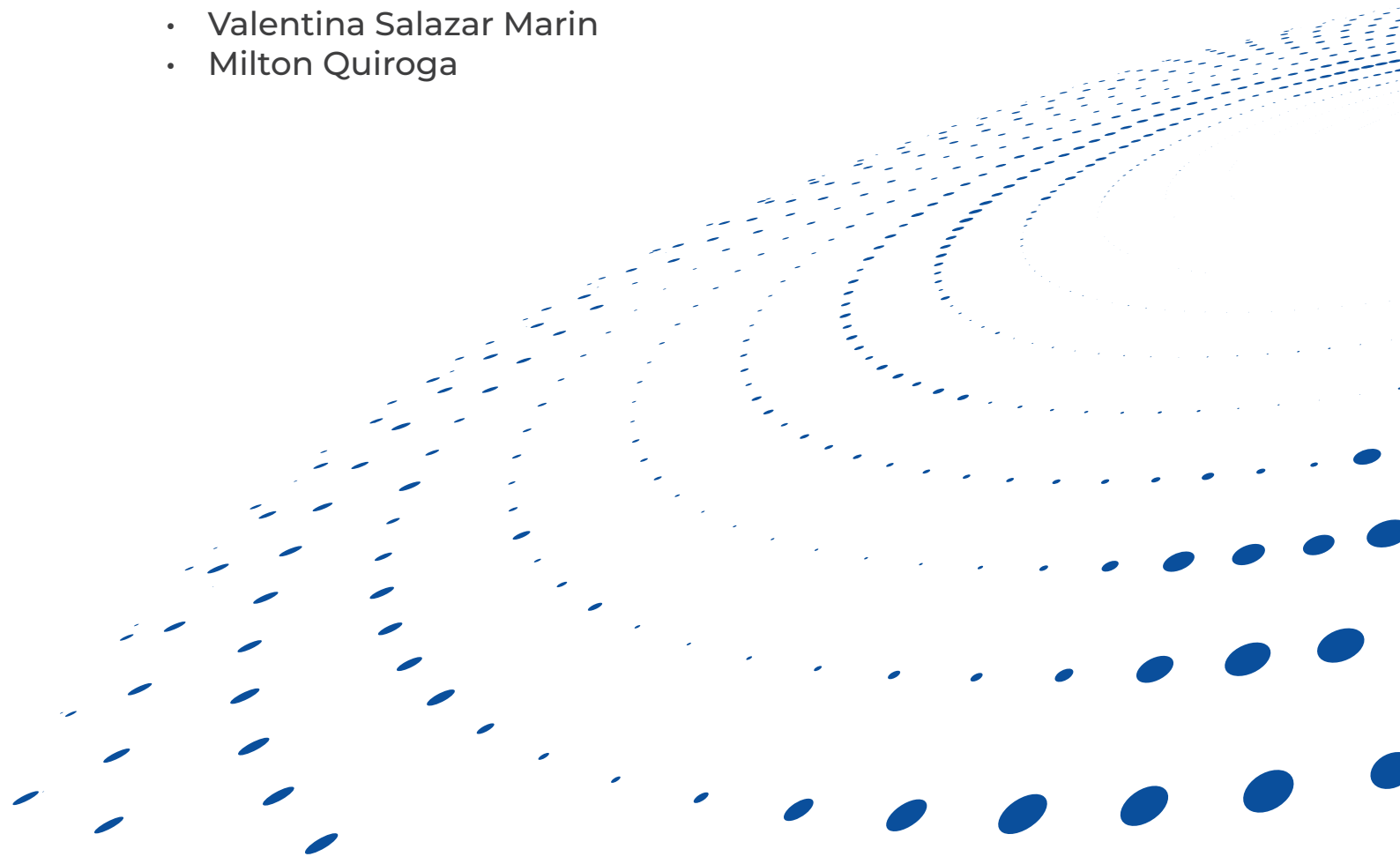
FLAR
FONDO LATINOAMERICANO DE RESERVAS

Marco regional de respuesta a incidentes y resiliencia cibernética

Guía técnica para gobierno, detección automatizada, clasificación estratégica, respuesta coordinada y cooperación interinstitucional

Autores:

- Fondo Latinoamericano de Reservas - FLAR
- Bancos centrales miembros
- Valentina Salazar Marin
- Milton Quiroga



Índice general

Índice de tablas

Introducción

En un entorno marcado por la creciente sofisticación y persistencia de las amenazas cibernéticas, la capacidad de los bancos centrales y demás instituciones financieras para responder con eficacia a los incidentes y sostener su resiliencia operativa se ha convertido en un imperativo estratégico. Tal exigencia no solo obedece a la necesidad de custodiar los activos y la información crítica de cada entidad, sino que constituye un pilar fundamental para preservar la estabilidad y la confianza en el sistema financiero regional en su conjunto.

La presente guía se concibe como un instrumento de referencia práctico y accionable, diseñado para que los bancos centrales puedan utilizarlo como una herramienta de autodiagnóstico, acoplar sus contenidos a las particularidades de su contexto regulatorio y tecnológico e implementar mejoras de manera progresiva. Así, sus objetivos centrales son tres: en primera instancia, colocar a disposición un esquema estructurado alineado con estándares internacionales (NIST SP 800-61, ISO/IEC 27035 y el CERT-RMM), el cual describa las fases esenciales del ciclo de vida de un incidente; en segundo término, proporcionar plantillas, flujogramas y listas de verificación, de modo que cada entidad pueda examinar su propio nivel de madurez, reconocer brechas y gestionar esfuerzos con plena autonomía; y, en tercer lugar, establecer una nomenclatura uniforme y un lenguaje operativo común que favorezcan el intercambio de información y la cooperación intrarregional, elementos imprescindibles para anticipar amenazas sistémicas en la infraestructura financiera.

El alcance del documento abarca seis dominios críticos que articulan la disciplina de atención a incidentes: gobernanza, detección automatizada, declaración y clasificación, respuesta y recuperación, recopilación de lecciones aprendidas y comunicación interinstitucional. Se reconoce que cada organización posee una postura de ciberseguridad y unos recursos distintos, por lo que la guía se ha elaborado de forma modular, permitiendo a cada una priorizar las áreas de mayor necesidad o impacto.

Consolidada así, esta obra aspira a convertirse en una brújula técnica y normativa que cada banco central pueda consultar, integrar y escalar en consonancia con su realidad institucional, fortaleciendo capacidades individuales y colectivas, al tiempo que promueve una cultura de preparación, respuesta coordinada y aprendizaje continuo.

1 Gobernanza y revisión continua en el ciclo de incidentes

La resiliencia cibernética de un banco central descansa en una gobernanza sólida y en un proceso de gestión de incidentes concebido como una función estratégica, no como un ejercicio reactivo aislado. Este dominio establece los lineamientos para que las entidades participantes consoliden marcos de decisión claros, roles definidos, mecanismos de coordinación interna y regional, así como un ciclo de actualización continua alineado con los estándares internacionales y con los requerimientos normativos latinoamericanos.

1.1 Propósito, alcance y principios rectores

La atención de incidentes en bancos centrales y entidades conexas debe concebirse como una capacidad institucional permanente, vinculada con el sistema integral de administración de riesgos, los esquemas de continuidad de las operaciones, las infraestructuras tecnológicas, las funciones de ciberseguridad, las instancias jurídicas, los equipos de comunicación estratégica y los órganos de dirección superior. Por ende, este eje no se limita a procedimientos técnicos, sino que configura un componente estructural de la gobernanza corporativa y de la protección de la estabilidad financiera, sustentándose en los siguientes principios rectores:

- **Enfoque basado en el riesgo sistémico**: privilegiar la atención a situaciones con capacidad de comprometer los sistemas de pago, la salvaguarda de información clasificada, las operaciones de mercado abierto, los mecanismos de provisión de liquidez o la credibilidad de la moneda y de la institución emisora.
- **Responsabilidad y trazabilidad institucional** (*accountability and traceability*): establecer estructuras formales, mandatos inequívocos, líneas de autoridad definidas y registros verificables que documenten decisiones, coordinaciones interáreas y actuaciones emprendidas durante todo el ciclo del evento.

- **Integración con directrices internacionales**: armonizar políticas, protocolos y guías internas con estándares ampliamente reconocidos, con el propósito de evitar superposiciones normativas, facilitar la interoperabilidad entre jurisdicciones y fortalecer la comparabilidad de las prácticas implementadas.
- **Proporcionalidad y escalabilidad**: calibrar controles, tiempos de respuesta, estructuras organizativas y recursos especializados de acuerdo con el entorno institucional, el grado de complejidad tecnológica y el perfil de amenazas específico, preservando un umbral mínimo común de competencias esenciales.
- **Mejora continua**: incorporar de manera sistemática los resultados de ejercicios de simulación, eventos reales, auditorías internas y externas, diagnósticos de madurez, evaluaciones de desempeño y modificaciones regulatorias, con el fin de optimizar la eficacia del proceso y reducir vulnerabilidades recurrentes.

A partir de estos lineamientos, se estructuran los capítulos subsiguientes, los cuales desarrollan capacidades especializadas de detección temprana (Capítulo 2), criterios de clasificación y umbrales de escalamiento (Capítulo 3), mecanismos de respuesta y recuperación coordinada (Capítulo 4), esquemas de aprendizaje organizacional (Capítulo 5) y arreglos de colaboración interinstitucional y regional (Capítulo 6).

1.2 Validación y alineamiento del proceso existente

El proceso de gestión de incidentes cibernéticos debe someterse a revisiones sistemáticas con el propósito de conservar su pertinencia frente a la mutación constante de las amenazas, la transformación de las arquitecturas tecnológicas, la introducción de exigencias regulatorias emergentes y los aprendizajes derivados de eventos pasados. Un esquema invariable resulta incongruente con la celeridad con la cual los actores hostiles modifican sus tácticas, técnicas y procedimientos (TTP), así como con el grado de complejidad de las ofensivas dirigidas contra infraestructuras financieras críticas.

Con el fin de respaldar esta actualización continua, se propone utilizar como referentes estructurantes ciertos estándares internacionales ampliamente consolidados, en concreto, la guía NIST SP 800-61 Rev. 3 y la norma ISO/IEC 27035, entendidas como instrumentos de armonización conceptual y operativa:

- **NIST SP 800-61**: La publicación converge con el *NIST Cybersecurity Framework* (CSF) 2.0 y traslada la gestión de incidentes desde una visión meramente técnica hacia una función institucional integrada en el tratamiento del riesgo. El ciclo de vida queda orquestado con las funciones del CSF 2.0: gobernanza (*govern*), identificación (*identify*) y protección (*protect*) como pilares de preparación; detección

(*detect*), respuesta (*respond*) y recuperación (*recover*) para la ejecución táctica; y una capa transversal de retroalimentación estructurada orientada a incorporar lecciones aprendidas y fortalecer la madurez organizacional [1].

- **ISO/IEC 27035**: La serie aporta principios, procesos y recomendaciones detalladas para afrontar incidentes de seguridad de la información con criterios de coherencia, trazabilidad y reproducibilidad. La parte 1 (ISO/IEC 27035-1) describe conceptos esenciales, fases y responsabilidades clave; la parte 2 (ISO/IEC 27035-2) provee directrices para minimizar el impacto y prevenir recurrencias [2]. Un elemento vertebral es la mención explícita del análisis de riesgos como insumo para la priorización, la delimitación de funciones y el diseño de mecanismos de mejora continua [3].

La convergencia con estos marcos no exige una adopción literal, sino la selección de componentes comunes que posibiliten: configurar un ciclo de vida homogéneo y claramente delimitado; precisar responsabilidades, líneas de reporte y facultades decisorias en cada etapa; y garantizar que los procedimientos internos resulten auditables, comparables entre instituciones y susceptibles de adaptación a los ordenamientos regulatorios latinoamericanos, sin perder consistencia técnica ni alineación con las mejores prácticas internacionales.

1.2.1 Base común regional y modelo escalable

La cooperación entre bancos centrales y autoridades afines constituye un amplificador estratégico de capacidades técnicas, analíticas y operativas. En este contexto, resulta imprescindible emprender un ejercicio sistemático de contraste entre lineamientos internos que permita reconocer prácticas de gobernanza y respuesta sólidas, registrar divergencias normativamente justificadas y derivar, a partir de esto, un umbral de referencia mínimo para la región. Dicho insumo debe configurarse como corpus orientador para instituciones con niveles incipientes de madurez y, de manera simultánea, como instrumento de perfeccionamiento para organizaciones con esquemas avanzados de gestión de incidentes.

La noción de modelo escalable adquiere relevancia crítica al considerar las asimetrías en la dimensión institucional, la disponibilidad de recursos, la complejidad infraestructural y la exposición a amenazas específicas. Por consiguiente, se privilegia una arquitectura flexible que habilite la implementación progresiva de controles especializados, herramientas de automatización y mecanismos de coordinación interinstitucional, minimizando fricciones organizacionales y preservando la coherencia regional.

En tal sentido, se propone la consolidación de un marco común que:

- Identifique arreglos de gobernanza, procesos de respuesta y mecanismos de supervisión ya probados en distintas jurisdicciones, susceptibles de ser reinterpretados como referentes regionales.
- Integre un repertorio de exigencias mínimas sugeridas, delimitando una jerarquía de comités, atribuciones del equipo de gestión de incidentes (*Computer Security Incident Response Team*, CSIRT), criterios de severidad, protocolos de comunicación interna y reportes externos a contrapartes relevantes.
- Defina trayectorias de madurez graduales, de modo que cada entidad pueda transitar desde facultades esenciales hacia funcionalidades avanzadas.
- Conserve márgenes de modificación suficientes para internalizar diferencias en estructuras organizacionales, niveles tecnológicos y entornos regulatorios, sin erosionar la consistencia con principios técnicos comunes.

1.2.2 Revisión de requisitos regulatorios locales

La diversidad y fragmentación de las regulaciones en América Latina demanda un enfoque sistemático para delimitar las obligaciones de notificación de eventos de ciberseguridad y los parámetros que determinan su calificación como *incidentes reportables* (es decir, sucesos cuya comunicación a la autoridad competente resulta obligatoria según la normativa aplicable). Con el propósito de favorecer el cumplimiento normativo y propiciar convergencias técnicas entre jurisdicciones, la Tabla 1.1 organiza la información relativa a la entidad supervisora, el alcance institucional, los umbrales de criticidad, los campos mínimos exigidos y los canales oficiales de remisión. Los horizontes temporales de notificación, junto con su vinculación con sistemas de clasificación, matrices de escalamiento y criterios de severidad, se desarrollarán en secciones posteriores, con el fin de preservar consistencia metodológica y prevenir redundancias innecesarias.

Tabla 1.1: Requisitos regulatorios en los bancos de Latinoamérica respecto a la clasificación y reporte de incidentes cibernéticos.

País	Autoridad y norma	Alcance	Incidente reportable	Datos o acciones mínimas	Canal de envío
Colombia	Superintendencia Financiera de Colombia (SFC): Circular Externa 033 de 2020 (TUIC) y reporte de métricas e indicadores según formato 408 [4].	Entidades vigiladas por SFC.	Eventos que comprometen C/I/D, afectación de clientes u operación e incidentes con potencial sistémico. Formato 408 recoge métricas periódicas e indicadores de SI/CS para supervisión continua.	Identificador del evento, fecha/hora (ocurrencia y detección), severidad, servicio afectado, IoC, TLP y medidas adoptadas.	Buzón y plataformas institucionales de la SFC; trazabilidad mediante etiquetado y referencias cruzadas TUIC/Formato 408.
México	Comisión Nacional Bancaria y de Valores (CNBV): CUB, anexo 64, con plantilla de incidentes [5].	Instituciones de banca múltiple y entidades supervisadas por CNBV.	Afectación a canales, interrupciones, accesos no autorizados, fuga de información o fraude tecnológico.	Fecha/hora de ocurrencia y detección, duración, canal afectado, alcance, medidas de contención y recuperación.	SITI (Sistema Interinstitucional de Transferencia de Información) de CNBV.

Brasil	Conselho Monetário Nacional (CMN), Resolución 4.893/2021, y Banco Central do Brasil (BCB), Resolución 85/2021 (política de ciberseguridad y requisitos para terceros) [6]; actualización de 2024 sobre comunicación de incidentes relevantes [7].	Instituciones reguladas por BCB/CMN; pagos y servicios críticos.	Eventos que comprometen servicios críticos, incidentes relevantes, interrupciones operativas y terceros críticos (incluye nube).	Identificación del evento, impacto en servicios, terceros involucrados, medidas y tiempos de restablecimiento.	Vía canales del BCB según normativas aplicables.
Perú	Superintendencia de Banca, Seguros y AFP (SBS): Resolución SBS 504-2021 (Reglamento para la gestión de la seguridad de la información y ciberseguridad) [8].	Empresas del sistema financiero supervisadas por la SBS.	Reporte en cuanto se advierta un incidente significativo (pérdida de información, fraude, interrupción o afectación reputacional).	Identificación de activos, descripción del evento, alcance, medidas inmediatas, acciones de recuperación y evidencias para forense.	Canal oficial SBS (según instructivos).

Argentina	Banco Central de la República Argentina (BCRA): Lineamientos para respuesta y recuperación ante ciberincidentes y Comunicación A 8280/2025, con obligación expresa de notificación [9].	Entidades financieras bajo BCRA.	Pérdida/divulgación de datos críticos, interrupciones relevantes, afectación de canales y fraudes asociados.	Datos de ocurrencia y detección, sistemas impactados, alcance, medidas de contención y comunicación.	Canal BCRA conforme lineamientos actualizados.
Chile	Comisión para el Mercado Financiero (CMF): NCG 510/2024 (riesgo operacional y ciberseguridad) y NCG 529/2024 (reemplaza el anexo 2 de reporte de incidentes operacionales vía canal CMF) [10].	Entidades reguladas por CMF (engloba infraestructuras de mercado listadas por la Comisión).	Incidentes con afectación a funciones críticas, canales, datos o terceros.	Registro del incidente, medidas, recuperación, comunicación a autoridades y partes interesadas según severidad.	Menú «Incidentes y Pérdidas Operacionales» en el canal oficial CMF.
Uruguay	Banco Central del Uruguay (BCU): Comunicación 2024/018 (seguimiento de incidentes en pagos) y Guía de estándares mínimos [11]; Registro Nacional de Incidentes de Ciberseguridad [12].	Entidades del sistema financiero supervisadas por BCU; coordinación con CERTuy para incidentes de alto impacto.	Eventos operativos y cibernéticos que afecten la prestación de servicios, canales, sistemas propios o de terceros con impacto reputacional y sistémico.	Registro del evento, tipología, alcance, contingencias y recuperación con evidencias y trazabilidad.	Vías formales del BCU y, según criticidad, canales CERTuy (contacto y guía pública de reporte).

1.3 Soporte ejecutivo e integración con funciones internas

El respaldo expreso y sostenido de la alta dirección constituye la piedra angular de cualquier programa de respuesta a incidentes y resiliencia cibernética en un banco central. Dicho amparo trasciende lo simbólico: se manifiesta en la asignación de recursos financieros, capital humano e infraestructura tecnológica, en la consagración de la ciberseguridad como prioridad institucional y en la promoción de una cultura donde la salvaguardia digital se concibe como responsabilidad colectiva [13]. Ausente este impulso, los esfuerzos del CSIRT y de las demás áreas involucradas pierden alcance y su impacto queda mermado.

Más allá del apoyo proveniente del nivel directivo, resulta esencial instaurar una articulación coherente y mecanismos de coordinación claramente delineados con las áreas funcionales más relevantes. Un ciberincidente difícilmente se limita al ámbito técnico; sus efectos repercuten en diversas esferas del funcionamiento institucional [14]:

- **Área legal**: fundamental desde el inicio para evaluar las implicaciones legales y regulatorias, corroborar el cumplimiento normativo (especialmente, en protección de datos y finanzas), encargarse de las cadenas de custodia requeridas y asesorar en la interacción con las autoridades.
- **Comunicaciones (corporativas/prensa)**: se ocupa de la narrativa pública con informes precisos y transparentes, evitando rumores que erosionen la confianza.
- **Gerente de continuidad del negocio (*Business Continuity Manager*, BCM)**: garantiza que los planes de respuesta a incidentes se coordinen con los de continuidad y recuperación ante desastres. Esto asegura que la prioridad sea la restauración de los servicios críticos, minimizando el impacto en las operaciones esenciales del banco y en el sistema financiero.
- **Oficial de protección de datos personales (ODP)**: crucial si el incidente involucra datos personales. Su rol es sopesar el alcance de eventuales brechas, determinar las notificaciones obligatorias a afectados y autoridades, así como velar por la concordancia con los lineamientos de privacidad pertinentes.

La ausencia de una integración efectiva y de un claro respaldo ejecutivo no solo debilita el margen de maniobra técnica, sino que puede amplificar de forma exponencial las consecuencias jurídicas, reputacionales y económicas de un incidente. Un episodio cibernético de gran envergadura constituye, en esencia, una crisis corporativa que exige una reacción concertada por toda la entidad y no simplemente una tarea delegada al departamento de TI o al CSIRT. Cuando la alta dirección interviene sin la información adecuada ni la coordinación dictada por protocolos claros, su acción puede entorpecer en vez de facilitar la contención y la recuperación [13].

A fin de coordinar de forma temprana a los actores mencionados, se propone un protocolo de activación basado en la notación BPMN (*Business Process Model and Notation*), donde se definen los gatillos de alerta, rutas de escalamiento y controles de avance que permiten dar seguimiento a las decisiones. Este diagrama brinda una representación inequívoca de las etapas primordiales, simplifica la comprensión, favorece la puesta en marcha y respalda la auditoría posterior. Gracias a esta cartografía, las advertencias se emiten sin dilaciones y los actores clave participan de forma ordenada desde las primeras fases de un evento grave.

