línea base Cumplo: Dependerá de ejecución
- Acción: Monitoreo en tiempo real; autorización pre-firmada para gastos de respuesta urgente

Etapa 5: Cierre y lecciones aprendidas

KPI 5.1: Completitud de AAR (After Action Review)

- Definición: % de preguntas del template de AAR contestadas y documentadas (<5 días post-incidente)
- Target: 100%
- Preguntas mínimas: ¿Qué pasó? ¿Cuándo nos dimos cuenta? ¿Qué hicimos mal? ¿Qué hacemos diferente?
- Línea base Cumplo: 0 (aún no hay AAR)
- Acción: Facilitar sesión de AAR dentro de 3 días; documentar

KPI 5.2: Implementación de hallazgos

- Definición: % de recomendaciones de AAR que pasan de "plan de acción" a "implementado" en 90 días
- Target: 70% de quick wins; 30% de cambios estructurales en 6 meses
- Línea base Cumplo: 0 (primer incidente)
- Acción: Asignar dueños de acción; seguimiento trimestral

KPI 5.3: Mejora de MTTD post-aprendizaje

- Definición: Reducción de MTTD comparando incidentes similares (p. ej., 45 min en primer incidente → <20 min en incidentes posteriores)
- Target: 50% de reducción en 6 meses
- Línea base Cumplo: 45 min (actual)
- Acción: Implementar recomendaciones de herramientas (SIEM, EDR)

SLAs del proceso: tiempos objetivo y cumplimiento

13.2 SLA

Los SLA nos permitirán establecer compromisos medibles para la respuesta de incidentes

SLA 1: Respuesta inicial (On-call activado)

- Tiempo objetivo: <15 minutos desde alerta crítica
- Métrica: MTTA
- Cumplimiento esperado: 95%
- Consecuencia incumplimiento: Revisión de esquema de on-call; escalada a ejecutivos

SLA 2: Confirmación de incidente

- Tiempo objetivo: <1 hora desde alerta hasta clasificación de severidad
- Métrica: Tiempo desde T0 a CSIRT confirma "esto es incidente"
- Cumplimiento esperado: 90%
- Consecuencia: Retraso en activación de comité; impacto en decisiones tempranas

SLA 3: Contención de Severidad Crítica

- Tiempo objetivo: <2 horas desde confirmación hasta atacante bloqueado
- Métrica: MTTC
- Cumplimiento esperado: 85% (depende de complejidad técnica)
- Consecuencia: Potencial expansión del incidente; propagación a otros sistemas

SLA 4: Notificación a stakeholders internos

- Tiempo objetivo: <1 hora desde confirmación de incidente (CISO notifica CEO/Directorio)
- Métrica: Tiempo desde incidente confirmado a email/reunión de actualización enviada
- Cumplimiento esperado: 100%
- Consecuencia: Sorpresas en junta directiva; gestión de crisis fuera de control

SLA 5: Recuperación de servicios críticos (Sitio Pagadores)

- Tiempo objetivo: <4 horas desde aprobación de recuperación a operativo
- Métrica: MTTR
- Cumplimiento esperado: 80% (depende de integridad de backups, validaciones)
- Consecuencia: Prolongación de indisponibilidad; presión en clientes

SLA 6: Reporte a reguladores (si aplica)

- Tiempo objetivo: <24 horas desde confirmación de exposición de datos
- Métrica: Notificación a CMF/CSIRT/SII
- Cumplimiento esperado: 100% (obligatorio)
- Consecuencia: Sanción regulatoria; desconfianza de supervisores

SLA 7: Comunicación externa (clientes)

- Tiempo objetivo: <4 horas desde decisión de comunicar (aprobada por Comité) a mensaje en canales públicos
- Métrica: Tiempo desde aprobación a publicación de comunicado
- Cumplimiento esperado: 90%
- Consecuencia: Rumores sin control, información falsa

13.3.- After Action Review

El After Action Review nos permite determinar las lecciones aprendidas durante el incidente, asi poder prepararnos para evitar la nueva ocurrencia de este y/o mejorar las acciones de respuesta, este se realizará 2–5 días después de cierre técnico del incidente y responderá a preguntas objetivas:

1. ¿Qué planeamos que sucediera?

    - Servicios operativos 24/7 sin interrupciones
    - Controles de seguridad (IAM, firewall) previniendo acceso no autorizado
    - Detección automática de anomalías en <1 hora

2. ¿Qué realmente sucedió?