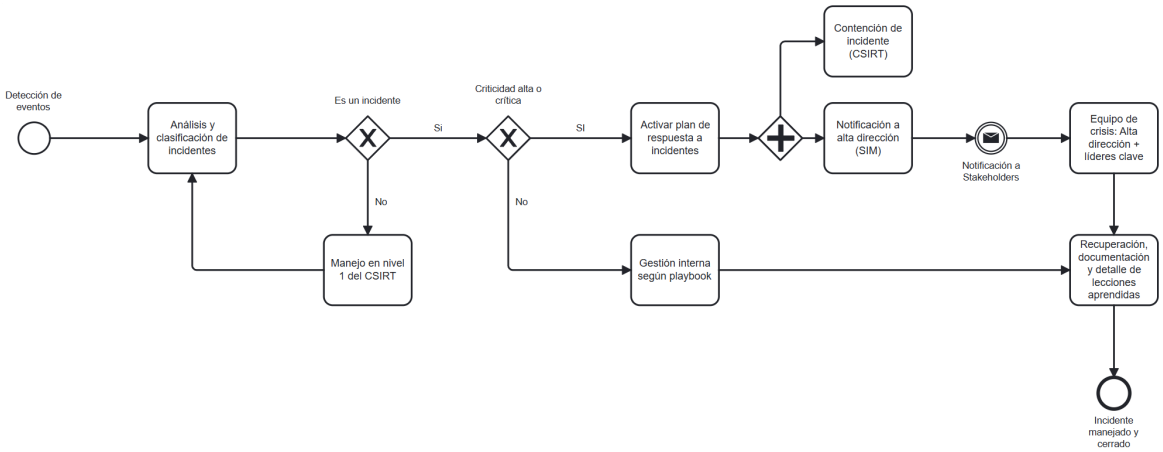


Figura 1.1: Protocolo de activación y flujograma de notificación a alta dirección.

1.4 Roles y responsabilidades esenciales

Un esquema eficaz de manejo de incidentes cibernéticos exige una definición rigurosa de funciones y responsabilidades que trascienda el ámbito del CSIRT. Aunque este conjunto especializado constituye el núcleo operativo frente a eventos de ciberseguridad, la complejidad de los escenarios contemporáneos implica la intervención sinérgica de múltiples dependencias, con mandatos definidos y líneas de decisión inequívocas. La Tabla 1.2 presenta una propuesta de distribución de roles institucionales [15] [16] [17], susceptible de ser calibrada por cada entidad conforme a su estructura orgánica, nivel de madurez y disposiciones internas aplicables.

Tabla 1.2. Descripción de las responsabilidades que adquiere cada área en gestión de incidentes.

Rol	Responsabilidades principales
Equipo CSIRT	
Comandante del incidente/*Security Incident Manager*(SIM)/líder del CSIRT	Gestión general del incidente, coordinación del equipo, toma de decisiones tácticas y comunicación con la alta dirección.
Analistas de seguridad (N1)	Detección inicial, análisis de alertas, monitorización de sistemas e identificación de IoC.
Investigadores de seguridad (N2)	Análisis en profundidad de eventos escalados, recolección, preservación e inspección de evidencia digital para determinar alcance, causa raíz y actores del incidente.
Coordinador de respuesta a incidentes (N3)	Facilita la ejecución del plan de respuesta, vela por el cumplimiento de los procedimientos, documenta el incidente y actúa como responsable técnico del proceso.
Roles de soporte y estratégicos	
Coordinador legal	Asesora sobre implicaciones jurídicas y obligaciones regulatorias y coordina, cuando corresponda, con asesores externos.
Vocero de crisis o encargado de comunicaciones	Conduce las comunicaciones externas (medios, clientes, público) e internas, garantizando mensajes coherentes y alineados con la estrategia institucional
Enlace con la alta dirección	Funciona como canal de comunicación bidireccional entre el equipo de respuesta y la alta dirección, asegurando que cuente con información oportuna para la toma de decisiones estratégicas.
Encargado de continuidad del negocio	Verifica que las acciones de respuesta y recuperación se ajusten a los planes de continuidad del negocio, priorizando la restauración de los servicios críticos.
Oficial de protección de datos personales	Evalúa el impacto del incidente sobre los datos personales, coordina las notificaciones a titulares o autoridades de protección de datos y garantiza el cumplimiento de las normativas aplicables.

Continúa en la página siguiente

Tabla 1.2. Descripción de las responsabilidades que adquiere cada área en gestión de incidentes. (Continuación)

Recursos humanos	Interviene en incidentes que involucren a empleados (p. ej., amenazas internas o errores humanos) y apoya los procesos de comunicación interna.

Para formalizar estas interacciones y asegurar la rendición de cuentas, se recomienda la utilización de una matriz RACI («Responsable», «Aprobador», «Consultado» e «Informado») (Tabla 1.3), la cual constituye una herramienta fundamental para suprimir ambigüedades y cerciorarse de que la totalidad de las tareas críticas cuente con un propietario claro y que las partes interesadas adecuadas sean consultadas o informadas [15] [16]. Lo anterior resulta vital en situaciones de alta presión como un ciberincidente, donde la coordinación y la claridad en los compromisos adquiridos pueden marcar la diferencia entre una respuesta exitosa y una que agrave la situación.

Tabla 1.3: Matriz RACI para la gestión de un incidente cibernético.

R = Responsable (*Responsible*), A = Aprobador (*Accountable*), C = Consultado (*Consulted*), I = Informado (*Informed*)									
Actividad	**Líder del incidente**	**Analista de seguridad**	**Investigadores de seguridad**	**Coordinador legal**	**Vocero**	**Alta dirección**	**Continuidad del negocio**	**Protección de datos personales**	**Otros (TI, negocios o similares)**
Preparación									
Desarrollo/actualización política de respuesta a incidentes.	A	C	C	C	I	A	C	C	C
Desarrollo/actualización de *playbooks*/SOP.	R	A	C	C	I	I	C	I	C
Adquisición y mantenimiento de herramientas de TI.	R	A	C	I	I	I	I	I	C
Capacitación y simulacros.	R	A	R	C	C	I	R	C	R
Detección y análisis									
Monitoreo de alertas y detección inicial.	I	R	C	I	I	I	I	I	C
Validación y clasificación inicial.	A	R	C	C	I	I	C	C	C

Análisis técnico profundo (causa raíz y alcance).	A	C	R	C	I	I	I	C	I
Evaluación de impacto (operacional, financiero, reputacional y legal).	A	C	C	R	R	R	R	R	R
Contención, erradicación y recuperación									
Implementación de medidas de contención.	R	A	C	C	I	I	C	C	C
Erradicación de la amenaza.	R	A	R	I	I	I	I	I	C
Restauración de sistemas y datos.	A	C	I	I	I	I	R	I	R
Verificación posterior a la recuperación.	A	R	I	I	I	I	C	I	R
Actividades posincidente									
Elaboración de informe *post mortem*.	R	A	C	C	C	I	C	C	C
Identificación e implementación de lecciones aprendidas.	A	C	C	C	C	R	C	C	C

Actualización de la base de conocimiento.	R	A	C	I	I	I	I	I	I
Comunicaciones y notificaciones									
Comunicación interna.	R	C	I	I	A	I	I	I	I
Notificación a alta dirección.	R	I	I	I	I	A	I	I	I
Notificación a reguladores.	A	I	I	R	C	R	I	C	I
Comunicación con clientes/público (si aplica).	A	I	I	C	R	R	I	C	I
Comunicación con fuerzas de seguridad (si aplica).	A	I	C	R	C	R	I	I	I
Coordinación legal y de cumplimiento									
Asesoramiento legal durante el incidente.	C	I	C	A	C	C	I	C	I
Gestión de evidencia para fines legales.	C	C	A	R	I	I	I	I	I
Notificación de brechas de datos.	C	I	I	A	C	C	I	R	I

1.5 Diagnóstico de madurez

Con el propósito de que los bancos centrales puedan identificar su estado actual y delinear un itinerario de evolución frente a incidentes cibernéticos, se recomienda acoplar un modelo de madurez. El modelo de madurez de resiliencia del CERT (CERT-RMM) [18] constituye una referencia sólida en esta materia. Aunque en su versión original se enfoca en distintos niveles de desarrollo organizacional, para los fines de esta guía se presenta una adaptación sustentada en cinco etapas progresivas, inspiradas tanto en el enfoque de los niveles de madurez del *Capability Maturity Model Integration* (CMMI) del ISACA [19] como en la *Cyber Resilience Review* (CRR) elaborada por CISA [20], la cual toma como base conceptual el propio CERT-RMM:

1. **Nivel 1 - Inicial (*ad hoc*)**: Las respuestas a incidentes surgen de manera improvisada, sin planificación previa ni criterios documentados. Las acciones dependen del conocimiento individual y de la reacción espontánea del personal disponible, lo que genera resultados inconsistentes y difíciles de reproducir. No existen procedimientos formalizados ni mecanismos sistemáticos para afrontar escenarios críticos. Ajustado de CMMI *Level 1: Initial* y CRR *MIL0: Incomplete*.

2. **Nivel 2 - Gestionado (repetible básico)**: Se observan ciertas prácticas elementales que han surgido con base en experiencias previas, aunque su aplicación varía según el caso y no existe una adopción transversal. Pueden existir esfuerzos aislados de planificación o seguimiento, pero sin uniformidad metodológica. La documentación disponible es limitada, desactualizada o no se comunica de forma efectiva. La formación del personal es esporádica y no responde a un enfoque articulado. Ajustado de CMMI *Level 2: Managed* y CRR *MIL1: Performed*.

3. **Nivel 3 - Definido (estandarizado)**: En este nivel, las respuestas se encuentran respaldadas por procedimientos formales aprobados y difundidos en toda la entidad. Las políticas, flujos operativos y manuales de referencia cubren los escenarios más frecuentes, complementados con los roles de intervención y responsabilidades claramente delimitados. El personal recibe formación periódica con base en planes formulados y las acciones se ejecutan de forma coherente con otras funciones de TI y de seguridad. Adaptado de CMMI *Level 3: Defined*, CRR *MIL2: Planned* y CRR *MIL3: Managed*.

4. **Nivel 4 - Medido (cuantitativamente gestionado)**: La entidad recopila información cuantitativa sobre los tiempos de detección (MTTD), el desempeño en la resolución (MTTR), el impacto financiero y la frecuencia de ocurrencia. Tales datos se examinan para verificar la consistencia de las respuestas ejecutadas y se utilizan como insumo en revisiones periódicas que se elevan al nivel directivo. Las respuestas se desarrollan dentro de márgenes previamente fijados, con un

comportamiento previsible y trazable. Adaptado de CMMI *Level 4: Quantitatively Managed* y CRR *MIL4: Measured.*

5. **Nivel 5 - Optimizado (mejora continua)**: La entidad asume un enfoque prospectivo, orientado por la inspección rigurosa de métricas e incidentes pasados. Se promueve la innovación y la optimización mediante nuevas tecnologías, ejercicios avanzados de simulación y ajustes metodológicos constantes. Además, las acciones se alinean con las metas institucionales de resiliencia y las respuestas ante escenarios disruptivos se integran como parte fundamental de la conducción estratégica del banco. Adaptado de CMMI *Level 5: Optimizing* y CRR *MIL5: Defined*.

A partir del modelo descrito, se desarrolla un cuestionario de autodiagnóstico simplificado (Tabla 1.4), el cual permite a cada banco central examinar, de forma realista, el nivel de madurez que más se aproxima a sus prácticas actuales frente a incidentes cibernéticos. Este instrumento no busca emitir juicios normativos ni establecer comparaciones entre entidades, sino proporcionar una base objetiva sobre la cual cada institución pueda trazar prioridades, detectar vacíos y proyectar sus próximos pasos en función de su contexto particular. Dicho ejercicio también puede favorecer el diálogo interno entre áreas clave, como seguridad de la información, tecnología, continuidad operativa, legal y auditoría, al brindar un lenguaje común para abordar temas sensibles desde una mirada constructiva.

Tabla 1.4. Asignación de niveles de madurez de resiliencia acorde al desempeño en actividades relacionadas con el manejo de incidentes.

Área de proceso	Nivel 1: Inicial	Nivel 2: Gestionado	Nivel 3: Definido
1. Política y plan de respuesta a incidentes	No existe una política ni un plan formal. Las respuestas son *ad hoc*.	Existe un plan básico o informal, pero no siempre se sigue o está actualizado.	Existe una política formal y un plan de respuesta a incidentes documentado, aprobado, comunicado y consistentemente desplegado para los incidentes comunes [21].

Continúa en la página siguiente

Tabla 1.4. Asignación de niveles de madurez de resiliencia acorde al desempeño en actividades relacionadas con el manejo de incidentes. (Continuación)

2. Roles y responsabilidades (CSIRT y otros)	No hay roles formalmente asignados para la respuesta a incidentes.	Los roles existen de manera informal y las responsabilidades no se encuentran documentadas de forma precisa.	Los roles y responsabilidades del CSIRT y otros *stakeholders* clave están formalmente definidos, documentados y comunicados [21].
3. Detección y análisis de incidentes	La detección es reactiva, a menudo por impacto visible o notificación de terceros.	Se utilizan algunas herramientas básicas de monitoreo, pero la investigación es limitada.	Se utilizan herramientas de detección (SIEM o EDR) con reglas definidas. Existe un proceso formal para analizar y clasificar incidentes.
4. Contención, erradicación y recuperación	Las acciones son improvisadas y pueden ser inconsistentes.	Se aplican medidas básicas de contención, pero pueden no ser efectivas o rápidas.	Existen procedimientos documentados (SOP/-*playbooks*) para contener, erradicar y recuperarse de los tipos de incidentes más comunes.
5. Lecciones aprendidas y mejora continua	No se realiza un análisis formal posincidente.	Se discuten informalmente algunos incidentes, pero no hay un proceso estructurado de lecciones aprendidas.	Se realiza una valoración *post mortem* para incidentes significativos, se documentan las lecciones aprendidas y se identifican algunas mejoras.

Continúa en la página siguiente

Tabla 1.4. Asignación de niveles de madurez de resiliencia acorde al desempeño en actividades relacionadas con el manejo de incidentes. (Continuación)

6. Herramientas y tecnología de respuesta a incidentes	Se utilizan herramientas básicas de TI, no específicas para respuesta a incidentes.	Se han implementado algunas herramientas de seguridad (como antivirus o *firewall*), pero no están integradas.	Se utilizan herramientas dedicadas para la respuesta a incidentes (SIEM, EDR, herramientas forenses, etc.) y están razonablemente configuradas.
7. Capacitación y concienciación	No hay capacitación formal en la respuesta a los incidentes.	Se ofrece capacitación básica en seguridad, pero de forma esporádica.	El personal del CSIRT y otros roles clave reciben capacitación regular y específica en respuesta a incidentes. Se realizan simulacros básicos.
8. Comunicación y coordinación (interna y externa)	La comunicación durante un incidente es desorganizada y *ad hoc*.	Existen canales de comunicación informales y la coordinación es deficiente o insuficiente.	Existen protocolos de comunicación definidos para *stakeholders* internos y externos [21].

2 Detección automatizada y monitoreo continuo

La detección temprana de amenazas cibernéticas, combinada con un escrutinio ininterrumpido de la superficie tecnológica, resulta determinante para desplegar respuestas oportunas y precisas. En ese escenario, la automatización ya no constituye un valor añadido, sino un elemento nuclear: gracias a la orquestación de reglas avanzadas y motores de análisis heurístico, los bancos centrales procesan volúmenes masivos de telemetría y generan alertas en lapsos que, hasta hace pocos años, habrían sido inalcanzables para un analista humano.

2.1 Capacidades avanzadas de ingesta y monitoreo

Las plataformas de *Gestión de Información y Eventos de Seguridad* (*Security Information and Event Management*, SIEM) y de *Detección y Respuesta en Endpoints* (*Endpoint Detection and Response*, EDR) constituyen componentes neurálgicos dentro de la arquitectura de defensa cibernética de un banco central. No obstante, su aporte estratégico proviene menos de la mera implementación tecnológica que del aprovechamiento riguroso de sus capacidades avanzadas.

En el caso de los sistemas SIEM, además de la recopilación, normalización y correlación de registros logs provenientes de servidores, redes, aplicaciones e infraestructuras de seguridad, las soluciones contemporáneas incorporan funcionalidades críticas para el entorno financiero [22], entre ellas: detección sustentada en modelos de comportamiento, integración con orquestación, automatización y respuesta en seguridad (*Security Orchestration, Automation and Response*, SOAR), enriquecimiento continuo mediante inteligencia de amenazas (*Threat Intelligence*) y construcción de indicadores alineados con el riesgo operativo y la supervisión proactiva. Concretamente, las soluciones de SIEM modernas abarcan [22] [23]:

- **Analítica de comportamiento de usuarios y entidades (UEBA, *User and Entity Behavior Analytics*)**: aprovecha modelos estadísticos y algoritmos de aprendizaje

automático para localizar conductas atípicas en cuentas, servicios o equipos, lo que permite inferir compromisos, abuso de privilegios o amenazas internas con mayor fineza.

- **Convergencia con inteligencia de amenazas**: enriquece los eventos con indicadores de compromiso (IoC), referencias a campañas activas, vulnerabilidades explotadas y perfiles de adversarios, incrementando la precisión en la detección y disminuyendo falsos positivos en infraestructuras financieras críticas.
- **Orquestación y automatización de respuestas de seguridad (SOAR, *Security Orchestration, Automation and Response*)**: habilita flujos estructurados mediante *playbooks* que coordinan los controles técnicos, el escalamiento, la notificación y la contención frente a patrones recurrentes, garantizando actuaciones coherentes y repetibles.
- **Ingesta masiva y tratamiento eficiente de telemetría**: procesa volúmenes elevados de registros provenientes de entornos heterogéneos, con capacidades de normalización, indexación y retención prolongada, lo que favorece investigaciones forenses, reconstrucción cronológica de incidentes y cumplimiento de exigencias supervisoras.
- **Análisis en tiempo casi real y detección de anomalías**: aplica correlación avanzada y modelos de línea base para reconocer desviaciones sutiles respecto al comportamiento esperado, permitiendo una reacción temprana ante tácticas sofisticadas dirigidas a sistemas de pago, servicios críticos y plataformas de alta sensibilidad sistémica.

Por su parte, las herramientas EDR proporcionan telemetría sobre la actividad en estaciones de trabajo y servidores, localización temprana de patrones anómalos, contención remota de activos comprometidos, reconstrucción detallada de la secuencia de ataque y soporte técnico para estudios forenses digitales; ello reviste carácter determinante, dado que los *endpoints* suelen constituir vectores iniciales o puntos de pivote en campañas dirigidas contra infraestructuras críticas del sistema financiero. En concreto, los EDR pueden otorgar [24]:

- **Visibilidad granular en puntos finales**: registra eventos detallados vinculados con la creación de procesos, las conexiones de red, las modificaciones de configuración, la consulta de archivos sensibles y la carga de componentes, suministrando contexto técnico exhaustivo.
- **Diagnóstico de comportamiento y TTP**: contrasta la actividad observada con marcos como MITRE ATT&CK, permitiendo identificar *malware* inédito, técnicas *fileless* y cadenas de ataque complejas que eluden firmas convencionales.
- **Módulos de investigación y diagnóstico**: proporciona líneas de tiempo, vistas grá-

ficas de relaciones, recolección de material probatorio y herramientas de investigación profunda que simplifican la interpretación de alertas, la estimación de impacto y la formulación de hipótesis forenses.

- **Facultades remotas de respuesta y contención**: posibilita la ejecución de acciones dirigidas, como aislamiento lógico del dispositivo comprometido, interrupción selectiva de procesos maliciosos, eliminación de artefactos sospechosos o confinamiento en cuarentena, reduciendo la superficie de exposición sin afectar innecesariamente a los servicios esenciales.
- **Vinculación con inteligencia de amenazas en entornos finales**: contrasta indicadores locales con fuentes confiables sobre adversarios, campañas y fallas explotadas, apoyando el reconocimiento temprano de patrones coincidentes en estaciones de trabajo y servidores críticos.
- **Búsqueda proactiva de amenazas (*Threat Hunting*)**: explora métricas históricas y en curso mediante consultas avanzadas, reforzando la capacidad preventiva en contextos de elevada criticidad sistémica.

En la medida en que las plataformas EDR se equipan con las facultades descritas, tienden a converger funcionalmente con esquemas de detección y respuesta extendidas (*Extended Detection and Response*, XDR). No obstante, desde una perspectiva técnica, el EDR continúa focalizado en la superficie de endpoints, mientras que el XDR integra de forma nativa múltiples dominios (identidad, red, correo, nube y aplicaciones críticas), ofreciendo una capa unificada de diagnóstico y respuesta coordinada [25].

Al momento de seleccionar e implantar estas soluciones, los bancos centrales deben atender a múltiples factores:

- **Escalabilidad**: entendida como la aptitud de la plataforma para procesar miles de eventos diarios sin degradar su rendimiento ni elevar la latencia de cruce entre datos.
- **Protección de la información y soberanía**: toda alternativa tecnológica deberá desplegarse en entornos locales o en la nube sometidos a la jurisdicción aplicable, con cifrado persistente y controles de ingreso robustos.
- **Resiliencia inherente**: dado que el propio SIEM/EDR se convierte en un activo de alto valor, es imprescindible reforzar sus componentes con microsegmentación, MFA y copias aisladas de la base de datos.
- **Integración con el ecosistema existente**: la solución elegida debe intercambiar datos sin fricciones con *firewalls* de nueva generación, plataformas de prevención de fuga o pérdida de datos, gestores de identidad y demás componentes del centro de operaciones de seguridad.

La decisión final rebasa el plano puramente tecnológico; debe reflejar el perfil de riesgo del banco, los activos esenciales (sistemas de pagos, reservas estratégicas o información macroeconómica) y la pericia del personal que interpretará los hallazgos. Una herramienta vanguardista mal afinada o sin personal con formación adecuada disparará una cantidad excesiva de falsos positivos y, por consiguiente, ocultará señales genuinas de intrusión. Por tanto, conviene acompañar cualquier despliegue con un programa de refinamiento constante, revisiones de casos de uso y ejercicios periódicos de validación.

2.2 Criterios homogéneos para la validación automatizada de incidentes

La automatización constituye un componente ineludible para depurar el caudal de alertas originado por sensores de seguridad contemporáneos; no obstante, su eficacia solo emerge cuando la lógica subyacente a la determinación de cada evento se rige por parámetros inequívocos, documentados y verificables. Tales pautas han de permitir que un orquestador —por ejemplo, una solución de SIEM acoplada con un módulo SOAR— distinga entre tres categorías esenciales: incidentes que exigen intervención humana inmediata; sucesos de gravedad intermedia que admiten tratamiento automático predefinido; y señales sin relevancia o falsos positivos que únicamente introducen ruido estadístico en el entorno de monitoreo.

El eje conceptual para dicha clasificación se consolida en una matriz de severidad (Tabla 2.1), donde confluyen, por un lado, el impacto proyectado (financiero, reputacional, operacional o regulatorio) y, por otro, la probabilidad de ocurrencia o confirmación técnica. Cada intersección produce una etiqueta de prioridad (P1, P2, P3 o P4), lo que facilita el mapeo directo a niveles de escalamiento y plazos de resolución [26]. Resulta fundamental que cada banco central parametrice los umbrales según su propia tolerancia al riesgo y las exigencias normativas del entorno jurisdiccional local, dado que un nivel de afectación reputacional tolerable para cierta entidad puede ser absolutamente inaceptable para otra con mayor exposición sistémica.

Tabla 2.1. Matriz de asignación de severidad a incidentes según su impacto y probabilidad (ejemplo conceptual).

Severidad del incidente		**Impacto**			
		Crítico	**Alto**	**Medio**	**Bajo**
Probabilidad	**Alta** (observada frecuentemente, IoC de alta confianza o vulnerabilidad explotada activamente)	**P1 - Crítico** (respuesta inmediata y remisión máxima)	**P1 - Crítico / P2 - Alto** (respuesta inmediata/urgente y remisión alta)	**P2 - Alto / P3 - Medio** (respuesta rápida y remisión moderada)	**P3 - Medio / P4 - Bajo** (respuesta programada y monitoreo)
	Media (ocasional, IoC de confianza media, vulnerabilidad existe, pero sin explotación activa conocida)	**P1 - Crítico / P2 - Alto** (respuesta inmediata/urgente y remisión alta)	**P2 - Alto / P3 - Medio** (respuesta rápida y remisión moderada)	**P3 - Medio / P4 - Bajo** (respuesta programada y monitoreo)	**P4 - Bajo** (monitoreo y considerar archivo)
	Baja (rara vez observada, IoC baja confianza, vulnerabilidad teórica o difícil de explotar)	**P2 - Alto / P3 - Medio** (respuesta rápida y remisión moderada)	**P3 - Medio / P4 - Bajo** (respuesta programada y monitoreo)	**P4 - Bajo** (monitoreo y considerar archivo)	**P4 - Bajo / Informativo** (archivo y revisión periódica)

En términos ilustrativos, las categorías pueden contemplar circunstancias como:

- **P1 – Crítico**: exfiltración masiva de información sensible, interrupción sistémica de infraestructuras de pago, infección por *ransomware* con impacto sobre procesos esenciales o cualquier evento con potencial de comprometer funciones nucleares del banco central.
- **P2 – Alto**: filtración significativa, aunque contenida, degradación severa de servicios relevantes sin colapso sistémico o incidente con afectación reputacional considerable ante contrapartes o ciudadanía.
- **P3 – Medio**: interrupción acotada, exposición limitada de datos no estratégicos o comportamiento anómalo que exige verificación, pero sin indicios inmediatos de daño estructural.

- **P4 – Bajo**: manifestaciones menores sin incidencia apreciable sobre la continuidad operativa ni involucramiento de activos de información sensibles.

Para convertir la matriz conceptual en decisiones automáticas reproducibles, se diseña la Tabla 2.2 que actúa como núcleo lógico para la construcción de reglas en plataformas SIEM y herramientas SOAR. En dicho artefacto se consignan, para cada fuente de alerta, indicadores relevantes, umbrales cuantitativos (por ejemplo, volumen de datos transferidos, número de hosts afectados o duración de las conexiones sospechosas), acción preconfigurada sugerida (bloqueo de direcciones IP, aislamiento de puntos finales, revocación de credenciales, entre otros) y el grupo responsable de la revisión [14]. Esta formalización reduce la fatiga de los analistas, dado que desvía aquellas tareas repetitivas de baja criticidad que no exigen un tratamiento manual y, en paralelo, acelera la contención en los escenarios de mayor riesgo.

Tabla 2.2. Plantilla de decisión para validación automatizada (ejemplo conceptual)

Fuente de alerta	Indicador clave o evento	Umbral	Nivel de confianza de alerta	Acción automatizada sugerida	Escalamiento requerido
EDR	Detección de *ransomware* (firma/comportamiento).	1 instancia confirmada	Alto	Aislar *endpoint*, bloquear hashes conocidos y crear tiquete P1.	Inmediata a líder CSIRT y equipo de respuesta rápida.
SIEM (*Threat Intelligence*)	Conexión saliente a C&C (*Command and Control*) conocido.	1 conexión	Alto	Bloquear IP/dominio en *firewall* y crear tiquete P1.	Inmediata a analista N2 y líder CSIRT.
SIEM (UEBA)	Múltiples inicios de sesión fallidos desde IP inusual para cuenta de administrador.	5 intentos en 1 min	Medio	Bloquear IP temporalmente y alertar a analista N1.	A analista N1 para investigación.

Continúa en la página siguiente

Tabla 2.2. Plantilla de decisión para validación automatizada (ejemplo conceptual) (Continuación)

IDS o IPS	Escaneo de puertos masivo desde IP externa.	1000 puertos en 5 min	Medio	Bloquear IP en *firewall*, registrar evento, crear tiquete P3.	A analista N1 para revisión.
Reporte phishing usuario	Correo reportado con adjunto malicioso (verificado por *sandbox*).	1 reporte verificado	Alto	Buscar y eliminar correo similar en toda la organización y crear tiquete P2.	A equipo de respuesta a *phishing* y analista N2.
Firewall	Denegación de múltiples conexiones a servicio no autorizado.	100 denegaciones/-min desde misma fuente	Bajo	Registrar evento, sin acción automática.	Revisión periódica por analista N1 si persiste.

La tabla de decisión no puede permanecer estática, sino que debe examinarse periódicamente con fundamento en indicadores como el índice de falsos positivos, el MTTD y el tiempo medio de contención (MTTC). Asimismo, nuevas tácticas descritas en la taxonomía de MITRE ATT&CK o variantes de ransomware con técnicas de evasión inéditas exigen refinar umbrales y gatillos. Solo así, el engranaje automatizado conservará pertinencia frente a un panorama de amenazas que evoluciona con gran dinamismo.

2.3 Consolidación de salidas del pipeline de detección

La fase de agrupación de fuentes y mapeo avanzado en plataformas SIEM y EDR culmina en un conjunto acotado de eventos con evidencia suficiente para ser considerados *candidatos a incidente*. En este punto, la función central del *pipeline* consiste en transformar señales dispersas en casos priorizados, enriquecidos con contexto técnico, atribución preliminar y trazas verificables, reduciendo el ruido y alineando los hallazgos con los umbrales de riesgo previamente consensuados por el banco central.

Cada alerta consolidada debe ingresar en un registro normalizado que preserve, al menos, el origen de la detección, los activos comprometidos, las técnicas y tácticas asociadas según MITRE ATT&CK, los IoC relevantes, la clasificación preliminar de seve-

ridad y el ecosistema afectado (servicios críticos, infraestructuras de pago o canales externos).

La salida del *pipeline* técnico no implica aún comunicación formal hacia terceros, sino que se trata de un punto de decisión trazable. Los eventos priorizados se remiten al marco del Capítulo 3 (declaración, taxonomía y matriz de escalamiento), donde se confirma si proceden como incidentes declarados, se asigna un nivel P1–P4 y se determinan destinatarios internos. A partir de dicha clasificación, los casos que alcancen los umbrales correspondientes se proyectan hacia los procedimientos descritos en el Capítulo 4 (respuesta, contención, recuperación y notificación externa), garantizando continuidad lógica entre la detección automatizada, la decisión institucional y la comunicación coordinada.

3 Declaración, caracterización y escalamiento de incidentes

Posterior a la detección y la revisión preliminar de un evento anómalo, es indispensable activar mecanismos formales que indiquen expresamente su condición como incidente, determinen con precisión su naturaleza y lo eleven de manera oportuna hasta los niveles de autoridad correspondientes. Dichas fases garantizan una interpretación común entre todos los implicados, una asignación idónea de prioridades y la puesta en marcha de recursos técnicos, humanos y financieros congruentes con la criticidad del suceso.

3.1 Taxonomía de incidentes

Una taxonomía estandarizada constituye la piedra angular de cualquier sistema maduro de respuesta cibernética, dado que al emplear un vocabulario uniforme:

- se facilita la comunicación interna y externa, a razón de que cada uno de los involucrados (incluidos otros bancos y reguladores) puede describir los incidentes en un lenguaje común que evite ambigüedades;
- se potencia el análisis de tendencias, puesto que la categorización homogénea revela patrones de ataque, tácticas repetitivas y vulnerabilidades explotadas con mayor frecuencia, lo cual guía la defensa y la asignación de recursos;
- se posibilita la comparación de métricas entre bancos, construyendo un esquema de referencia riguroso;
- se simplifica la elaboración de informes regulatorios, puesto que múltiples autoridades o supervisores exigen la clasificación de incidentes conforme a esquemas puntuales. La Taxonomía Única de Incidentes Cibernéticos (TUIC) de la Superintendencia Financiera de Colombia, por ejemplo, constituye un esfuerzo regional para normalizar tal información [4];

- se robustece el intercambio de inteligencia, dado que un lenguaje compartido agiliza la distribución de IoC en plataformas como MISP (*Malware Information Sharing Platform*).

Adoptar una taxonomía concertada a escala latinoamericana multiplicaría el valor de la inteligencia colectiva: la detección temprana de campañas dirigidas contra el sector financiero resultaría más ágil, la coordinación defensiva ganaría proactividad y cada banco central obtendría un beneficio recíproco de la experiencia acumulada por sus homólogos.

La Tabla 3.1 integra y armoniza diversos recursos, como las categorías funcionales de la TUIC y los grupos temáticos propuestos en la *Common Taxonomy for Law-Enforcement and the National Network of CSIRTs* [27]. Cada familia se desglosa en subcategorías alineadas con las técnicas de MITRE ATT&CK, lo que habilita la correlación automática con fuentes de inteligencia de amenazas y la comparación entre entidades homólogas. A cada subcategoría se le ha asignado un identificador alfanumérico único, de modo que dicha clave funcione como etiqueta estándar en flujos de notificación, tableros SIEM/SOAR y reportes exigidos por autoridades supervisoras. En suma a ello, las descripciones condensan el propósito y la mecánica de la conducta adversa, permitiendo que analistas, auditores y responsables de cumplimiento capten de inmediato la relevancia operativa y regulatoria del evento.

Tabla 3.1. Taxonomía de incidentes cibernéticos y mapeo con MITRE ATT&CK.

Código alfanumérico	Categoría principal	Subcategoría – Técnica MITRE ATT&CK vinculada	Descripción
ACC – Acceso	Intrusiones / intento de intrusión	**ACC-01**: Uso de credenciales válidas (T1078).	Autenticación obtenida sin autorización mediante datos legítimos.
		ACC-01.1: *Credential Stuffing* (T1110.004).	Combinación masiva de pares usuario-contraseña filtrados hasta lograr inicio de sesión. Apunta a múltiples cuentas y plataformas en paralelo.
		ACC-02: Explotación de servicios expuestos (T1190).	Aprovechamiento de fallas en aplicaciones públicas para lograr ejecución remota y sesión interactiva.
		ACC-03: Adivinación de contraseñas (T1110.001).	Enfocado normalmente en una sola cuenta. Puede emplear diccionarios, patrones predecibles o reglas de complejidad.

Continúa en la página siguiente

Tabla 3.1. Taxonomía de incidentes cibernéticos y mapeo con MITRE ATT&CK. (Continuación)

MAL – Malware	Código malicioso	**MAL-01:** Datos cifrados para impacto (T1486).	Cifrado o bloqueo de activos digitales con exigencia de rescate monetario (*ransomware*).
		MAL-02: Canal cifrado (T1573).	Programa que intercepta operaciones financieras, crea túneles cifrados y extrae datos sensibles (troyano).
		MAL-03: Captura de entradas (T1056.001).	Captura de pulsaciones, pantallas o portapapeles con finalidad de obtener credenciales o secretos (*spyware / keylogger*).
		MAL-04: Transferencia de herramientas de infiltración (T1105).	Componente inicial que descarga y despliega cargas adicionales en el entorno comprometido.
DIS – Disponibilidad	Denegación de servicio / interrupción	**DIS-01:** DoS de red (T1498).	Saturación de ancho de banda o tablas de estado que impide la conectividad.
		DIS-01.1: DDoS volumétrico	Tráfico distribuido originado en *botnets* que excede la capacidad de procesamiento del destino.
		DIS-02: DoS de capa aplicación (T1499)	Consumo de recursos mediante peticiones HTTP, DNS o API de alto costo computacional.
		DIS-03: Falla de componente crítico.	Interrupción derivada de avería física, corte energético o error de configuración que afecta a los servicios esenciales.

Continúa en la página siguiente

Tabla 3.1. Taxonomía de incidentes cibernéticos y mapeo con MITRE ATT&CK. (Continuación)

FRD – Fraude	Actividad fraudulenta	**FRD-01:** Fraude en transacciones electrónicas. Entre otras técnicas, • T1114 - *Email Collection*, • T1056.004 - *Input Capture: Credential API Hooking*.	Intercepción de correos con estados de cuenta, OTP o enlaces de confirmación que habilitan la toma de control de transacciones.
			Inserción de componentes que extraen credenciales directamente de procesos de banca electrónica.
		FRD-02: Alteración de sistemas para beneficio indebido. Entre otras técnicas, • T1491.001 *Stored Data Manipulation,* • T1491.002 *Transmitted Data Manipulation.*	Modificación premeditada de lógica de negocio, registros o parámetros contables para desviar recursos.
DAT – Datos	Fuga / exfiltración / alteración de información	**DAT-01:** Fuga y exfiltración se relacionan de manera directa con la táctica *Exfiltration* y las técnicas T1020, T1041, T1048, T1052, T1567, T1011 y T1030.	Distintos vectores —desde canales C2 cifrados hasta servicios web o soportes físicos— por los que un adversario extrae información confidencial.
		DAT-02: Alteración, se vincula con la táctica *Impact* a través de T1565 (manipulación selectiva), T1485 (destrucción), T1486 (cifrado extorsivo) y T1491 (*defacement*).	Degradación de la integridad, disponibilidad o confianza en los datos más valiosos de la entidad.
		DAT-03: Pérdida accidental.	Extravío, eliminación involuntaria o envío erróneo de archivos confidenciales.

Continúa en la página siguiente

Tabla 3.1. Taxonomía de incidentes cibernéticos y mapeo con MITRE ATT&CK. (Continuación)

POL – Política	Violación de política / uso indebido	**POL-01:** Uso de cuentas válidas configuradas por la organización (T1078.003).	Empleo de cuentas en la nube para finalidades ajenas al marco institucional.
		POL-02: Abuso interno de privilegios.	Personal que accede, divulga o manipula información fuera de su competencia o mandato.
REC – Reconocimiento	Actividad de reconocimiento	**REC-01:** Escaneo activo (T1595).	Sondeo sistemático de puertos, servicios o certificados con miras a identificar vectores de entrada.
		REC-02: Recopilación de información de la víctima (T1589 – T1592)	Obtención de datos sobre personal, tecnologías y proveedores mediante OSINT, ingeniería social, etc.
OTH – Otro	Incidentes no clasificados o indeterminados	Definir según caso.	Sucesos singulares que no encajan en las categorías previas, por lo que su estudio retroalimenta la matriz taxonómica.

A fin de enriquecer el catálogo, resulta indispensable elaborar un glosario de términos esenciales de los incidentes. Tal compendio debe entregar definiciones precisas y sucintas para cada categoría y subcategoría, además de conceptos técnicos críticos: evento, alerta, vulnerabilidad, amenaza, IoC, TTP, contención, erradicación, entre otros. Las acepciones han de derivarse de fuentes autorizadas como NIST SP 800-61 Rev.3 o ISO/IEC 27035, construyendo así un léxico uniforme y alineado con los estándares internacionales.

3.2 Formulario estándar de incidente

La elaboración meticulosa y coherente de registros constituye un fundamento ineludible dentro del ciclo de respuesta a incidentes cibernéticos, por lo que es indispensable disponer de un formulario homogéneo que capte todos los detalles sustantivos. Este

esquema no solo favorece el seguimiento interno, sino que también establece la base probatoria para la investigación forense digital, respalda los informes enviados a la alta dirección o a los órganos supervisores y, de forma decisiva, enriquece el repositorio institucional de lecciones aprendidas.

La plantilla propuesta (Tabla 3.2) organiza bloques de datos alineados con cada fase temporal del suceso: identificación inicial, clasificación taxonómica, cronología de detección y contención, activos comprometidos, impacto preliminar, artefactos preservados y acciones correctivas aplicadas. Cada campo remite a estándares reconocidos —NIST SP 800-61, ISO/IEC 27035 y el *Format for Incident Reporting Exchange* (FIRE) [28]— y es acorde con los lineamientos sugeridos por Google [29], con el fin de mantener la compatibilidad con las regulaciones vigentes en el sector bancario y las buenas prácticas en materia de ciberseguridad.

Tabla 3.2. Plantilla de documentación y seguimiento de un incidente.

Sección	Campo	Descripción / datos a ingresar
1. Resumen del incidente	ID del incidente	Referencia al formulario de incidente.
	Fecha del *post mortem*	
	Participantes en el *post mortem*	Nombres y roles.
	Fecha y hora de inicio del incidente	
	Fecha y hora de detección	
	Fecha y hora de resolución completa	
	Duración total del impacto	
	Breve descripción del incidente	
	Severidad final del incidente	P1 a P4.

Continúa en la página siguiente

Tabla 3.2. Plantilla de documentación y seguimiento de un incidente. (Continuación)

2. Impacto real del incidente	Impacto financiero	Cuantificar, si es posible, los costos directos e indirectos y las pérdidas estimadas.
	Impacto operacional	Servicios afectados, duración de la interrupción o número de usuarios/transacciones impactadas.
	Impacto reputacional	Cobertura mediática, sentimiento de clientes/*stakeholders* o quejas recibidas.
	Impacto regulatorio/legal	Notificaciones realizadas, investigaciones iniciadas o multas potenciales.
	Impacto en la confidencialidad, integridad y disponibilidad (CIA)	De los datos o sistemas.
3. Cronología detallada de eventos clave	Listar secuencialmente los eventos más importantes desde el inicio hasta el cierre, con *marcas temporales* precisas. Incluir detección, análisis, decisiones clave, acciones de contención, erradicación, recuperación y comunicaciones.	
4. Análisis de causa raíz (RCA)	¿Cuál fue la causa técnica inmediata del incidente?	Por ejemplo, explotación de vulnerabilidad CVE-xxxx, configuración errónea de *firewall* o credenciales comprometidas.
	Utilizando una técnica como la de «Los 5 ¿por qué?» (*5 whys*) o similar, ¿cuáles fueron las causas subyacentes?	Profundizar hasta encontrar las fallas fundamentales en procesos, tecnología o factor humano.
	¿Hubo factores contribuyentes?	Falta de parches, capacitación inadecuada, documentación desactualizada, fallas en la comunicación, etc.

Continúa en la página siguiente

Tabla 3.2. Plantilla de documentación y seguimiento de un incidente. (Continuación)

5. Evaluación de la respuesta al incidente	Acciones inmediatas tomadas (respuesta y recuperación)	¿Qué se hizo, quién lo hizo, cuándo y por qué se tomó esa decisión?
	Análisis de los *playbooks* utilizados	Descripción de los *playbooks* empleados, evaluando la pertinencia de las tareas realizadas en concordancia con estos.
	¿Qué funcionó bien durante la respuesta?	Aspectos positivos: herramientas efectivas, comunicación clara, rápida toma de decisiones, SOP útiles, etc.
	¿Qué no funcionó bien o podría mejorar?	Desafíos encontrados: retrasos en la detección/respuesta, falta de información, herramientas inadecuadas, SOP confusos o inexistentes, problemas de comunicación/coordinación, decisiones erróneas, entre otros.
	¿Se siguieron los planes y procedimientos establecidos?	Si/no y la justificación.
	¿Fueron efectivas las comunicaciones internas y externas?	
6. Lecciones aprendidas clave	Listar los aprendizajes más importantes derivados del incidente y la respuesta.	Lo que funcionó, lo que falló y «dónde hubo suerte».
7. Plan de acción y mejoras propuestas	Para cada lección aprendida o área de mejora identificada, proponer acciones correctivas y preventivas específicas y medibles.	Lista con tipo (prevenir/mitigar/proceso), dueño, prioridad, vínculo a bug/tiquete, estado y criterio de éxito.

Aunque esta guía brinda un formulario preliminar, resulta oportuno reconocer que el FIRE, publicado en 2024 por el Financial Stability Board, se perfila como el referente sectorial más robusto. FIRE proporciona una «gramática común» que estandariza atributos, definiciones y reglas sintácticas, afianzando la comunicación granular, estructurada y automatizable entre entidades supervisadas y autoridades. Diversos actores de la industria, entre ellos el Investment Company Institute, han respaldado su adop-

ción gradual, subrayando que un esquema convergente reduce cargas duplicadas y alinea reportes con directivas como DORA, NIS2, CER, CIRCIA y las nuevas normas de la SEC [28]. En consecuencia, se recomienda que los bancos centrales utilicen el esquema propuesto como punto de partida y, conforme a FIRE continúe refinándose y las normativas locales evolucionen, evalúen de manera progresiva la incorporación de sus campos adicionales.

3.3 Criterios y matriz de escalamiento de incidentes

Una matriz de escalamiento consolida el flujo de notificaciones, señalando, para cada nivel de severidad, los destinatarios pertinentes y las ventanas temporales correspondientes [14]. Tal cartografía procedimental es crucial para coordinar la respuesta y cumplir los plazos fijados por los supervisores [30]. Los tiempos y audiencias deberán adaptarse a la organización interna de cada banco central, a su apetito de riesgo y a los mandatos de reporte que imponga la jurisdicción aplicable.

La rapidez con la que un incidente se transfiere desde el nivel operativo inicial hacia esferas con mayor autoridad resulta decisiva para limitar su impacto. Un esquema de escalamiento, por tanto, debe trazar rutas inequívocas —respaldadas por umbrales técnicos y de negocio— que indiquen cuándo elevar la atención y a quién convocar en cada escenario [17]. La lógica subyacente se orienta a que la información correcta llegue, sin dilaciones, a los responsables provistos de recursos y facultades para adoptar medidas concluyentes.