    - Acceso no autorizado a cuenta administrativa comprometida
    - Instalación de ransomware en componentes críticos de AWS
    - Indisponibilidad parcial de sitios pagadores/inversionistas por ~2 horas
    - Incertidumbre sobre exposición de datos por ausencia de DLP

3. ¿Por qué hubo diferencias? (causa raíz)

    - Debilidad: Sin SIEM → correlación de eventos manual, más lenta
    - Debilidad: Sin DLP → no se puede confirmar rápidamente si datos fueron exfiltrados
    - Debilidad: Backup no testeado recientemente → riesgo de restauración lenta
    - Acierto: Cloud Logs habilitados → permitieron reconstrucción

4. ¿Qué mantenemos igual? (aciertos)

    - Respuesta operativa del CSIRT fue ordenada y coordinada
    - Cloud Logs proporciona evidencia suficiente
    - Comunicaciones internas ejecutivas actualizadas cada 2 horas

5. ¿Qué haremos diferente?

ID	Hallazgo	Prioridad	Quick win	Estructural
H1	Falta de supervisión de uso de cuenta privilegiada	Crítica	Implementar alerta de uso de cuenta privilegiada y rotación continua de estas credenciales	Política IAM global
H2	SIEM inexistente	Alta	Evaluar herramientas en 1 mes	Implementación 3–6 meses
H3	DLP no implementado	Alta	Scoping de datos sensibles en AWS (1 mes)	Implementación 6 meses
H4	Respaldos sin validación periódica	Media	Crear calendario de pruebas de restauración (semestrales)	Automatizar validación
H5	Playbooks de IR incompletos	Media	Documentar ransomware + compromiso IAM (2 sem)	Biblioteca de 10+ playbooks en 3 meses

13.4.- Backlog

A continuación, se definen los trabajos que, luego del incidente, se vieron como puntos de mejora y cómo se implementarán.

Quick Wins (implementación 0–4 semanas)

Supervisión de cuentas privilegiadas (1–2 semanas)

- Implementar un PAM para la administración y protección de credenciales
- Aumentar los requisitos para las contraseñas de cuentas privilegiadas
- Validación: Reporte de uso y rotación de estas cuentas

Calendario de restore test (1 semana)

- Crear schedule: 1 test por servicio crítico cada 30 días
- Responsable: TI / Continuidad
- Evidencia: acta de prueba con fecha, resultado (OK/Fallido), tiempo de restauración

Documentar 3 playbooks clave (2 semanas)

- Playbook: Ransomware en AWS
- Playbook: Compromiso de cuenta privilegiada
- Playbook: Exfiltración de datos
- Formato: 5–10 pasos, roles, decisiones clave, evidencia a capturar

Scoping de datos sensibles en AWS (1–2 semanas)

- Inventario: dónde están datos personales/financieros exactamente
- Clasificación: PII, datos financieros, datos tributarios
- Baseline para futura implementación de DLP

Cambios estructurales (4–12 meses)

Implementar SIEM básico (6–12 meses)

- Opción: Splunk, ELK, o servicio AWS native (CloudWatch Insights)
- Integraciones: Cloud Logs, Firewall, Antivirus, Google AIM
- Reglas de correlación mínimas: accesos administrativos anómalos, picos de lectura de BD, cambios de permisos

Implementar EDR (Endpoint Detection & Response) (6–8 meses)

- Cobertura: servidores críticos en AWS + on-premises
- Capacidades: detección de comportamiento anómalo, aislamiento de endpoints, respuesta automatizada
- Opción: CrowdStrike, Microsoft Defender, Wazuh

DLP (Data Loss Prevention) (8–12 semanas)

- Objetivo: detectar exfiltración de datos en tiempo real
- Scope inicial: datos personales/financieros en S3 y RDS
- Tipo: Network DLP (monitoreo de egress) + Endpoint DLP (copia a USB, correo)

Endurecimiento de IAM (4–8 semanas)

- Audit: revisar todos los roles y permisos en AWS
- Aplicar "least privilege": eliminar permisos excesivos
- Segmentación: roles separados por función (desarrollo, operación, auditoría)
- Break-glass: cuenta de emergencia con aprobación manual para accesos críticos

Runbooks y capacitación (4–6 semanas)

- Biblioteca: 10+ playbooks documentados (ransomware, exfiltración, DDoS, fraude, etc.)
- Capacitación: 2 sesiones hands-on para CSIRT + TI
- Drill trimestral: simulación de incidente de severidad Alta