La guía para distinguir entre transferencias internas y externas debe contemplar las siguientes consideraciones [14] [17]:

Escalamiento interno:

- **Analista N1 a analista N2/especialista**: Cuando un incidente requiere un conocimiento especializado para su diagnóstico o resolución mayor que el que posee el analista de primer nivel.
- **Al líder del CSIRT**: Cuando un incidente alcanza un umbral de severidad predefinido (P1 o P2 según la matriz previa), múltiples sistemas críticos revelan síntomas de compromiso simultáneo, la contención inicial falla o se solicita coordinación interdepartamental significativa.
- **Al CISO** *(Chief Information Security Officer)*: Situaciones con implicaciones regulatorias o reputacionales relevantes que obligan a notificar al CISO, quien, a su vez, puede elevar el reporte a la alta dirección.

- **A la alta dirección** (CEO o directorio): Para situaciones que amenazan la continuidad operativa del banco, la estabilidad financiera, la confianza pública o que conllevan graves consecuencias legales o regulatorias. La notificación a este nivel se rige por el flujograma 1.1.
- **A otras unidades de negocio o soporte** (legal, comunicaciones, continuidad o privacidad): De conformidad con la naturaleza del incidente y los *triggers* definidos en los protocolos de colaboración. Una fuga de datos personales, por ejemplo, activa de inmediato la participación del responsable de protección de datos y del equipo jurídico.

Escalamiento externo

- **A proveedores de servicios de seguridad gestionados** (*Managed Security Service Providers*, MSSP) **o consultores externos**: Cuando la investigación demanda destrezas poco habituales (inspección de malware, ingeniería inversa de *firmware* bancario o contención en entornos de tecnología operativa) resulta apropiado recurrir a proveedores especializados o al MSSP.
- **A otras instituciones financieras** (pares o CSIRT sectorial): Para compartir IoC y tácticas de ataque observadas que podrían afectar a otras entidades del sector, fomentando una defensa colectiva.
- **A entidades reguladoras y supervisoras**: De acuerdo con las obligaciones de notificación de la normativa aplicada. Esto es particularmente crítico en el sector financiero, donde los plazos suelen ser estrictos.
- **A fuerzas y cuerpos de seguridad**: Episodios que involucren extorsión, fraude de alto monto o cuando así lo soliciten la regulación o la evaluación del equipo jurídico.
- **A proveedores de servicios de Internet** (*Internet Service Providers*, ISP) **o de certificados digitales**: Necesarios para solicitar bloqueo de tráfico malicioso, revocación de certificados fraudulentos, etc.

El momento exacto de escalar se rige por criterios objetivos [17] [30]:

- **Severidad predefinida**: Definida en la Tabla 2.1, la cual es el principal motor en el escalamiento.
- **Impacto potencial o real**: Considerar el impacto en los servicios esenciales, la confidencialidad de los datos, la reputación y el cumplimiento.
- **Tipo de activo afectado**: Los incidentes que repercuten sobre sistemas de pago, bases de datos de clientes o infraestructura de producción requieren un escalamiento más rápido.

- **Limitaciones técnicas o de autoridad**: Si el equipo o individuo que lidera la respuesta no dispone de los recursos, la potestad o el conocimiento para abordar el incidente.
- **Mandatos regulatorios o contractuales**: Obligaciones de notificación a terceros que pueden dictar plazos específicos para el escalamiento y la comunicación.
- **Evolución dinámica del incidente**: Un incidente que inicialmente parece de baja severidad puede escalar cuando la situación se agrava o se descubre nueva información.

En concordancia con lo anterior, la Tabla 3.3 traduce la clasificación de severidad en decisiones concretas de escalamiento, indicando, para cada prioridad, los responsables internos que deben ser convocados, las referencias externas relevantes y los horizontes sugeridos de aviso interno de acuerdo con NIST, ISO/IEC 27035 y ENISA [17]. Las interacciones formales con autoridades supervisoras, CSIRT nacionales o sectoriales y foros especializados, junto con los canales, formatos y plazos regulatorios dirigidos a terceros, se desarrollan con mayor detalle en capítulos próximos.

Tabla 3.3. Matriz de escalamiento de incidentes según la severidad declarada (ejemplo conceptual).

Severidad	Criterio	Escalamiento interno	Escalamiento externo
P1 – Crítico	Impacto sistémico, exfiltración masiva de datos sensibles o amenazas que comprometan funciones esenciales del banco.	**Inmediato**: líder del incidente o de CSIRT, CISO, presidencia/dirección general, asesoría jurídica, comunicaciones, continuidad de negocio y privacidad.	Según norma aplicable: autoridad financiera primaria, CSIRT nacional o sectorial, fuerzas de seguridad (delito flagrante), proveedores de mitigación (p. ej., anti-DDoS).
P2 – Alto	Afectación a servicios clave, fuga relevante o deterioro reputacional notorio.	**≤ 1 h**: líder del incidente/CSIRT y CISO. **≤ 4 h**: asesoría jurídica, comunicaciones, continuidad, privacidad. **Alta dirección**: informativo, a juicio del CISO.	Sujeto a umbrales regulatorios: supervisor financiero, CSIRT nacional/sectorial (para IoC), autoridad de protección de datos si involucra información personal.

Continúa en la página siguiente

Tabla 3.3. Matriz de escalamiento de incidentes según la severidad declarada (ejemplo conceptual). (Continuación)

P3 – Medio	Interrupción moderada o un brecha menor.	**≤ 8 h**: líder del incidente/CSIRT (informativo al CISO). **Áreas de negocio y jurídica**: cuando proceda.	**Opcional**: CSIRT sectorial para intercambio de IoC de bajo impacto.
P4 – Bajo	Afectación mínima sin datos sensibles.	**≤ 24 h**: líder del incidente para realizar registro y seguimiento.	No se prevé contacto con terceros.

Un traslado tardío deja al adversario suficiente margen para profundizar el daño; uno prematuro produce ruido, dispersa esfuerzos y arriesga la confidencialidad de la investigación. Por ello, los flujos de escalamiento se documentan en el plan de respuesta a incidentes, se enseñan a todo el personal implicado y se ensayan mediante ejercicios regulares que validan los tiempos de alerta y las vías de comunicación. Con tal enfoque, el escalamiento deja de depender de la intuición bajo presión y se convierte en una cadena de responsabilidad perfectamente cartografiada que refuerza la agilidad y el rigor de la respuesta institucional. Adicionalmente, es crucial reconocer que la matriz constituye un artefacto dinámico que debe revisarse con regularidad, sobre todo cuando evolucionen las normas aplicables o la estructura corporativa. Su aplicación rigurosa influye de manera decisiva en la conducción de una crisis y en la atenuación de las repercusiones negativas del incidente.

4 Respuesta, contención y recuperación estructurada

4.1 Acuerdos de asistencia especializada (Incident Response Retainer)

Un IRR es un convenio prenegociado con un proveedor DFIR (*Digital Forensics and Incident Response*) que garantiza prioridad 24/7, SLA con tiempos objetivo para inicio de actividades y contención, en conjunto con condiciones comerciales previamente delimitadas antes de cualquier contingencia [31]. Su valor estratégico en el ecosistema bancario se refleja en la reducción del *time-to-engage* (tiempo hasta el despliegue del equipo), la previsibilidad de costos y escalamiento, además de la preservación de pruebas en los términos de auditoría y supervisión que apliquen.

El IRR se desenvuelve en un ciclo de respuesta integral [32]. En la etapa de preparación, el IRR colabora en planes de respuesta, evaluaciones de alistamiento (*breach preparedness assessments*) y desarrollo de playbooks. En detección y triaje, incorpora monitoreo de redes, inteligencia de amenazas y procedimientos de clasificación temprana para dimensionar el evento con rapidez. En la contención, determina el alcance del ataque y aísla componentes comprometidos, mientras que en la erradicación recurre a forense digital y a la indagación de causa raíz para suprimir artefactos maliciosos y cerrar brechas. En la recuperación, prioriza la restauración segura y los planes de continuidad del negocio, además del retorno a operación normal. Por último, la revisión posincidente sistematiza las lecciones aprendidas, actualiza los playbooks y eleva el nivel defensivo [32].

En términos de postura proactiva y reactiva, un IRR eficaz combina ambos frentes [32]. En la dimensión proactiva converge la caza de amenazas (búsqueda de adversarios basada en hipótesis) y diagnósticos de vulnerabilidades, con el fin de atenuar las deficiencias de forma anticipada. En la dimensión reactiva, la respuesta acelerada y la priorización permiten una remediación con SLA definidos, de modo que la interrupción sea mínima y la restauración ocurra bajo criterios de seguridad verificables.

Desde la óptica de cumplimiento y regulación, un IRR robustece la conformidad con lineamientos como HIPAA, PCI DSS y GDPR, al demostrar debida diligencia en la protección de datos sensibles y la conducción ordenada de incidentes [32]. Para una implementación sólida, el IRR debe acoplarse a las capacidades de seguridad existentes y considerar la formación del personal, tal que cada rol reconozca su papel en el ciclo de respuesta. Así, el servicio no solo aporta soporte de emergencia, sino que también fortalece la postura organizacional, aporta a la resiliencia operativa y disminuye el impacto de eventos futuros [32].

4.2 Activación de pólizas y coordinación con asegurador

Cuando exista póliza de ciberseguridad, se deberá activar tempranamente la cobertura, comunicándose con la compañía aseguradora para conservar los amparos y prevenir controversias sobre el siniestro. Ello comprende: (i) aviso inmediato [33] a la línea 24/7 o al buzón de reclamaciones, con una descripción preliminar de hechos sin admisión de responsabilidad; (ii) verificación de cláusulas de consentimiento previo para gastos —servicios forenses (respuesta técnica), asesoría jurídica y demás— y, cuando proceda, empleo de proveedores de panel del asegurador (*on-panel vendors*) o preaprobación de firmas preferentes [34]; (iii) escalamiento jurídico mediante el abogado designado para dirigir el trabajo técnico bajo privilegio legal, preservar evidencia y armonizar la narrativa con mandatos regulatorios y normas de protección de datos; (iv) revisión de exclusiones materiales, como ciberguerras o ataques patrocinados por un Estado [35], y de cláusulas de sanciones, así como de requisitos de notificación por extorsión o ransomware; en estos escenarios, además, es indispensable consultar los listados de la OFAC (*Office of Foreign Assets Control*) para comprobar que la entidad no ha infringido sanciones federales en pagos de rescate [36].

En adición a lo anterior, la institución debe comprender con precisión los parámetros contractuales: la franquicia o deducible es el monto que se descuenta del siniestro antes de la indemnización, mientras que la retención funciona como tramo que el asegurado asume íntegramente antes de que opere la cobertura. Por su lado, los sublímites delimitan cuantías máximas para conceptos concretos —como interrupción del negocio, extorsión y notificación a afectados)— dentro del límite agregado de la póliza [37]. Finalmente, en interrupciones, suelen regir *waiting periods* (períodos de carencia) expresados en horas, tal que solo si la indisponibilidad supera ese umbral temporal se activan los amparos de pérdida de ingresos y costos extraordinarios.

4.3 Procedimientos operativos estándar (SOP)

Los SOP, o *playbooks*, constituyen instrucciones secuenciales que direccionan la ejecución técnica y la coordinación táctica ante tipologías de incidente bien definidas, en especial bajo condiciones de alta presión. Su enfoque debe ser inequívocamente práctico y accionable: responsabilidades puntuales, herramientas a utilizar, decisiones preconfiguradas, puntos de control verificables, criterios de escalamiento claros y rutas de comunicación previamente acordadas, evitando documentos meramente conceptuales. Cada banco central debería mantener un catálogo mínimo de SOP alineado con los escenarios más probables o de mayor impacto para el sistema financiero. A continuación, se describen pautas esenciales de diseño y contenido.

4.3.1 Ataque de ransomware

Fases: En concordancia con la guía *#StopRansomware* elaborada por la CISA, el MS-ISAC, el NSA, y el FBI, con apoyo de Microsoft [38], las posibles fases son:

1. Detección y análisis inicial.
2. Comunicación con expertos o socios estratégicos para determinar el alcance y examinar los mecanismos de contención.
3. Aislamiento y contención.
4. Identificación de la cepa.
5. Evaluación de la propagación.
6. Protección y validación de copias de seguridad.
7. Análisis de opciones de descifrado (sin pagar rescate como política general).
8. Erradicación del ransomware y vectores de persistencia.
9. Recuperación segura desde *backups* limpios.
10. Análisis forense posincidente, contemplando el criterio de expertos o socios estratégicos.
11. Comunicación y reporte.

Consideraciones para bancos centrales: Ante un episodio de ransomware en un banco central, la prioridad inmediata es aislar los componentes críticos (sistemas de pago, plataformas de liquidación y módulos de administración de reservas), valorar el impacto sobre la estabilidad financiera y activar la coordinación con CSIRTs del sector y autoridades competentes. La contención también exige evaluar opciones de restauración

a partir de copias de seguridad cifradas y sin conexión [38], además de contemplar la asistencia de especialistas externos o fuerzas del orden. La eventual decisión de cancelar un rescate debe ser excepcional, sujeta a políticas nacionales, exigencias legales y un estudio reputacional estricto. Todo lo anterior se enmarca en un plan de respuesta al ransomware formalmente documentado y ensayado de manera periódica, el cual aborde pasos de recuperación de datos y criterios de resolución [38].

4.3.2 Fuga de datos personales

Fases: Tomando en consideración la guía de la Federal Trade Commission de Estados Unidos [39], se proponen los siguientes pasos:

1. Detección y confirmación de la brecha.
2. Contención inmediata (asegurar sistemas, revocar accesos, aislar segmentos de red, etc.).
3. Evaluación del tipo y volumen de datos comprometidos —con especial atención a información de identificación personal (PII), datos financieros sensibles o documentos clasificados del banco—.
4. Análisis forense (causa raíz, alcance y atribución si es posible).
5. Notificación a afectados y reguladores (según la matriz de comunicación y plazos legales).
6. Erradicación de la causa de la brecha.
7. Recuperación de sistemas.
8. Fortalecimiento de controles preventivos.
9. Monitoreo posbrecha.

Consideraciones para bancos centrales: Las decisiones adoptadas ante un incidente de esta naturaleza repercuten de forma directa en la confianza institucional y en la solidez del sistema financiero. Por ello, rigen obligaciones estrictas de notificación ante superintendencias y autoridades de protección de datos, con plazos, formatos y contenidos delimitados por la normativa vigente[39]. Asimismo, la comunicación pública debe llevarse a cabo con rigor[39]: mensajes precisos y verificables, voceros previamente designados, consistencia entre canales oficiales y monitoreo del efecto reputacional para evitar asimetrías informativas y preservar la credibilidad.

4.3.3 Indisponibilidad de servicios críticos

Fases: De acuerdo con la guía para entender y mitigar amenazas DoS del NCSC [40]:

1. Detección y confirmación de la indisponibilidad, distinguiendo un ataque de una falla operativa.
2. Diagnóstico del tipo de ataque (volumétrico, capa de aplicación, protocolo) o causa de la falla.
3. Activación de servicios de mitigación de DDoS (proveedores externos o soluciones internas).
4. Filtrado de tráfico malicioso.
5. Escalado de capacidad de infraestructura (ancho de banda, servidores, entre otros).
6. Conmutación por error (*failover*) a sistemas de respaldo.
7. Comunicación proactiva con usuarios/entidades afectadas.
8. Restauración gradual del servicio,.
9. Monitoreo intensivo posrestauración.
10. Análisis de causa raíz.

Consideraciones para bancos centrales: Impacto potencial en sistemas de pago interbancarios, liquidación de valores y otros servicios esenciales para la estabilidad del mercado. Ante escenarios DDoS de gran escala, se requieren planes de respuesta robustos y previamente ensayados, articulados con proveedores de infraestructura crítica para garantizar continuidad operativa. Por otro lado, dado que las autoridades financieras clasifican como incidentes graves aquellos que interrumpen la prestación normal de servicios o retrasan la ejecución de transacciones dentro de los plazos establecidos, los protocolos deben contemplar notificaciones inmediatas a las áreas de negocio pertinentes y, cuando proceda, a los entes reguladores.

4.3.4 Respuesta a fraude financiero cibernético

Fases: En casos de fraude (p.ej., transferencias no autorizadas, desfalcos digitales o ataques a la integridad de sistemas), se contemplan las siguientes etapas [41]

1. Detección de actividad fraudulenta (alertas y reportes de clientes/empleados).
2. Bloqueo inmediato de cuentas/transacciones/canales sospechosos.

3. Recopilación y preservación de evidencia (logs transaccionales, datos de sesión o comunicaciones).
4. Análisis forense para identificar el *modus operandi* y vulnerabilidades explotadas.
5. Colaboración con otras instituciones financieras si el fraude es interbancario.
6. Notificación a autoridades (policía, unidades de delitos financieros o reguladores encargados).
7. Comunicación con clientes afectados.
8. Intentos de recuperación de fondos.
9. Revisión y fortalecimiento de controles antifraude.

Consideraciones para bancos centrales: En el sector bancario, cerca del 40 % de los incidentes cibernéticos tienen un origen delictivo, donde destacan técnicas como phishing y malware orientadas a facilitar esquemas de fraude [42]. Ante este panorama, disponer de protocolos correctamente delimitados y personal entrenado en su aplicación constituye una práctica indispensable para reducir el impacto.

A pesar de que los bancos centrales no administran cuentas de clientes minoristas, sus plataformas resultan atractivas para intentos de fraude sofisticado o pueden ser explotadas como vectores dirigidos al sistema financiero completo. De ahí la importancia de una coordinación estrecha con las entidades supervisadas y de la investigación rigurosa de amenazas internas, por ejemplo, el fraude cometido por personal con acceso privilegiado.

4.3.5 Suplantación de identidad por correo electrónico (phishing/BEC)

Fases: En referencia a las actividades sugeridas por Microsoft para retomar el control de una cuenta de correo expuesta [43], las fases son:

1. Identificación y reporte del correo/comunicación sospechosa.
2. Alerta generalizada a empleados si se trata de una campaña masiva. En caso de que el correo corporativo se encuentre comprometido, se debe exigir el uso de canales alternos.
3. Bloqueo de remitentes/dominios/URLs maliciosas a nivel de *gateway* de correo y filtros web.
4. Inspección del payload (adjuntos, enlaces) en un entorno seguro (*sandbox*).
5. Exploración de las reglas del correo y de los accesos a las cuentas potencialmente comprometidas.

6. Verificación de posibles acciones no autorizadas (transferencias, cambios de configuración, etc.).
7. En caso de confirmar que la cuenta ha sido comprometida.
    - Deshabilitarla o resetear las credenciales, imponiendo la utilización de MFA.
    - Revocar los accesos activos del usuario.
    - Revisar y remover dispositivos o métodos registrados como segundo factor de autenticación, los cuales no sean reconocidos por el usuario afectado.
8. Eliminación de correos maliciosos de buzones.
9. Refuerzo de concienciación y capacitación específica.
10. Estudio de los procesos en los que se modifican o agregan cuentas involucradas en transacciones bancarias, a fin de evaluar si los controles son adecuados y suficientes.

Consideraciones para bancos centrales: Este procedimiento aborda incidentes de *spear phishing* y falsificación de correo electrónico, en los que un adversario suplanta a un ejecutivo o a una institución con el fin de inducir acciones indebidas. Los perfiles que poseen elevados privilegios y los altos directivos constituyen objetivos de gran atractivo para este tipo de ataques, dado el alcance de sus autorizaciones sobre recursos críticos. Ante tales eventos, la reacción inmediata resulta esencial para evitar que cuentas sensibles sean explotadas, lo cual podría derivar en movimientos no autorizados, filtración de información confidencial o afectaciones a la estabilidad operativa de la organización.

Un SOP constituye un manual para que el personal actúe con precisión durante un ciberataque, se comunique de modo coherente y restablezca la normalidad en el menor tiempo posible. Por tal motivo, no puede permanecer como un documento concebido sin cuidado y desatendido después de su elaboración, sino que debe redactarse con claridad, ser accesible incluso cuando los sistemas principales se hallen fuera de servicio y mantenerse disponible en formatos alternos como copias impresas o repositorios aislados. Su valor se incrementa cuando se somete periódicamente a simulacros y ejercicios de mesa, puesto que tales prácticas revelan deficiencias, fortalecen la coordinación y preparan al equipo. Adicionalmente, exige actualizaciones constantes que sean consecuentes con las lecciones derivadas de incidentes reales y la evolución del panorama de amenazas. Un SOP desfasado o de difícil implementación puede convertirse en un obstáculo adicional en medio de una crisis, en lugar de constituir un instrumento confiable para direccionar la respuesta.

4.4 Comunicación estratégica con las partes interesadas internas y externas

La atención a incidentes de seguridad trasciende la dimensión técnica y demanda una comunicación precisa y oportuna con todos los actores involucrados, tanto internos como externos: los cuerpos de seguridad en caso de configurarse delito, las instituciones financieras pares cuando exista riesgo de propagación sistémica o ataque activo compartido, los proveedores directamente implicados y, de ser pertinente, el público general si se han visto afectados servicios esenciales o datos sensibles de clientes.

A este respecto, un enfoque proactivo y cuidadosamente coordinado resulta fundamental para reducir el deterioro reputacional, proyectar transparencia ante los interlocutores relevantes, sostener la credibilidad institucional y atender de manera diligente las expectativas regulatorias.

En primera instancia, es esencial unificar los mensajes mediante una línea oficial avalada por el comité responsable, de modo que cada vocero transmita información coherente y verificable. En adición a ello, deben emplearse canales confiables, tales como el portal institucional, correos electrónicos firmados digitalmente o conferencias de prensa formales, permitiendo que las partes interesadas reconozcan la autenticidad de los comunicados.

Las buenas prácticas internacionales recomiendan que los planes de respuesta contemplen protocolos de crisis debidamente definidos, acompañados de canales alternativos que garanticen la continuidad aun si los mecanismos habituales resultan inoperables. En situaciones donde el correo electrónico corporativo o la red interna se ven afectados, el equipo de respuesta debe recurrir a medios redundantes como telefonía segura, radios, aplicaciones de mensajería cifrada o cualquier sistema independiente de la infraestructura principal. Además, a fin de que esta dinámica sea efectiva, resulta imprescindible mantener actualizada una lista de contactos de emergencia que indique responsables internos, proveedores críticos y equipos especializados como los CERT/CSIRT nacionales, lo cual posibilita una articulación rápida y ordenada en circunstancias adversas [44].

Asimismo, es indispensable instaurar un esquema de escalamiento interno que determine con precisión quién notifica a la alta dirección, en qué circunstancias se convoca a un comité de crisis y cómo se distribuyen las actualizaciones a las áreas involucradas. Una dinámica comunicativa correctamente orquestada permite que las máximas instancias de decisión actúen con fundamento en argumentos confiables y que el personal comprenda con claridad su rol durante la contingencia [45].

Otro elemento central es la estricta observancia de los plazos regulatorios: un retraso

en la notificación puede acarrear sanciones y minar la legitimidad institucional. En el sector financiero se observan ventanas cada vez más estrictas y, sobre todo, un énfasis en avisos tempranos al supervisor tras la clasificación del evento como crítico. En **Estados Unidos**, la regla conjunta de OCC, FDIC y la Reserva Federal requiere informar tan pronto como sea posible y a más tardar en 36 horas desde que la entidad determina que el suceso alcanza el umbral de notificación [46].

En **Europa**, DORA introduce un modelo escalonado con aviso inicial en menos de 4 horas tras la clasificación como «mayor» y 24 horas desde la detección, seguido de reporte intermedio a 72 horas y cierre a 1 mes, armonizando criterios entre sectores y en concordancia con NIS2 [47]. Por su lado, el Reino Unido conserva el principio de notificación inmediata o en fase temprana a la FCA/PRA.

En América Latina, las tendencias se alinean con tal aceleración. En **Argentina**, el Banco Central exige una comunicación inicial en la primera hora de detección, mensajes de seguimiento mientras persista la contingencia y un informe de cierre con plazo máximo de cinco días [9]. En **Chile**, la CMF ordena reportar incidentes operacionales a través del sistema RIO en menos de 30 minutos desde que la entidad toma conocimiento, al tiempo que la nueva Ley Marco de Ciberseguridad impone alerta temprana junto con hitos subsiguientes en 72 horas, 7 días para el plan de acción y 15 días para el documento final [48].

Los plazos anteriores se computan desde el momento en que el evento se categoriza y se eleva al área correspondiente. Esta precisión debe figurar de forma expresa en la normativa y en los SOP, con el propósito de eliminar ambigüedades y de modo que el indicador de cumplimiento refleje la respuesta efectiva y no el ruido de la telemetría. Tal criterio previene, además, comunicaciones prematuras durante el triaje inicial.

Con el propósito de unificar la información expuesta y correlacionar los niveles de severidad delimitados en las secciones previas, la Tabla 4.1 que establezca el contenido mínimo, los destinatarios, el canal preferente, el vocero autorizado y los horizontes temporales para los distintos tipos de incidentes [30] [49].

Tabla 4.1: Canales, formatos y plazos regulatorios en la interacción con terceros.

Nivel de severidad	Stakeholder	Responsable de comunicación	Mensaje	Canal de comunicación	Plazos de notificación (desde confirmación)
P1 – Crítico	**Regulador financiero principal**	CEO/presidente del banco central, con apoyo del área legal y el CISO.	Notificación inicial de incidente grave, impacto potencial, acciones de contención en curso y compromiso de cooperación.	Canal formal designado por el regulador: portal seguro, correo cifrado o llamada directa.	Inmediato o según plazo más estricto (por ejemplo, menor a una hora o en un rango de 2 a 4 horas).
	CSIRT nacional y/o financiero	Líder CSIRT / CISO	Compartir IoC, TTP observados y solicitar apoyo/información si es necesario.	Plataforma de intercambio de inteligencia (como MISP) y correo seguro.	Tan pronto como sea posible para alertar a otras instituciones en el sector.
	Aseguradora	Oficial legal/gestor de siniestros con CISO	Hechos conocidos, potenciales impactos, medidas de contención en curso; solicitud de activación de póliza y confirmación del panel o de los proveedores autorizados.	*Hotline* 24/7 de la póliza y correo de reclamaciones indicado en condiciones particulares.	Inmediato (ideal 1–2 h) y siempre antes de incurrir en gastos cubiertos, para preservar el consentimiento.

	Forense digital / IR de panel	CISO	Activación del proveedor de panel o firma preaprobada, alcance inicial, cadena de custodia, imágenes forenses y contención táctica.	Canal habilitado por el asegurador o contrato marco.	Inmediato; sujeto al consentimiento del asegurador respectivo.
	Fuerzas y cuerpos de seguridad	El funcionario de legal o de seguridad designado.	Reporte formal del delito (si aplica) y provisión de pruebas según protocolos.	Contacto oficial.	Tan pronto como se determine la naturaleza delictiva y se asegure la evidencia.
	Otras entidades del sistema financiero, si el impacto es sistémico	CEO/presidente o vocero designado.	Información sobre el impacto en servicios interconectados, acciones de mitigación y tiempos estimados de restauración.	Canales de comunicación interbancarios acordados con antelación.	Dependiendo de la evaluación de impacto y de la coordinación.
	Medios de comunicación y público general	Vocero de crisis designado (previa aprobación de alta dirección y departamento legal)	Reconocimiento del incidente (si es público o inevitable), acciones tomadas para proteger a los usuarios/sistema, compromiso con su resolución y dónde obtener información actualizada.	Comunicado de prensa oficial, sitio web institucional y redes sociales oficiales (con moderación).	Cuando la información se encuentre verificada y sea estratégicamente necesario. Evitar comunicación prematura o imprecisa.

	Clientes/usuarios afectados directamente (si el banco central ofrece servicios directos al público o entidades)	Área de atención al cliente o de comunicaciones.	Información clara sobre el impacto en sus datos o servicios, qué deben hacer, cómo protegerse y canales de ayuda.	Correo directo, portal de clientes y SMS (con precaución por *phishing*).	Sin demora indebida, especialmente si existe riesgo para los individuos.
P2 - Alto	**Regulador financiero principal**	CISO o líder legal	Notificación de incidente alineada con umbrales regulatorios, impacto evaluado y plan de remediación.	Canal formal dispuesto.	Siguiendo los plazos regulatorios (por ejemplo, menor a 24 o 72 horas).
	Autoridad de protección de datos (si se materializa una brecha de PII)	Oficial de privacidad o líder legal	Notificación de brecha de datos personales según normativa.	Canal formal dispuesto.	En los plazos que imponga la ley de protección de datos (por ejemplo, 72h).
	CSIRT nacional o financiero	Líder CSIRT	Compartir IoC y TTP.	Plataforma de intercambio.	Según relevancia y oportunidad.
	Aseguradora	Legal/gestor de siniestros	Aviso formal conforme a póliza; validación de si procede panel o pre-aprobación de proveedores preferidos.	*Hotline*/correo póliza.	Temprano (mismas 24–72 h o antes, según póliza).
	Forense (si hay indicios técnicos relevantes)	CISO	Revisión preliminar, contención selectiva, orientación sobre telemetría y registro de tiempos para reclamación.	Canal asegurador.	Según evaluación de impacto (preferible 24 h).

P3 – Medio / P4 - Bajo	**Regulador financiero principal**	Generalmente no requerido a menos que exista una obligación concreta o necesidad de escalamiento.			
	CSIRT nacional o financiero	Líder CSIRT	Compartir IoC si son novedosos o de interés general.	Plataforma de intercambio.	Discrecional.

La matriz propuesta constituye una referencia práctica. En complemento a ella, cada organización debe:

- Caracterizar detalladamente a todos sus interlocutores relevantes y comprender sus expectativas en materia de información.
- Conocer de manera exhaustiva las obligaciones normativas de notificación en su jurisdicción, abarcando plazos, contenido requerido, formatos aceptados y canales oficiales.
- Preparar plantillas prediseñadas que contemplen diferentes situaciones y audiencias, susceptibles de ser ajustadas con rapidez.
- Establecer y verificar periódicamente los canales de transmisión, previendo alternativas en caso de fallas en los medios principales.

Configurada así, la estrategia no solo vela por el cumplimiento normativo, sino que también contribuye a controlar la narrativa pública, gestionar la percepción social y preservar la legitimidad institucional.

4.5 Registro y trazabilidad

Durante y después de un incidente resulta esencial conservar un histórico íntegro y verificable de la totalidad de las acciones efectuadas. Una bitácora de incidentes documenta de manera cronológica qué se realizó, en qué momento, por quién y bajo qué razonamiento, constituyéndose en una herramienta insustituible tanto para auditorías internas y evaluaciones retrospectivas como para eventuales investigaciones externas o requerimientos regulatorios. En virtud de ello, tal registro apoya múltiples áreas:

- Análisis forense, al reconstruir con precisión la secuencia de eventos y las medidas aplicadas.
- Adhesión a normativas y capacidades de auditoría, al proveer pruebas de diligencia debida y observancia de estándares aplicables.
- Extracción de lecciones aprendidas, reconociendo aciertos, deficiencias y oportunidades de perfeccionamiento.
- Potenciales acciones legales, dado que puede ser aprovechada en investigaciones criminales o disputas.
- Rendición de cuentas. Al dejar constancia clara de responsabilidades individuales en cada fase del incidente, ofrece un sustento objetivo para eventuales comunicaciones con terceros.

En este sentido, un registro bien estructurado debe ser claro, cronológico y exhaustivo, preferiblemente almacenado en un formato centralizado que contemple, como mínimo, los campos expuestos en la Tabla 4.2 para cada acción consignada en el formulario estándar de incidente (Tabla 3.2):

Tabla 4.2. Bitácora de acciones para la gestión de incidentes (ejemplo conceptual).

Campo	Descripción
ID del incidente	Identificador único del incidente al que se refiere la acción (enlace al formulario de incidente).
Fecha/hora (*timestamp*)	Fecha y hora exactas (con zona horaria) en que se realizó la acción.
Responsable	Nombre y rol de la persona que ejecutó la acción.
Descripción detallada de la acción	Qué se hizo específicamente en un texto claro y conciso, pero completo.
Herramientas utilizadas	Software, hardware o scripts empleados para la acción.
Resultado	¿Cuál fue el efecto de la acción? ¿se logró el objetivo esperado?
Evidencia recolectada / referencia	Hash de archivos, capturas de pantalla, nombres de archivos de log relevantes, número de tiquete de actividad programada que justifique el hallazgo, etc.
Observaciones / comentarios adicionales	Cualquier información adicional relevante, problemas encontrados, decisiones tomadas.
Estado de la tarea asociada (si se maneja como tareas)	Pendiente, en progreso, completada o bloqueada.

Cada entrada debe reflejar con nitidez qué sucedió y qué respuesta se implementó, trazando un hilo continuo desde la detección inicial hasta la restauración plena. Asimismo, es crucial que la bitácora sea actualizada en tiempo real o lo más cerca posible al desarrollo de las tareas asociadas a un caso.

Tal disciplina de documentación constituye un componente esencial en la gestión: aquello que no se consigna no puede ser posteriormente examinado ni perfeccionado. Lo anterior explica que los marcos de ciberseguridad insistan en la necesidad de una documentación meticulosa como parte del ciclo de aprendizaje y perfeccionamiento institucional [44].

4.6 Forense digital en el entorno financiero

En ecosistemas de pagos y liquidación de alto valor, la perspectiva forense se fundamenta en estándares técnicos que salvaguardan la integridad, la autenticidad y la cadena de custodia de la evidencia. La serie ISO/IEC 27037/27041/27042/27043 delimita: identificación, recolección, adquisición y resguardo (27037); aseguramiento metodológico y control de calidad de técnicas (27041); inspección pericial e interpretación (27042); y principios y procesos de investigación (27043). Las guías respectivas aconsejan, entre otras medidas, sincronización horaria confiable (NTP seguro), imágenes bit a bit con sumas criptográficas verificables (hashes), rotulado y embalaje adecuados, documentación cronológica granular de cada intervención y registros firmados o sellados digitalmente con fines de auditoría y eventuales actuaciones regulatorias o judiciales.

5 Lecciones aprendidas e institucionalización del conocimiento

5.1 Plantilla de post mortem

El análisis posincidente, conocido como *post mortem* o *after-action review*, constituye una revisión estructurada que, una vez restablecido el servicio, indaga con rigor qué ocurrió, por qué se produjo, qué funcionó, qué pudo ejecutarse mejor y qué transformaciones son necesarias para disminuir las recurrencias y elevar la calidad de la respuesta futura. Este ejercicio se sustenta en una cultura *blameless* que fomenta la transparencia: el foco recae en las condiciones del sistema que habilitaron modos de falla indeseados y no en la búsqueda de culpables.

A fin de lograr consistencia comparativa, una plantilla estandarizada organiza la información en secciones correctamente delimitadas: resumen ejecutivo conciso, cuantificación de la afectación, causas raíz y disparador, mecanismos de detección y tiempos asociados, cronología con marcas temporales verificables, acciones de mitigación y de recuperación propuestas, lecciones aprendidas y anexos técnicos (gráficas, registros, hilos de chat, paneles y documentación de soporte). Por lo tanto, nuevamente, se recurre al formulario 3.2, desde la sección 4 en adelante.

A continuación, se presenta una descripción ampliada de cada bloque, alineada con la plantilla y preparada para bancos centrales y entidades financieras [29] [50] [51].

1. **Resumen del incidente**
    - **Campos mínimos**: ID del incidente, fecha del *post mortem*, participantes y roles, fecha y hora de inicio, detección y resolución, duración total, breve descripción y severidad final (P1–P4).
    - **Fuentes y evidencia**: Tiquete del gestor de incidentes, página de estado, información del sistema de cambios, acta de cierre y referencia a la matriz de severidad.
    - **Criterios de calidad:** Brevedad sin ambigüedad, marcas temporales en una

única zona horaria, severidad alineada con criterios vigentes y enlaces navegables a documentos primarios.

2. **Afectación real (financiera, operativa, reputacional, regulatoria y CIA)**
    - Campos mínimos:
        - **Financiera**: costos directos (horas, servicios externos, reposición) e indirectos (penalidades, productividad), método de estimación y horizonte temporal.
        - **Operativa**: servicios y procesos afectados, ventanas de degradación/interrupción, usuarios/transacciones estimadas.
        - **Reputacional**: cobertura mediática, tono/sentimiento, número de quejas o consultas.
        - **Regulatoria/legal**: notificaciones realizadas (fechas y destinatarios), investigaciones en curso, riesgos sancionatorios.
        - **Confidencialidad, integridad y disponibilidad (CIA)**: descripción corta por pilar (confidencialidad, integridad y disponibilidad) con argumentos asociados.
    - **Fuentes y evidencia**: Tableros de control de producto, reportes de atención al cliente, recortes de prensa o monitor de medios, acuses de recibo de autoridades, actas de asesoría jurídica y artefactos forenses.
    - **Criterios de calidad**: Cifras verificables o estimaciones con metodología descrita, delimitación del alcance y correspondencia entre métricas y plazos.
3. **Cronología de eventos clave**
    - **Campos mínimos**: Tabla con *timestamp*, evento, responsable y enlace directo al sustento (log, cambio, captura, hilo de chat, etc.).
    - **Fuentes y evidencia**: Canales de coordinación, logs de instrumentos de monitoreo, órdenes de cambio, tareas del *runbook* o capturas de consola.
    - **Criterios de calidad**: Continuidad temporal sin vacíos, coherencia con otras secciones, referencias accesibles y diferenciación entre hechos e hipótesis.
4. **Análisis de causa raíz (RCA)**
    - **Campos mínimos**: Causa técnica inmediata (por ejemplo, explotación CVE-XXXX o regla errónea), indagatoria con técnica de los *5 Porqués*, fallas subyacentes (diseño, controles, factor humano, entre otros) y factores contribuyentes (carencia de parches, capacitación inadecuada, documentación desactualizada o falencias en la comunicación).

- **Fuentes y evidencia**: Bitácora de modificaciones en parámetros importantes, reportes posteriores a cambios, volcados forenses, trazas de aplicación y diagramas de arquitectura antes/después.
- **Criterios de calidad**: Separación explícita entre disparador y causa sistémica, profundidad suficiente para localizar fallas estructurales, vínculos a pruebas y ausencia de lenguaje acusatorio (enfoque sin culpabilización tácita).

5. **Evaluación de la respuesta**
   - **Campos mínimos**:
     - **Acciones inmediatas**: qué se ejecutó, por quién, cuándo y bajo qué criterio; distinguir entre contención, erradicación y restauración.
     - **Fortalezas**: herramientas, decisiones y coordinaciones que aceleraron la estabilización.
     - **Oportunidades de mejora**: carencias de datos, ambigüedad en los procedimientos, escalamiento tardío y cuellos de botella en la aprobación.
     - **Adherencia a planes**: qué se siguió y cuáles fueron las desviaciones, junto con su justificación.
     - **Comunicaciones**: oportunidad, consistencia, cumplimiento de hitos (1 h/24 h/72 h) y efectividad de canales alternos.
   - **Fuentes y evidencia**: Bitácora del incidente, actas del *war room* (espacios de trabajo donde el equipo asignado centraliza la información respecto al manejo de un incidente), registros de SOAR/SIEM, acuses regulatorios y plantillas de comunicación.
   - **Criterios de calidad**: Vínculo claro entre decisión y resultado; medición de tiempos (MTTD/MTTR), trazabilidad al procedimiento operativo y cobertura de la totalidad de los frentes (técnico, negocio y regulatorio).
6. **Lecciones aprendidas**
   - **Campos mínimos**: De 3 a 5 hallazgos en formato «observación $\rightarrow$ implicación $\rightarrow$ cambio propuesto», priorizados por riesgo y factibilidad.
   - **Fuentes y evidencias**: Retrospectiva de participantes, métricas históricas, repositorio de *post mortems* y auditorías internas.
   - **Criterios de calidad**: Enunciados accionables y no genéricos, alineación con los objetivos de resiliencia y relación explícita con las acciones del plan de mejora.
7. **Plan de acción y mejoras propuestas**

- **Campos mínimos**: Acción concreta, tipo (correctiva/preventiva), problema que aborda, responsable único, fecha objetivo, indicador de éxito, enlace al tiquete y prioridad.
- **Fuentes y evidencia**: *Backlog*, resultados de pruebas, métricas posteriores a la modificación y actas de comités de cambio.
- **Criterios de calidad**: Estado final verificable, dueño inequívoco, dependencias registradas y cierre validado con indicios técnicos.

De forma complementaria, se sugiere la incorporación de un apartado de antecedentes y glosario donde se reúna, con precisión documental, la arquitectura relevante del servicio afectado, sus dependencias internas y de terceros, las definiciones operativas y los supuestos que condicionan el funcionamiento cotidiano. Esta sección debe apoyarse en diagramas vigentes, manuales técnicos, contratos de servicio y catálogos de activos, de manera que cualquier lector —inclusive fuera del dominio— comprenda el contexto sin ambigüedades. La calidad se aprecia en una terminología consistente, referencias a la última versión de cada artefacto y un hilo narrativo adecuado.

En coherencia con lo expuesto y siguiendo las recomendaciones de Google [29], un *post mortem* de alta calidad se distingue por una organización expositiva nítida (terminología delimitada, secciones bien articuladas y ejemplos esclarecedores) y, sobre todo, por un conjunto de acciones concretas con un titular definido, folio de seguimiento, prioridades explícitas y un estado final verificable. Bajo una cultura *blameless*, el examen se orienta a reconocer los vacíos de diseño que habilitaron modos de falla indeseables y propicia una indagación profunda más allá del componente inmediato, tomando en cuenta impactos interárea, debilidades sistémicas y perspectivas diversas. Con fundamento en esto, la sección de impacto es equilibrada y objetiva, mientras que la de causa raíz y detonantes ofrece una inmersión analítica con conclusiones correctamente argumentadas. Asimismo, la celeridad añade valor: redactar y circular el informe dentro de la primera semana posterior al cierre fortalece la memoria institucional y favorece la ejecución del plan [29].

A fin de consolidar incentivos, la alta dirección debe avalar y promover estos ejercicios: modelar lenguaje sin culpabilización, invitar a todas las personas involucradas a actuar como coautores, recoger retroalimentación, revisar resultados, visibilizar mejoras de confiabilidad en reportes y presentaciones, así como proyectar a quienes lideran el proceso como referentes [29].

Adicionalmente, la difusión transversal potencia el aprendizaje: anuncios amplios, entrenamientos que recrean casos reales (*Wheel of Misfortune*) y reportes semanales consolidan prácticas maduras [29]. En paralelo, cuando surjan señales de disfunción cultural (distanciamiento, falta de refuerzo, escasez de tiempo para redactar o repetición de fallas análogas), conviene ahondar en preguntas como: ¿las acciones demoran

en cerrarse? ¿la velocidad de publicación o asimilación de nuevos*features* eclipsa la remediación? ¿las medidas propuestas abordan el problema correcto? ¿urge refactorizar el servicio? ¿se aplican paliativos a un defecto estructural más profundo?, entre otras.

Respecto a los componentes del soporte tecnológico y su alcance: la plataforma de conducción de incidentes debe precargar metadatos operativos en el *post mortem*: roles y responsabilidades del comandante del incidente (figura única encargada de dirigir la respuesta y coordinar al resto del equipo), cronología detallada y bitácoras de comunicación, catálogo de servicios impactados, nivel de severidad y mecanismo de detección inicial; esto con el objetivo de reducir inconsistencias documentales y preservar el contexto desde el primer borrador. Este preensamble automatizado, recomendado en los lineamientos de SRE de Google, provee una narrativa centrada en procesos y diseño, no en personas, y acelera la elaboración del informe sin sacrificar el rigor analítico [29]. Finalmente, es aconsejable que el sistema almacene los *post mortems* en una base de datos consultable que habilite paneles de tendencias (tiempos de detección y de resolución, reincidencias por servicio, tasa de cierre de acciones, etc.), revisiones cruzadas entre equipos y retroalimentación a la arquitectura.

5.2 Bases de conocimiento en el ciclo de incidentes

La base de conocimiento constituye el repositorio central donde se captura, depura y pone a disposición, de manera metódica, toda la información derivada de incidentes y de la revisión*post mortem*. De acuerdo con el *Computer Security Incident Handling Guide* del NIST, el propósito trasciende la mera acumulación documental: articula un corpus utilitario para la investigación, el aprendizaje institucional y el soporte operativo [50]. En ella deben converger registros normalizados, metadatos enriquecidos (como servicios afectados, severidad, tiempo hasta la detección y la restauración o controles implicados), taxonomías consensuadas y un vocabulario controlado que homologue términos, como TTP de adversarios, vectores de intrusión y familias de vulnerabilidades [50] [51]. Esta plataforma habilita:

- Análisis de tendencias a largo plazo, como patrones recurrentes por tipo de incidente, técnicas predominantes y causas raíz sistémicas.
- Mejoras en playbooks y SOP mediante retroalimentación continua.
- Fortalecer la formación y la concienciación con casos reales (anonimizados cuando aplique) para equipos CSIRT y audiencias no técnicas.
- Sustentar la toma de decisiones al suministrar justificación histórica para priorizar inversiones, ajustar políticas o rediseñar arquitecturas.

Para maximizar su valor, conviene contemplar indexación avanzada, etiquetas TLP (*Traffic Light Protocol*) para la clasificación de sensibilidad mediante colores que limitan la divulgación [52], control de versiones y curaduría editorial, líneas de tiempo correlacionadas, enlaces a artefactos probatorios y mecanismos de consulta que integren señales de SIEM/SOAR [51]. Por último, un ciclo de vida claramente definido —ingesta, revisión, publicación y caducidad—, junto con métricas de calidad (completitud, consistencia terminológica, trazabilidad hacia tiquetes y cronologías), acorta los tiempos de resolución al facilitar que el personal localice con rapidez incidentes análogos y soluciones que ya han demostrado eficacia en contextos comparables.

5.2.1 MITRE ATT&CK: base de conocimiento sobre tácticas y técnicas adversarias

- **Caracterización y arquitectura**: ATT&CK constituye un compendio público que recopila los TTP empleados por actores maliciosos. Se fundamenta en tres pilares: adoptar la perspectiva del atacante, basarse en observaciones empíricas y sostener un nivel de abstracción que vincule acciones ofensivas con medidas defensivas [53].
- **Aplicación en el sector**: ATT&CK se ha consolidado como un léxico compartido entre especialistas en ciberseguridad. Propicia la normalización de discusiones, la validación de contramedidas y la evaluación de soluciones comerciales. La actualización constante de este marco ayuda a los bancos centrales a mantenerse al corriente de nuevas técnicas y a armonizar sus protocolos de respuesta [53].
- **Matrices especializadas**: se han elaborado matrices para entornos corporativos, plataformas móviles y sistemas de control industrial (ICS), de modo que ATT&CK puede adaptarse a los distintos recursos que operan los bancos centrales. Además, el MITRE también ha consolidado la matriz ATLAS (*Adversarial Threat Landscape for Artificial-Intelligence Systems*) para agresiones dirigidas a herramientas de IA [54].

5.2.2 MITRE D3FEND 1.0: base de conocimiento defensiva

Desde su gestación en 2021 como iniciativa experimental auspiciada por la Agencia de Seguridad Nacional de Estados Unidos (NSA), D3FEND evolucionó hasta alcanzar la versión 1.0 anunciada en enero de 2025 [55]. Tal propuesta, concebida como contrapartida defensiva del modelo MITRE ATT&CK, constituye un repertorio terminológico que describe con rigor técnicas de defensa cibernética y examina la interdependencia entre topologías de red, vectores de amenaza y contramedidas [56]. De acuerdo con el

boletín de la NSA, el sistema habilita a los expertos a ajustar su postura frente a amenazas cibernéticas concretas y reduce la superficie de exposición de los sistemas [57]. La versión 1.0 se presentó como una ontología informática, definida como un modelo conceptual formalizado que describe entidades y relaciones en un dominio, con la finalidad de consolidar un vocabulario y una conceptualización homogénea del ámbito ciberdefensivo [55]. Tal estructura ontológica se diseñó para ofrecer un esquema estable, extensible y apto para integrarse en las operaciones de ciberseguridad y en la toma de decisiones estratégicas.

Entre las innovaciones de D3FEND 1.0 destacan [55]:

- **Cyber Attack-Defense (CAD) Tool**: instrumento de diagramación que materializa la ontología y brinda a los usuarios la capacidad de crear grafos semánticos mediante nodos interconectados, aplicar inferencias derivadas de D3FEND y compartir estos diagramas en redes públicas o privadas.
- **Ampliación del catálogo de técnicas defensivas**: incorpora nuevos conceptos relacionados con la administración de identidades y control de acceso, tecnología operativa y endurecimiento de código fuente; además incluye la enumeración de debilidades comunes (*Common Weakness Enumeration*, CWE) para modelar vulnerabilidades.
- **Precisión ontológica y capacidad de extensión**: apoyada en OWL 2 DL, una especificación del lenguaje de ontología web que viabiliza descripciones lógicas expresivas, tal que resulta factible alinear D3FEND con ontologías de nivel superior y propiciar aplicaciones semánticas de mayor alcance.
- **Estrategia de ciclo de vida del contenido**: orientada a garantizar actualizaciones previsibles y favorecer que las herramientas se ajusten al ritmo de evolución de la ontología.

5.2.3 Estructura sugerida de repositorios y sistema de etiquetado

La disposición física o lógica de la base de conocimiento puede adoptar distintos esquemas. En cualquier caso, la combinación de un esquema de directorios correctamente definido y un etiquetado multidimensional suele otorgar gran eficacia para consulta, trazabilidad y caracterización.

Un ejemplo de jerarquía de carpetas adecuada para auditoría y recuperación rápida podría ser:

```
    /Incidentes_Reportados/
 2025/
     05-Mayo/
        INC-2025-00123/
            00_Formulario_Incidente.pdf
            01_Bitacora_Acciones.xlsx
            02_Informe_PostMortem.pdf
            03_Evidencia_Digital/
               Logs/
               Capturas_Pantalla/
               Pcaps/
            04_Metadata/
                INC-2025-00123_metadata.json
     06-Junio/
         ...
/Lecciones_Aprendidas/
 Por_Tipo_Incidente/
    Ransomware/
    Fuga_Datos/
 Por_Causa_Raiz/
     Error_Configuracion/
     Vulnerabilidad_Software/
/IoC_Repositorio/
 IoC_Actuales.csv
 IoC_Historico/
 Integraciones/
     MISP/
/Playbooks_SOPs/
 Vigentes/
 Historico/
     Diffs_y_Publicaciones/
```

Contenido mínimo por carpeta:

`00_Formulario_Incidente.pdf`: Resumen del evento: fecha/hora de detección, alcance preliminar, activos afectados, severidad y contacto del líder.

`01_Bitacora_Acciones.xlsx`: Cronología minuto a minuto: acción, responsable, evidencia asociada y referencia de tiquete.

`02_Informe_PostMortem.pdf`: Causa raíz, lecciones, acciones correctivas/preventivas, métricas (MTTD/MTTC/MTTR) y enlaces a playbooks e IoC.

`03_Evidencia_Digital/`

- **Logs/**: archivos de SIEM, EDR, firewall, *proxy* o sistemas.
- **Capturas_Pantalla/**: pruebas visuales con marca temporal.

- **Pcaps/**: capturas de red para examinar el tráfico.

`/Lecciones_Aprendidas/` Dos vistas complementarias para consulta rápida: por tipo de incidente y por causa raíz. Cada entrada se enlaza al incidente origen y al *post mortem* respectuvi.

`/IoC_Repositorio/` Catálogo central (CSV/JSON) con campos normalizados: *ioc_type* (dominio, IP y hash), valor, *first_seen, last_seen*, fuente y relación con el incidente.

En paralelo, un sistema de etiquetado robusto, sustentado en etiquetas o metadatos normalizados, habilita búsquedas *ad hoc* y analítica transversal [58]. Cada etiqueta debe definirse en un vocabulario controlado con descripciones inequívocas y ejemplos, evitando sinónimos no estandarizados que deterioren la precisión de las consultas. Asimismo, resulta aconsejable imponer metadatos obligatorios —autor, fecha de creación, última actualización, referencia al tiquete maestro y relación con incidentes previos— en conjunto con reglas de retención y retirada que preserven el valor histórico sin sacrificar orden ni cumplimiento normativo. Así, la base de conocimiento se convierte en un tejido coherente de evidencia, contexto y aprendizaje reutilizable, donde la recuperación de información y el cruce entre casos se realiza con rapidez y rigor.

5.3 Indicadores Clave de Seguridad (KSI)

En el ámbito de incidentes, los indicadores clave de seguridad (*Key Security Indicators*, KSI) —en estrecha relación con los KPI (*Key Performance Indicators*) y KRI (*Key Risk Indicators*)— conforman el andamiaje métrico que posibilita a los bancos centrales monitorear la eficacia de la respuesta, descubrir brechas de desempeño, fundamentar inversiones en ciberdefensa y demostrar la validez del programa ante la alta dirección y demás partes interesadas.

Con fundamento en lo anterior, se propone el listado disponible en la Tabla 5.1, la cual se construye a partir de una taxonomía homogénea de incidentes e hitos temporales (inicio, alerta, validación, contención y recuperación), con periodicidad de medición, fuentes trazables (SIEM, EDR, SOAR, tiquetes y cronologías forenses) y notas de interpretación. Cada indicador queda caracterizado por su propósito (velocidad, eficacia, cobertura, impacto y cumplimiento), su método de cálculo, la frecuencia de revisión y las cautelas para evitar sesgos. Tal repertorio se apoya en NIST SP 800-61 r3, CPMI-IOSCO para resiliencia en infraestructuras de mercado, ENISA para tendencias sectoriales y FIRST para tiempos recomendados en CSIRT [59], junto con las propuestas de proveedores bien posicionados en la industria [60].

Tabla 5.1: Catálogo de indicadores clave de seguridad vinculados al manejo de incidentes.

KSI	Descripción	Frecuencia de medición sugerida	Fuente de datos	Consideraciones
MTTD (*Mean Time To Detect/Identify*)	Promedio desde el inicio estimado hasta la detección/identificación.	Mensual o trimestral	SIEM/EDR, *tickets* y *post mortem*	Meta: minutos u horas; requiere buena estimación del «inicio».
MTTA (*Mean Time To Acknowledge*)	Promedio desde la alerta hasta el acuse de recibo por un analista.	Diario (críticas), semanal y mensual (agregado)	Plataforma de alertas, SOAR y SIEM	Meta en críticas: 15-30 min; reduce latencia de investigación.
MTTC (*Mean Time To Contain*)	Promedio desde validación hasta contención efectiva (detener propagación/impacto).	Mensual o trimestral	*Tickets* y *post mortem*	Meta: horas en críticos; definir qué eventos cuentan como «contenidos».
MTTR (*Mean Time To Resolve/Recover*)	Promedio desde validación hasta restauración a estado normal.	Mensual o trimestral	*Tickets*, *post mortem* y monitoreo	Buscar tendencia descendente; vincular a RTO/RPO del negocio.
Tiempo de permanencia (*Dwell Time*)	Intervalo desde inicio estimado hasta contención.	Trimestral	SIEM, forense y *post mortem*	Indicador sintético de exposición; complementa MTTD y MTTC.
% incidentes detectados internamente	Proporción identificada por controles propios vs. terceros.	Mensual o trimestral	SIEM, canal de terceros y regulador	Mayor proporción interna sugiere detección proactiva.
Precisión de alertas (*Alert Precision/PPV*)	Porcentaje de alertas que resultan válidas.	Mensual	SIEM/SOAR y muestreo QA	Mejora al reducir falsos positivos; favorece MTTA/MTTD.

Cobertura de detección	Porcentaje de TTP con detecciones implementadas.	Trimestral	Matriz ATTCK, catálogos	Enlazar a controles y casos de uso por dominio/activo.
% incidentes con exfiltración confirmada	Casos con extracción de datos verificada.	Mensual o trimestral	Forense, DLP y *post mortem*	Termómetro de impacto en confidencialidad.
Cumplimiento de ventanas regulatorias	Incidentes notificados dentro de plazos oficiales.	Mensual	Registro de reportes	Refleja disciplina de reporte y calidad de cronologías.
Tiempo a notificación a autoridad	Promedio desde validación hasta envío al supervisor.	Mensual	Registro de reportes	Alinear con plazos nacionales/internacionales.
% incidentes repetidos (misma causa raíz)	Recurrencia por causa no erradicada.	Trimestral o anual	Base de conocimiento y *post mortem*	Meta cercana al 0 %. Exige trazabilidad de acciones correctivas.
Costo promedio por incidente	Media de costos directos/indirectos por evento.	Trimestral o anual	Finanzas, pólizas y *post mortem*	Desagregar por severidad y tipo; útil para priorización.
Volumen por severidad y tipo	Conteo por taxonomía y nivel de impacto.	Mensual o trimestral	*Ticketing* y SIEM	Vigilar picos en críticos o familias de ataque.
% cumplimiento de SLA de respuesta/-recuperación	Adherencia a compromisos internoso de terceros.	Mensual	*Ticketing* y contratos	Meta: 95-100 % según acuerdo.
Ejecución de ejercicios (*tabletop/red team*)	Porcentaje de *playbooks* ensayados en período.	Trimestral	Plan de pruebas y bitácoras	Incrementa cohesión y reduce tiempos en eventos reales.

% lecciones implementadas en un plazo fijo	Adopción de acciones posincidente.	Mensual	Registro de lecciones y PMO	Correlacionar con descenso de repetición de fallas.
Incidentes de terceros	Proporción atribuible a proveedores/tercerización.	Trimestral	Gestión de terceros y contratos	Dato clave para continuidad y debida diligencia.
Éxito de contención automatizada	Porcentaje de eventos contenibles por automatización que sí se contuvieron sin intervención manual.	Mensual	SOAR/EDR y *runbooks*	Mide eficacia de automatismos y reglas.
MTBSI (*Mean Time Between Significant Incidents*)	Intervalo medio entre eventos de alto impacto.	Trimestral	Registro histórico y severidad	Complementa tasa de eventos; útil para apetito de riesgo.

En cuanto a los rangos de referencia, el acceso a *benchmarks* granulares y actuales para el sector financiero latinoamericano suele presentar dificultades, puesto que la información no siempre es pública ni homogénea. Aun así, fuentes globales como el *Cost of a Data Breach Report* (realizado por IBM y el Ponemon Institute) otorgan datos por industria que contribuyen con la calibración inicial. Por ejemplo, la edición 2025 de IBM reporta un promedio mundial cercano a 241 días para identificar y contener una brecha (suma de MTTI y MTTC) y un costo medio de 5.56 millones de dólares para el sector financiero en EE.UU. [61], cifras útiles para fijar las expectativas, siempre que se consulten las versiones más recientes.

La práctica más valiosa para los bancos centrales de la región consiste en construir un repositorio de métricas anónimas y agregadas dentro del foro, a fin de crear benchmarks regionales con mayor pertinencia contextual. En complemento a ello, y más allá de la comparación externa, cada institución debería establecer su propia línea base para cada indicador y trazar objetivos de mejora a partir de esas mediciones internas, priorizando tendencias sostenidas y reducciones verificables en los tiempos de detección, contención y restablecimiento, así como incrementos en la cobertura de monitoreo, la precisión de alertas y el cumplimiento de hitos de notificación.

Por otra parte, las debilidades que emergen de manera reiterada en simulacros de incidentes, pruebas de penetración, auditorías internas o externas y *post mortem* señalan frentes que requieren atención preferente. Tales hallazgos no deben quedar confinados a informes puntuales, sino convertirse en insumos que guíen la evolución del programa de respuesta y refuercen la resiliencia institucional. Se sugiere,

- **Convertir hallazgos en requisitos de madurez**: Cuando los ejercicios de crisis indican la falta de coordinación comunicacional, se expone un rezago en la capacidad de gobernanza durante situaciones críticas. La aspiración consiste en avanzar hacia un nivel superior a través de la formalización de procedimientos, el entrenamiento sistemático de voceros y equipos clave, así como la revisión periódica mediante simulaciones.
- **Trasladar recurrencias a KSI y metas de mejora**: Si persiste una latencia elevada en la detección de cierto vector, es pertinente fijar un indicador centrado en reducir el MTTD asociado a este. De forma análoga, cuando las inspecciones apuntan a fallos continuos en el ciclo de parches, adquieren relevancia métricas como el porcentaje de cumplimiento de la política de actualización o el tiempo medio para aplicar correcciones críticas [60].

Este enfoque transforma los insumos en recursos de mejora verificable de la respuesta a incidentes y de la resiliencia integral de la entidad. Así, el estudio de tendencias y causas atribuidas al deterioro de un KSI habilita un ciclo de optimización continua, contribuyendo a la postura en seguridad de la organización.

6 Comunicación y colaboración interinstitucional

6.1 Protocolo de reporte a autoridades y foros interinstitucionales

La comunicación y la cooperación interinstitucional constituyen un andamiaje esencial para la ciberresiliencia del sector financiero público, debido a que un incidente en un banco central puede escalar, producir efectos en la red y derivar en impactos sistémicos. Por tal razón, conviene estructurar un protocolo de reporte que armonice expectativas entre supervisores, CSIRT sectoriales y foros regionales, articulando (i) criterios de incidentes reportables con umbrales homogéneos de impacto (disponibilidad, integridad, confidencialidad o alcance transfronterizo); (ii) semántica de campos FIRE para consistencia multipaís; (iii) controles de difusión sustentados en TLP con sanitización previa de datos personales; y (iv) mecanismos técnicos de intercambio compatibles con STIX (modelo de objetos de ciberinteligencia) y TAXII (transporte seguro sobre HTTPS), así como con repositorios colaborativos tipo MISP cuando proceda. Con ello, la notificación interinstitucional preserva la trazabilidad, favorece la correlación entre eventos y acelera la toma de decisiones coordinada.

En términos operativos, el primer eje comprende los disparadores de reporte: categorías del incidente, tales como una brecha de datos personales, una interrupción amplia de servicios críticos, un fraude material o un evento con potencial sistémico. La priorización se acota mediante umbrales de impacto que combinan métricas financieras, el número de afectados, la duración de la indisponibilidad y el alcance geográfico. El segundo eje aborda los plazos: horizontes temporales desde la detección o confirmación hasta la notificación inicial, con repercusiones administrativas cuando se incumplen. El tercer eje cubre el contenido requerido: naturaleza del incidente, estimación de las consecuencias, medidas de contención ya aplicadas, plan de remediación y, cuando corresponda, IoC, referencias CVE y mapeo a MITRE ATT&CK para aportar contexto táctico. El cuarto eje precisa autoridades y canales: superintendencias financieras, uni-

dades de inteligencia financiera, CSIRT nacionales, autoridades de protección de datos e infraestructuras de mercado cuando proceda, con envío por portal seguro, correo cifrado S/MIME o PGP, SFTP o TAXII, en concordancia con la instrucción formal.

A fin de cohesionar jurisdicciones dispares, resulta aconsejable mapear cada criterio local a FIRE y alinear campos mínimos con objetos STIX (por ejemplo, `indicator`, `observed-data`, `attack-pattern`, `vulnerability` o `marking-definition/TLP`). Esta cartografía reduce la fricción multipaís, robustece la trazabilidad y facilita el mapeo entre eventos en repositorios colaborativos como MISP, preservando la confidencialidad mediante TLP y técnicas de seudonimización cuando existan PII.

Así, se sugiere que el protocolo de reporte abarque las etapas descritas a continuación, referenciando directamente algunos de los contenidos desarrollados en capítulos previos (3 y 4):

1. **Detección y clasificación inicial**
    - Identificación del evento o de la vulnerabilidad.
    - Priorización con matriz de severidad, ponderando el impacto técnico, operativo, financiero y reputacional, así como la materialidad y el riesgo sistémico.
    - Comprobación de si el evento encaja en las categorías de «reportable» según la norma local y las guías FSB/CPMI-IOSCO.
2. **Activación interna**
    - Aviso inmediato a la alta dirección o CISO.
    - Despliegue del plan de incidentes del banco central y coordinación con forense digital, continuidad del negocio y comunicaciones.
    - Almacenamiento de evidencia y elaboración de la cadena de custodia.
3. **Informe inicial**
    - Campos esenciales: qué ocurrió, cuándo, servicios afectados, alcance preliminar y acciones inmediatas de contención.
    - Exclusión de PII, IoC granulares o descripciones de vulnerabilidades no requeridas en la primera notificación [62].
    - Marcado de difusión con TLP 2.0 y selección de audiencias autorizadas.
    - Reservar los anexos técnicos para canales apropiados (TAXII o MISP).
4. **Notificación a las autoridades nacionales**
    - Remisión dentro de ventanas regulatorias (por ejemplo, 36–72 h o sin demora indebida).

- Utilizar los canales seguros designados por el regulador [62] —por ejemplo, formularios en línea, correos electrónicos específicos o líneas telefónicas dedicadas (ver Tabla 1.1).

5. **Coordinación interinstitucional y foros sectoriales**
   - En escenarios con implicaciones sistémicas o que afecten infraestructuras de mercado, la coordinación se extiende al BIS/CPMI-IOSCO.
   - La conciencia situacional sectorial y el apoyo técnico se fortalecen a través de CSIRT/CERT nacionales o financieros [62].
   - FLAR: promover la cooperación mediante el intercambio regional y la discusión de lecciones aprendidas.
   - *Operational Security Situational Awareness Teleconference* (OSSAT): participar en teleconferencias del BCE para compartir información sobre ciberdelincuencia, vulnerabilidades y tendencias [63]. Este espacio reúne a bancos centrales, miembros del SEBC, BIS y otras instituciones financieras internacionales (como el FMI y el Banco Mundial).
   - FS-ISAC: flujos Share/Connect para TTP e IoC operables [64].
   - CISA/CIRCIA: cuando aplique por jurisdicción o cooperación federal.
6. **Intercambio técnico de ciberinteligencia (CTI)**
   - Formato STIX 2.1 (objetos `incident`, `indicator`, `observed-data` o `marking-definition`).
   - Transporte TAXII 2.1 hacia comunidades confiables.
   - Consumo o publicación en MISP.
   - Contexto táctico con MITRE ATT&CK y vida útil de los IoC.
7. **Actualizaciones y cierre**
   - Comunicaciones periódicas con hitos, describiendo el alcance, la remediación o los riesgos residuales.
   - Informe de cierre y enlace con lecciones aprendidas y KSI.
   - Preservar la coherencia semántica y la consistencia documental para auditoría y revisión de lecciones aprendidas.

6.2 Formatos estandarizados para intercambio de indicadores

La cooperación técnica entre autoridades y foros sectoriales demanda formatos normalizados que garanticen coherencia semántica y automatización. En ese terreno, STIX 2.x (*Structured Threat Information eXpression*) funciona como lenguaje de modelado para ciberinteligencia en JSON, con objetos bien tipificados que capturan indicadores de compromiso (IoC), datos observados, patrones de ataque, familias de malware, conjuntos de intrusión, campañas, cursos de acción, relaciones y avistamientos (*sightings*) (Figura 6.1). El esquema incluye marcas de difusión compatibles con TLP y referencias a vulnerabilidades (por ejemplo, CVE), lo que viabiliza contexto táctico y control fino de audiencia sin sacrificar trazabilidad [65].

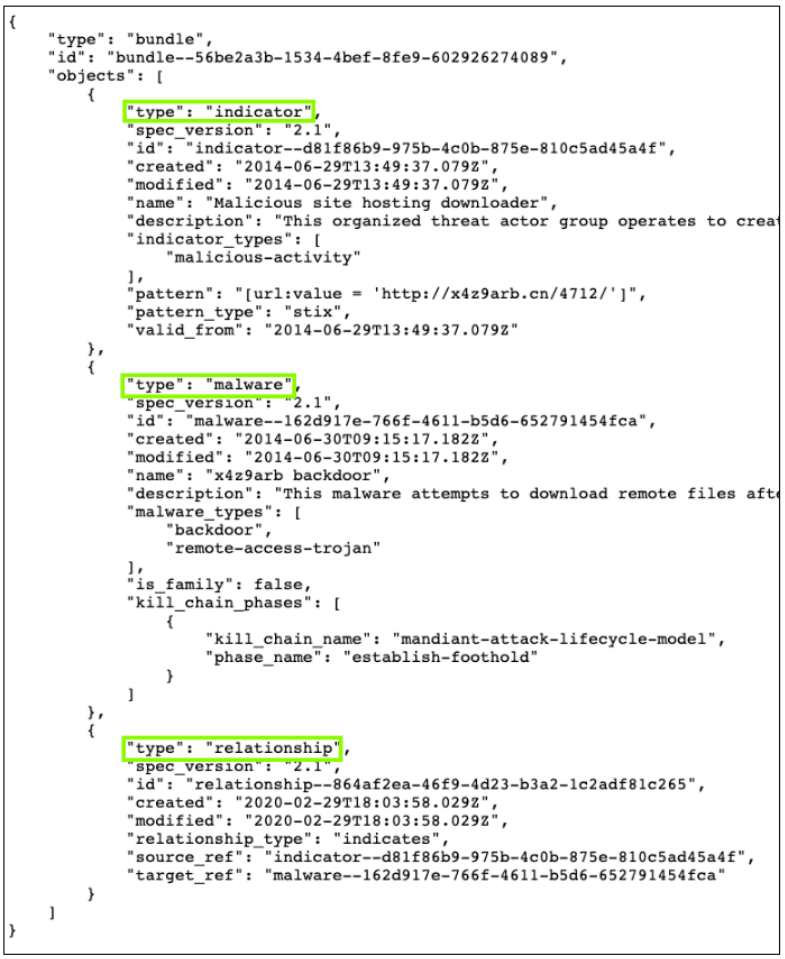


Figura 6.1: Formato STIX para un indicador de URL maliciosa. Fuente: *IR 380: STIX Threat Intelligence* [66].

Como complemento, TAXII (Trusted Automated eXchange of Indicator Information) provee el canal de transporte sobre HTTPS con descubrimiento, colecciones y endpoints para consulta, inserción y actualización de objetos STIX, además de estados de

ingesta, paginación y filtros por tiempo o tipo. Tal entramado aporta interoperabilidad entre CSIRT/CERT, reguladores y comunidades como FS-ISAC [65].

6.3 Repositorio colaborativo

6.3.1 Topologías y plataformas (SFTP, ISAC y MISP)

A continuación, se presentan topologías y plataformas que sirven como carriles técnicos complementarios.

SFTP seguro (Secure File Transfer Protocol)

Propósito: canal básico, de baja complejidad, para remitir archivos (por ejemplo, reportes de incidentes anonimizados, listados de IoC en CSV o texto estructurado).

Salvaguardas: autenticación fuerte (MFA y certificados del lado del cliente), cifrado de extremo a extremo, listas de control de acceso con segregación por entidad y registro detallado de descargas.

Ventajas: puesta en marcha rápida, amplia la combatibilidad, traza simple de intercambio y baja dependencia de software especializado.

Limitaciones: carencia de agrupación, búsqueda avanzada y orquestación de flujos. Adicionalmente, la administración operativa se complica a medida que se amplifica el volumen y la cantidad de participantes.

Buenas prácticas: *namespaces* por comunidad, políticas de retención y *hashing* de integridad. Además, guías de seudonimización para impedir la exposición de PII.

Portales de ISAC

De acuerdo con el Financial Services Information Sharing and Analysis Center [64]:

Modelo de referencia: FS-ISAC en el sector financiero; algunos portales se basan en MISP o en soluciones propietarias.

Capacidades: entrega de inteligencia accionable, apoyo a entidades afectadas, lectura del impacto sectorial y coordinación de respuesta entre pares.

Canales: flujos como *Share* (alertas y boletines) y *Connect* (debates confidenciales y salas de chat con TLP), con autenticación robusta y trazabilidad.

Comunidades de interés: creación de grupos acotados por subsector, temática o región para compartir material con granularidad adecuada.

Ventajas: curaduría experta, cobertura global y mecanismos de confianza entre los miembros. Además, integración con STIX/TAXII para el intercambio automatizado a través de HTTPS.

Consideraciones: gobernanza clara sobre quién publica, quién consume y qué marcas TLP rigen cada pieza. Adicionalmente, cerciorar la alineación con obligaciones locales para mantener equivalencias con FIRE del FSB.

Instancia MISP

Constituye una plataforma abierta orientada a IoC y conocimiento operativo sobre amenazas recientes, la cual normaliza, establece correspondencias y enriquece las evidencias técnicas, además de soportar exportaciones a STIX para automatizar flujos entre personas y sistemas.

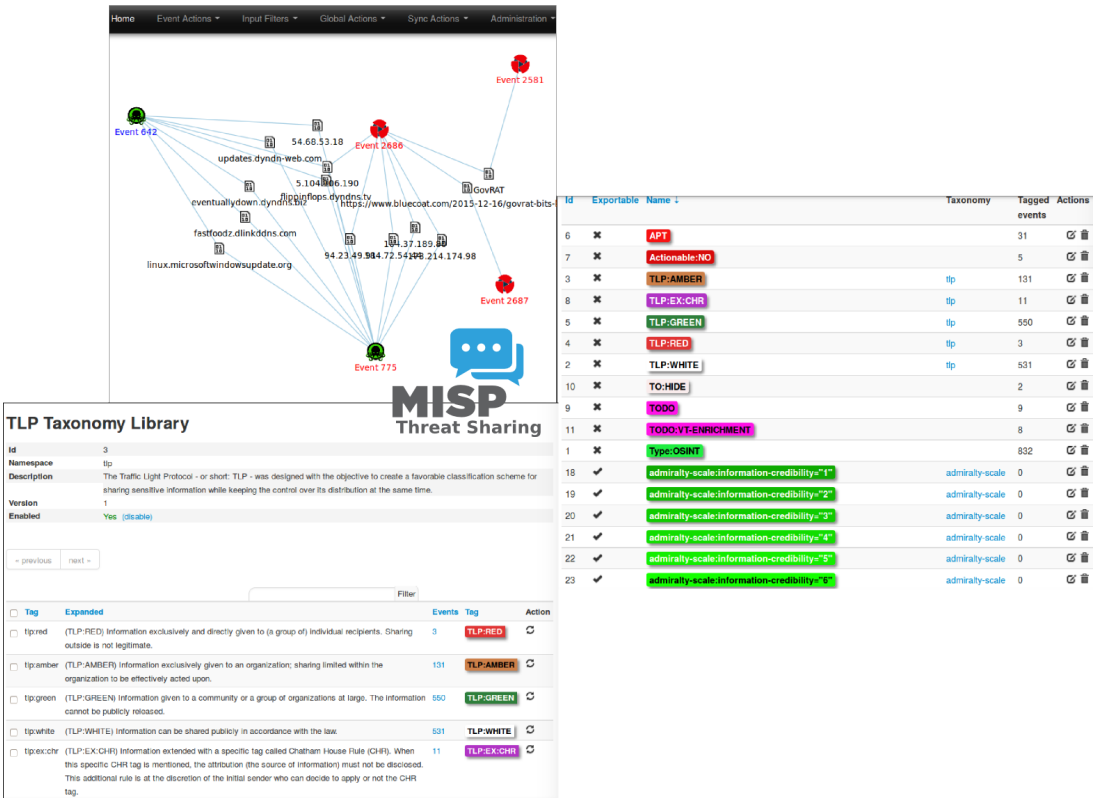


Figura 6.2: Componentes de la interfaz gráfica de MISP. Fuente: Repositorio de código-*MISP - Threat Intelligence Sharing Platform* [67].

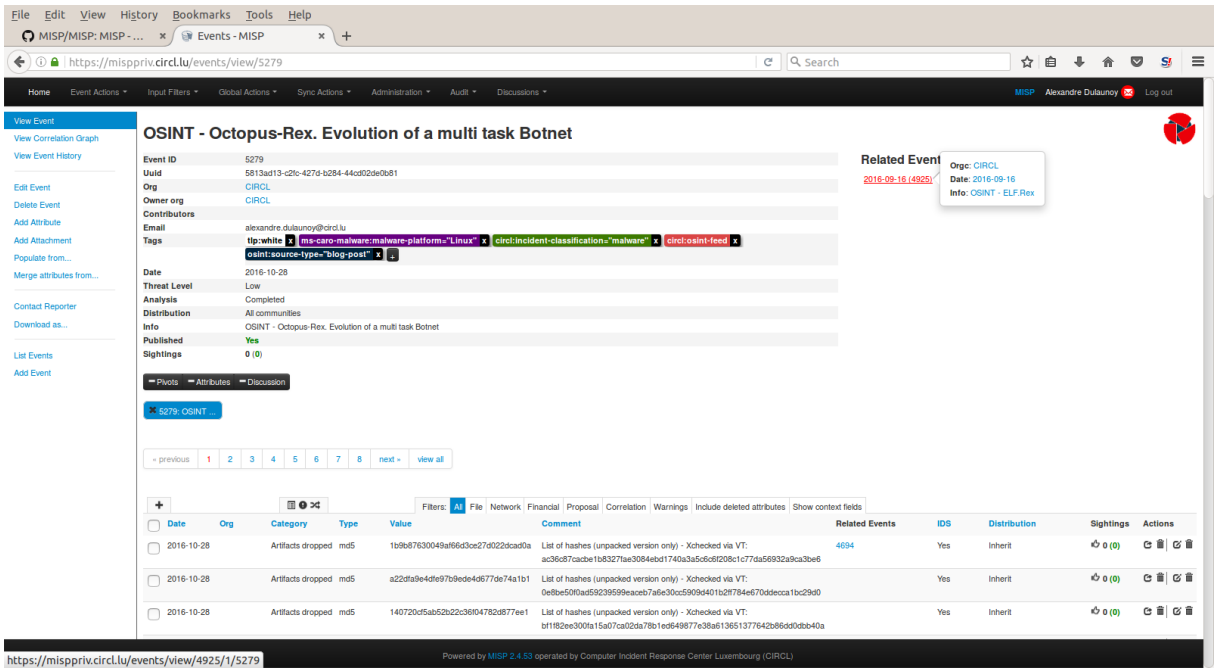


Figura 6.3: Vista de un evento codificado en MISP. Fuente: Repositorio de código*MISP - Threat Intelligence Sharing Platform* [67].

Comunidades: Equipos de malware y de seguridad operacional, inteligencia cibernética, DFIR y analistas de riesgo y fraude. En el sector financiero, opera tanto en grupos de confianza aislados (*air-gapped*) como en federaciones parcialmente conectadas, incluidos ISAC y operadores de pagos. Entre sus finalidades destacan la detección, el bloqueo y la inspección de campañas, siempre con prudencia frente a potenciales falsos positivos [68].

Capas: En la capa de datos, los «atributos» constituyen el bloque mínimo compartible (por ejemplo, dominio, IP, URL, hash o adjunto); sobre ellos, los «objetos» aportan plantillas estructuradas para describir entidades complejas; el «evento» actúa como contenedor con reglas de difusión y un *event report* en Markdown para narrativa humana y referencias internas [69]. Por su lado, la capa de contexto añade semántica mediante taxonomías y galaxias. Las primeras entregan vocabularios normalizados, mientras que las segundas incorporan metadatos ricos para representar conocimiento de alto nivel —por ejemplo, la matriz MITRE ATT&CK— y se interrelacionan entre sí, lo que potencia la navegación y el razonamiento en grafos [69].

Calidad y ciclo de vida: MISP posibilita la asociación entre eventos a partir de atributos coincidentes. En complemento a ello, define*warning lists* para reducir el ruido, avistamientos para la retroalimentación de vigencia y líneas de tiempo para visualizar la evolución. Además, admite interacciones con servicios externos mediante librerías (Shodan, VirusTotal, entre otros) y flujos de revisión antes de publicar.

Uso: En cuanto a la arquitectura, MISP puede desplegarse en una nube privada (por ejemplo, VPC sobre Amazon EC2), en contenedores [70] o en entornos *on-premise*. El

acceso operativo combina API para intercambios programáticos (sincronización con API key y reglas de selección *pull/push*) [69] e interfaz gráfica para intervención humana, entre otros para la redacción de reportes. Por otro lado, la integración con ecosistemas de detección (por ejemplo, SIEM, reglas y listas de bloqueo del firewall) aparece como una práctica habitual en las comunidades que buscan interrelación continua [71]. Finalmente, el control de difusión se expresa mediante niveles de distribución graduados: «solo mi organización», «solo esta comunidad», «comunidades conectadas», «todas las comunidades» y *sharing groups* [69].

Como buenas prácticas operativas, la entidad responsable de MISP subraya: titular eventos en inglés para lectura humana; priorizar objetos sobre atributos para enriquecer grafos; revisar las banderas to_ids —que concede la propagación a herramientas defensivas— y `correlation`; contextualizar en función de reglas de intercambios, tácticas del adversario, tipo de evento, familia de malware o tipo de incidente; acordar un vocabulario común con la comunidad; añadir tiempo (`first_seen`, `last_seen` y `sightings`) para gestionar vigencia [72]; comprobar las listas de alerta o definir las propias; y crear una descripción del evento en el reporte correspondiente.

Desde la perspectiva los encargados de la respuesta a incidentes, MISP favorece el intercambio bidireccional entre la plataforma y el ecosistema defensivo de la organización mediante el siguiente esquema de trabajo [71]:

1. Desde MISP se exportan artefactos hacia IDS/IPS (como Suricata, Bro o Snort), SIEM mediante un formato de evento común (*Common Event Format*, CEF), escáneres de host y motores de correlación en formatos OpenIOC, STIX 2.x, CSV o YARA, además de políticas DNS RPZ y grafos en Maltego.

2. En sentido inverso, flujos automáticos (sandbox de malware, *workbenches* de analistas o *feeds* de bajo valor que requieren mapeo) alimentan MISP, mientras que ZeroMQ (ZMQ) en modo publicador/suscriptor dispara eventos recién cargados para habilitar consultas en tiempo real y el módulo de *lookup expansion* coteja atributos contra registros del SIEM.

3. La retroalimentación operativa se consolida con avistamientos enviados desde IDS/IPS, *honeypots* o el propio SIEM —por ejemplo, validación de búsqueda de Splunk o comentarios sobre falsos positivos—, lo que permite refinar conjuntos de reglas en NIDS (N*etwork Intrusion Detection System*), derivar listas de bloqueo y zonas de política de respuesta (RPZ) en los DNS, así como formular directrices de detección a partir de IoC de modo automático o manual.

4. La API y PyMISP facilitan cargas masivas hacia el SIEM y la importación de indicadores desde herramientas externas, con notificaciones cuando dichos artefactos reaparecen en telemetría, fortaleciendo la alerta temprana, la caza de amenazas y la respuesta coordinada.

En un consorcio de bancos centrales, tres topologías para MISP resultan naturales: centralizada (instancia única operada por el foro), federada (instancias por entidad sincronizadas entre sí bajo acuerdos de confianza) e híbrida (hub común para material de alto interés, más nodos locales concentrados en necesidades particulares). La decisión depende de confianza, recursos y gobernanza sectorial, pudiendo combinar sincronización, feeds para entornos sin Internet y modelos *air-gapped* cuando la confidencialidad lo requiera.

6.3.2 Políticas de acceso

Las políticas de acceso del repositorio colaborativo deben regirse por los principios de *need-to-know* (necesidad de saber) y privilegio mínimo, con controles proporcionales a la sensibilidad de la información y trazabilidad completa sobre quién accede, qué consulta y cuándo lo hace.

- **Autenticación robusta (MFA)**: exigir MFA para todo ingreso — preferiblemente con tokens de hardware, certificados X.509 o aplicaciones TOTP— compaginado con políticas de bloqueo ante intentos fallidos y rotación periódica de credenciales.
- **Control de acceso basado en roles**: RBAC completado con permisos granulares de lectura, escritura y administración, alineados al rol funcional, la clasificación TLP y la pertenencia a grupos de intercambio. Adicionalmente, se sugiere segregar por colecciones y realizar recertificación periódica de privilegios.
- **Compromisos de confidencialidad**: requerir NDA (*non-disclosure agreement*) y, cuando aplique, MoU (*memorandum of understanding*) que delimiten el alcance, la propagación bajo control y las responsabilidades ante filtraciones.
- **Auditoría y trazabilidad**: instrumentar *logging* de accesos y acciones con sellado de tiempo, retención acorde al marco regulatorio y revisiones programadas.

6.3.3 Reglas de sanitización y esquemas de clasificación

Antes de difundir detalles sobre incidentes —en especial, cuando la circulación sea anónima o alcance audiencias amplias— conviene eliminar o seudonimizar todo elemento que pueda identificar a la entidad que reporta o a personas vinculadas (clientes o colaboradores); ejemplos típicos son nombres de host, direcciones IP internas, usuarios, rutas de archivos o tiquetes internos. Así, solo se conservarán identificadores cuando exista un acuerdo expreso para una investigación conjunta y con controles de divulgación acordes. Los procedimientos deben quedar normalizados, aplicarse de forma consistente y registrarse con trazabilidad.

En cuanto a la clasificación, se sugiere TLP 2.0, un sistema para determinar la sensibilidad y las reglas de redistribución a través de los siguientes distintivos [52]:

- **TLP:RED**. Impone acceso circunscrito a los asistentes o al círculo de confianza designados y prohíbe cualquier difusión adicional. Se emplea para materiales altamente sensibles, cuyo manejo inadecuado supondría un grave impacto.
- **TLP:AMBER**. Difusión dentro de la organización receptora y con aliados que necesiten conocer para prevenir o mitigar. No se publica ni se remite fuera de ese perímetro.
- **TLP:AMBER+STRICT**. Variante que restringe el alcance exclusivamente a la entidad receptora, excluyendo a terceros.
- **TLP:GREEN**. Intercambio con pares y asociados dentro de la comunidad o el sector. No apto para canales abiertos.
- **TLP:WHITE**. Divulgación sin restricciones, sujeta a derechos de autor.

El procesamiento y etiquetado de la información debe ser congruente con el RGPD y con las políticas internas de cada banco central, acorde a las exigencias en torno a periodos de retención, criterios de minimización y registros de consentimiento cuando corresponda.

6.4 VERIS como marco de catalogación y puente semántico hacia FIRE

VERIS (*Vocabulary for Event Recording and Incident Sharing*) ofrece un esquema JSON con enumeraciones controladas que describen, con precisión reproducible, los actores (`Activist`, `Auditor`, `Competitor`, `Customer`, `Force Majeure`, `Former Employee`, `Nation-State`, `Organized Crime`, entre otros), las acciones (*hacking*, phishing, malware, etc.), los activos comprometidos, los atributos de impacto (confidencialidad, integridad o disponibilidad), la cronología y las labores de contención [73]. Su adopción como lenguaje común dentro del repositorio puede robustecer la comparabilidad entre organizaciones y facilitar el acoplamiento con flujos de ciberinteligencia operativos.

MISP cuenta con taxonomías y etiquetas que permiten rotular eventos con categorías VERIS sin perder granularidad [71]. La práctica recomendada es: (i) catalogar el caso con etiquetas VERIS en el evento y, cuando aplique, en objetos o atributos concretos; (ii) complementar con TLP 2.0 para controlar la difusión; (iii) asociar galaxias pertinentes (por ejemplo, MITRE ATT&CK) que expresen tácticas o patrones de ataque. Con ello, la comunidad obtiene un grafo semántico coherente, apto para la correlación, el

enriquecimiento y la búsqueda avanzada.

En el plano de intercambio máquina-a-máquina, STIX sirve para representar el registro VERIS mediante objetos como `incident`, `observed-data`, `attack-pattern`, `malware`, `infrastructure`, `identity` y `relationship`. Las enumeraciones VERIS pueden quedar reflejadas en `object_marking_refs`, `labels` o `external_references` hacia el diccionario correspondiente, dado que el propio estándar STIX contempla referencias a entradas VERIS/VCDB [74].

Por último, mientras que FIRE fija un conjunto mínimo de campos transfronterizos para la notificación a las autoridades, VERIS aporta el andamiaje narrativo y la taxonomía forense que sustentan esos mismos campos: qué ocurrió, a quién afectó, cómo y con qué impacto.

Conclusión

La obra propone un marco integral para bancos centrales latinoamericanos que compagina gobernanza, identificación automatizada y decisión táctica con respuesta coordinada y cooperación regional. Primero, la dirección estratégica ancla propósitos, alcance y principios; armoniza procesos con referencias de clase mundial (NIST SP 800-61 Rev.3 e ISO/IEC 27035); consolida roles esenciales; y activa un ciclo de mejora basado en madurez. Luego, el pipeline de SIEM/EDR depura señales, aplica criterios homogéneos de verificación y entrega salidas priorizadas; dichas alertas transitan por taxonomías claras, formularios normalizados y una matriz de escalamiento que pauta severidades P1–P4 y destinatarios. A partir de ahí, los procedimientos operativos estándar (SOP) guían la contención y la recuperación ante escenarios críticos (ransomware, fuga de datos personales, indisponibilidad, fraude o phishing/BEC), mientras la comunicación estratégica orquesta mensajes con partes interesadas; todo ello queda respaldado por trazabilidad y prácticas forenses idóneas para el entorno financiero.

En paralelo, el documento institucionaliza el aprendizaje: *post mortem* con plantilla, bases de conocimiento enlazadas a MITRE ATT&CK y MITRE D3FEND e indicadores clave de seguridad que transforman hallazgos recurrentes en metas de desempeño. La dimensión interinstitucional cierra el ciclo: protocolo de reporte a autoridades y foros, estándares para intercambios (STIX/TAXII, con TLP 2.0), repositorios colaborativos sobre MISP y VERIS como vocabulario que actúa como puente semántico hacia FIRE en notificaciones que abarcan múltiples jurisdicciones.

En conjunto, la arquitectura descrita eleva la resiliencia sectorial, refuerza la estabilidad del sistema y provee trazas verificables de desempeño a lo largo de todo el ciclo de incidentes.

Referencias

[1] Ashden Fein, Micaela McMurrough, Caleb Skeath, Moriah Daugherty, Sierra Stubbs y Krissy Chapman. *NIST Publishes Updated Incident Response Recommendations and Considerations*. Covington y Burling. 2025. URL: https://www.insideprivacy.com/cybersecurity-2/nist-publishes-updated-incident-response-recommendations-and-considerations/ (vid. pág. 5).

[2] *ISO/IEC 27035 Information Security Incident Management – Training Courses*. Professional Evaluation y Certification Board. n.d. URL: https://pecb.com/en/education-and-certification-for-individuals/iso-iec-27035 (vid. pág. 5).

[3] *Incident Response Frameworks Explained*. Lumifi Cyber. 2025. URL: https://www.lumificyber.com/fundamentals/incident-response-frameworks-explained/ (vid. pág. 5).

[4] Superintendencia Finaciera de Colombia (SFC). *Conceptos Formato 408 Métricas e indicadores de SI y CS CE033-20*. 2021. URL: https://www.superfinanciera.gov.co/loader.php?lServicio=Tools2&lTipo=descargas&lFuncion=descargar&idFile=1060320 (vid. págs. 7, 29).

[5] Comisión Nacional Bancaria y de Valores. *ANEXO 64 Incidentes de afectación en materia de seguridad de la información*. 2018. URL: https://www.cnbv.gob.mx/Anexos/Anexo%2064%20CUB.pdf (vid. pág. 7).

[6] Banco Central do Brasil. *Resolução CMN n° 4.893 de 26/2/2021*. 2021. URL: https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?numero=4893&tipo=Resolu%C3%A7%C3%A3o%20CMN (vid. pág. 8).

[7] Banco Central do Brasil. *Resolução BCB n° 368 de 25/1/2024*. 2024. URL: https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o%20BCB&numero=368 (vid. pág. 8).

[8] Seguros y Administradoras Privadas de Fondos de Pensiones La Superintendenta de Banca. *Resolución S.B.S. nº 504-2021*. 2021. URL: https://intranet2.sbs.gob.pe/dv_int_cn/2046/v2.0/Adjuntos/504-2021.R.pdf (vid. pág. 8).

[9] Banco Central de la República Argentina. *Lineamientos para la Respuesta y Recuperación ante Ciberincidentes (RRCI). Adecuaciones.* 2025. URL: https://www.bcra.gob.ar/Pdfs/comytexord/A8280.pdf (vid. págs. 9, 50).

[10] Comisión para el Mercado Financiero (CMF). *Norma de carácter general n°529*.

2024. URL: https://www.cmfchile.cl/normativa/ncg_529_2024.pdf (vid. pág. 9).

[11] Banco Central del Uruguay. *Comunicación n° 2024/018 Comunicación de eventos vinculados a Tecnología, Sistemas y Seguridad de la Información – Actualización*. 2024. URL: https://www.bcu.gub.uy/Comunicados/seggco24018.pdf (vid. pág. 9).

[12] Gobierno del Uruguay. *Decreto N° 66/025*. 2025. URL: https://www.impo.com.uy/bases/decretos/66-2025 (vid. pág. 9).

[13] Tamara Franklin. *Where do execs fit into an incident management process?* Liquid Web. n.d. URL: https://www.liquidweb.com/blog/incident-management-process/ (vid. pág. 10).

[14] *Guide to Cyber Security Incident Response*. Evalian. n.d. URL: https://evalian.co.uk/guide-to-incident-response/ (vid. págs. 10, 26, 38).

[15] *Roles and responsibilities in Incident Detection and Response*. Amazon Web Services. n.d. URL: https://docs.aws.amazon.com/IDR/latest/userguide/idr-raci.html (vid. págs. 11, 13).

[16] Jonathan Jackson. *Incident Managment Process*. Computing y Telecommunications Services Wright State University. n.d. URL: https://www.wright.edu/sites/www.wright.edu/files/page/attachments/Incident_Management1.pdf (vid. págs. 11, 13).

[17] *Good Practice Guide for Incident Management*. European Network e Information Security Agent (ENISA), 2010. URL: https://www.enisa.europa.eu/sites/default/files/publications/Incident_Management_guide.pdf (vid. págs. 11, 38-40).

[18] Richard A. Caralli, Julia H. Allen, David W. White, Lisa R. Young, Nader Mehravari y Pamela D. Curtis. *CERT® Resilience Management Model, Version 1.2*. Carnegie Mellon University's Software Engineering Institute, 2016. URL: https://www.sei.cmu.edu/documents/1629/CERT_Resilience_Management_Model_Version_1_2.pdf (vid. pág. 17).

[19] *CMMI Levels of Capability and Performance*. ISACA, n.d. URL: https://cmmiinstitute.com/learning/appraisals/levels (vid. pág. 17).

[20] *Cyber Resilience Review (CRR)*. U.S. Department of Homeland Security Cybersecurity e Infrastructure Security Agency (CISA), 2020. URL: https://www.cisa.gov/sites/default/files/c3vp/csc-crr-method-description-and-user-guide.pdf (vid. pág. 17).

[21] *Cyber Resilience Review (CRR) Question Set with Guidance*. U.S. Department of Homeland Security Cybersecurity e Infrastructure Security Agency (CISA), 2020. URL: https://www.cisa.gov/sites/default/files/c3vp/csc-crr-question-set-and-guidance.pdf (vid. págs. 18-20).

[22] *How Banks Can Achieve PCI DSS Compliance with Google Chronicle SIEM*. Cyber-

Proof Research Team. 2025. URL: https://www.cyberproof.com/blog/how-banks-can-achieve-pci-dss-compliance-with-google-chronicle-siem/ (vid. pág. 21).

[23] *What Is the Role of AI and ML in Modern SIEM Solutions?* Palo Alto Networks. n.d. URL: https://www.paloaltonetworks.com/cyberpedia/role-of-artificial-intelligence-ai-and-machine-learning-ml-in-siem#the (vid. pág. 21).

[24] Anne Aarness. *What is Endpoint Detection and Response (EDR)*. CrowdStrike. 2025. URL: https://www.crowdstrike.com/en-us/cybersecurity-101/endpoint-security/endpoint-detection-and-response-edr/ (vid. pág. 22).

[25] Luke Hunsinger. *EDR vs MDR vs XDR*. CrowdStrike. 2025. URL: https://www.crowdstrike.com/en-us/cybersecurity-101/endpoint-security/edr-vs-mdr-vs-xdr/ (vid. pág. 23).

[26] *How the Probability and Impact Matrix Enhances Risk Management*. SearchInform. n.d. URL: https://searchinform.com/articles/risk-management/tools/probability-and-impact-matrix/ (vid. pág. 24).

[27] *Common Taxonomy for Law Enforcement and The National Network of CSIRTs*. European Network e Information Security Agent (ENISA), 2017. URL: https://www.europol.europa.eu/cms/sites/default/files/documents/common_taxonomy_for_law_enforcement_and_csirts_v1.3.pdf (vid. pág. 30).

[28] *Format for Incident Reporting Exchange (FIRE)*. Financial Stability Board (FSB), 2025. URL: https://www.fsb.org/uploads/P150425-1.pdf (vid. págs. 35, 38).

[29] Betsy Beyer, Niall Richard Murphy, David K. Rensin, Kent Kawahara y Stephen Thorne, eds. *The Site Reliability Workbook: Practical Ways to Implement SRE*. Disponible en línea en el sitio oficial de Google SRE. Sebastopol, CA: O'Reilly Media, 2018. URL: https://sre.google/workbook/table-of-contents/ (vid. págs. 35, 58, 61, 62).

[30] Mary Brooks y Sofia Lesmes. *Cybersecurity Incident and Breach Reporting Requirements*. R Street Institute. 2022. URL: https://www.rstreet.org/commentary/cybersecurity-incident-and-breach-reporting-requirements/ (vid. págs. 38, 39, 50).

[31] *What is an Incident Response Retainer, Key Features and Benefits, and Why It Matters?* Sygnia. 2025. URL: https://www.sygnia.co/blog/what-is-incident-response-retainer/ (vid. pág. 42).

[32] Mitangi Parekh. *What is an Incident Response Retainer?* eSentire. 2025. URL: https://www.esentire.com/cybersecurity-fundamentals-defined/glossary/what-is-an-incident-response-retainer (vid. págs. 42, 43).

[33] *When to Notify Your Cyber Carrier of a Security Incident*. Troutman Pepper Locke. 2025. URL: https://www.consumerfinancialserviceslawmonitor.com/2025/03/when-to-notify-your-cyber-carrier-of-a-security-incident/ (vid. pág. 43).

[34] Anthony Hess. *Cyber Insurance Vendor Panels: A Guide to Smart Decision Making*. Howden Group Holdings. 2023. URL: https://www.howdengroup.com/uk-en/benefits-of-insurers-cyber-response-panel (vid. pág. 43).

[35] *Cyber war clauses*. Lloyd's Market Association. n.d. URL: https://lmalloyds.com/specialist-areas/underwriting/wordings/cyber-war-clauses/ (vid. pág. 43).

[36] *Updated Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments*. Department of the Treasury. 2021. URL: https://ofac.treasury.gov/media/912981/download?inline (vid. pág. 43).

[37] Steven Hadwin, Jamie Monck-Mason y Willis Towers Watson. *Cyber Insurance: an overview*. Thomson Reuters, 2020. URL: https://www.wtwco.com/-/media/wtw/insights/2020/08/cyber-insurance-an-overview.pdf (vid. pág. 43).

[38] *Guía para StopRansomware*. Grupo de trabajo conjunto contra el ransomware de los Estados Unidos (JRTF), 2023. URL: https://www.cisa.gov/sites/default/files/2023-06/stopransomware_guide_final_es.pdf (vid. págs. 44, 45).

[39] *Data Breach Response: A Guide for Business*. Federal Trade Commission. 2023. URL: https://www.ftc.gov/business-guidance/resources/data-breach-response-guide-business (vid. pág. 45).

[40] *Responding to a DoS attack*. National Cyber Security Centre (NCSC). 2024. URL: https://www.ncsc.gov.uk/collection/denial-service-dos-guidance-collection/a-minimal-denial-of-service-response-plan (vid. pág. 46).

[41] *Handling Financial Cybercrimes Standard Operating Procedures*. Cybersecurity Awareness y Creative Handholding Kendra, 2022. URL: https://cawach.gujgov.edu.in/dist/documents/sop/cyberAwareness/Handling_Financial_Cyber_Crimes.pdf (vid. pág. 46).

[42] Iván Abarca. *Construyendo ciber resiliencia en la industria financiera*. Banco Central de Chile. 2023. URL: https://www.bcentral.cl/contenido/-/detalle/construyendo-ciber-resiliencia-en-la-industria-financiera (vid. pág. 47).

[43] *Respond to a compromised cloud email account*. Microsoft. 2025. URL: https://learn.microsoft.com/en-us/defender-office-365/responding-to-a-compromised-email-account (vid. pág. 47).

[44] República Argentina - Poder Ejecutivo Nacional. *Guía de Notificación y Gestión de Incidentes de Ciberseguridad*. 2023. URL: https://www.argentina.gob.ar/sites/default/files/infoleg/disp3-386227.pdf (vid. págs. 49, 56).

[45] *Gestión de seguridad de la información y ciberseguridad*. Comisión para el Mercado Financiero, 2020. URL: https://www.cmfchile.cl/portal/prensa/615/articles-29314_doc_pdf.pdf (vid. pág. 49).

[46] *Final Rule on Computer-Security Incident Notification Requirements for Banking Organizations and Their Service Providers*. Federal Deposit Insurance Corporatio. 2021. URL: https://www.fdic.gov/news/board-matters/2021/2021-11-17-n

otational-mem.pdf (vid. pág. 50).
[47] *Joint draft Technical Standards on major incident reporting*. European Banking Authority, 2024. URL: https://www.eba.europa.eu/sites/default/files/2024-07/6d341d14-0c54-44ff-a849-21561baee157/JC%202024-33%20-%20Final%20report%20on%20the%20draft%20RTS%20and%20ITS%20on%20incident%20reporting.pdf (vid. pág. 50).
[48] Miniterio del Interior y Seguridad Pública. *Ley 21663 | Ley Marco de Ciberseguridad*. 2023. URL: https://www.bcn.cl/leychile/navegar?i=1202434 (vid. pág. 50).
[49] Comisión para el Mercado Financiero (CMF). *Norma de Gestión de Riesgo Operacional de Sociedades Administradoras de Sistemas de Compensación y Liquidación, Empresas de Depósito y Custodia de Valores, Bolsas de Valores, Bolsas de Productos, Intermediarios de Valores, corredores de Bolsas de Productos y Administradoras Generales de Fondos*. 2023. URL: https://www.cmfchile.cl/institucional/legislacion_normativa/normativa_tramite_ver_archivo.php?id=2023080854&seq=1 (vid. pág. 50).
[50] *Computer Security Incident Handling Guide*. National Institute of Standards y Technology (NIST), 2025. URL: https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf (vid. págs. 58, 62).
[51] *CRR Supplemental Resource Guide Incident Management*. Carnegie Mellon University, 2016. URL: https://www.cisa.gov/sites/default/files/c3vp/crr_resources_guides/CRR_Resource_Guide-IM.pdf (vid. págs. 58, 62, 63).
[52] *Traffic Light Protocol (TLP) Definitions and Usage*. U.S. Department of Homeland Security Cybersecurity e Infrastructure Security Agency (CISA). 2022. URL: https://www.cisa.gov/news-events/news/traffic-light-protocol-tlp-definitions-and-usage (vid. págs. 63, 80).
[53] *¿Qué es el MITRE ATTCK Framework?* Trend Micro. n.d. URL: https://www.trendmicro.com/es_es/what-is/cyber-attack/mitre-attack-framework.html (vid. pág. 63).
[54] Varun Kumar. *MITRE ATLAS Framework 2025 – Guide to Securing AI Systems*. Practical DevSecOps e Hysn Technologies. 2025. URL: https://www.practical-devsecops.com/mitre-atlas-framework-guide-securing-ai-systems/ (vid. pág. 63).
[55] Va. McLean y Mass Bedford. *MITRE Launches D3FEND 1.0 – A Milestone in Cybersecurity Ontology*. MITRE Corporation. 2025. URL: https://www.mitre.org/news-insights/news-release/mitre-launches-d3fend-10-milestone-cybersecurity-ontology (vid. págs. 63, 64).
[56] Abby Curtis. *What Is MITRE D3FEND?* Splunk. 2024. URL: https://www.splunk.com/en_us/blog/learn/mitre-defend.html (vid. pág. 63).
[57] *NSA Funds Development, Release of D3FEND*. National Security Agency (NSA).

2021. URL: https://www.nsa.gov/Press-Room/Press-Releases-Statements/Press-Release-View/Article/2665993/nsa-funds-development-release-of-d3fend/ (vid. pág. 64).

[58] Mike Simon. *Contextual Observability: Using Tagging and Metadata To Unlock Actionable Insights*. Splunk. 2025. URL: https://www.splunk.com/en_us/blog/observability/contextual-tagging-metadata.html (vid. pág. 66).

[59] *Security Incident Timing Metrics version 1.0 Specification Document*. Forum of Incident Response y Security Teams (FIRST), 2023. URL: https://www.first.org/global/sigs/metrics/Security-Incident-Timing-Metrics_v1.0.pdf (vid. pág. 66).

[60] *Cybersecurity Metrics KPIs: What to Track in 2025*. SentinelOne. 2025. URL: https://www.sentinelone.com/cybersecurity-101/cybersecurity/cybersecurity-metrics/ (vid. págs. 66, 70).

[61] *Cost of a Data Breach Report 2025 The AI Oversight Gap*. IBM y Ponemon Institute, 2025. URL: https://www.ibm.com/es-es/reports/data-breach (vid. pág. 70).

[62] *Cyber Incident Reporting Guide*. National Credit Union Administration. 2025. URL: https://ncua.gov/regulation-supervision/regulatory-compliance-resources/cybersecurity-resources/cyber-incident-reporting-guide (vid. págs. 72, 73).

[63] *Meeting of the CBCG Council was held*. Central Bank of Montenegro. 2025. URL: https://www.cbcg.me/en/public-relations/news/press-releases/meeting-of-the-cbcg-council-was-held?id=2868 (vid. pág. 73).

[64] *Sharing and Communications During an Incident*. FS-ISAC. n.d. URL: https://www.fsisac.com/incident-response (vid. págs. 73, 75).

[65] Adam Goss. *STIX/TAXII: A Complete Guide to Automated Threat Intelligence Sharing*. Kraven Security. 2025. URL: https://kravensecurity.com/stix-and-taxii-a-full-guide/ (vid. págs. 74, 75).

[66] Sam Bowne. *IR 380: STIX Threat Intelligence*. 2022. URL: https://samsclass.info/152/proj/IR380.htm (vid. pág. 74).

[67] *MISP - Threat Intelligence Sharing Platform*. Computer Incident Response Center Luxembourg (CIRCL). n.d. URL: https://github.com/MISP/MISP?tab=readme-ov-file (vid. págs. 76, 77).

[68] *Una introducción al Intercambio de Información de Ciberseguridad - MISP - Threat Sharing*. Computer Incident Response Center Luxembourg (CIRCL). 2024. URL: https://www.misp-project.org/misp-training/0-intro-shorter_es.pdf (vid. pág. 77).

[69] *MISP Concepts Cheat sheet*. Computer Incident Response Center Luxembourg (CIRCL). 2024. URL: https://www.misp-project.org/misp-training/cheatsheet.pdf (vid. págs. 77, 78).

[70] *Implementación de una plataforma de inteligencia de amenazas*. Amazon Web

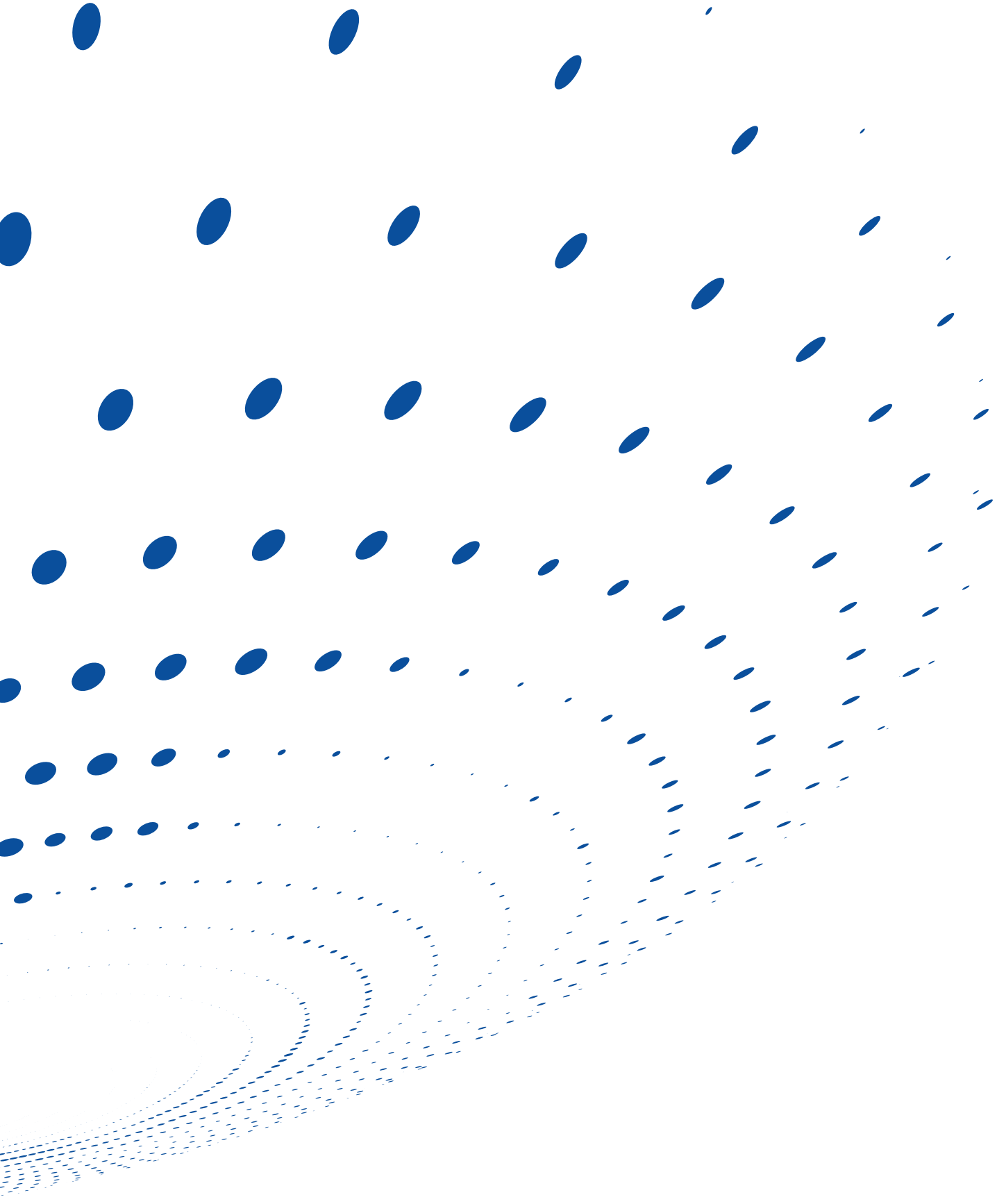
Services (AWS). n.d. URL: https://docs.aws.amazon.com/es_es/prescriptive-guidance/latest/cyber-threat-intelligence-sharing/architecture-threat-intelligence-platform.html (vid. pág. 77).

[71] *MISP - User Guide A Threat Sharing Platform*. Computer Incident Response Center Luxembourg (CIRCL), 2024. URL: https://www.circl.lu/doc/misp/book.pdf (vid. págs. 78, 80).

[72] *10 Mandamientos de MISP*. Computer Incident Response Center Luxembourg (CIRCL). 2024. URL: https://www.misp-project.org/misp-training/MISP%2010%20Mandamientos%20ES.pdf (vid. pág. 78).

[73] *VERIS: A Powerful Taxonomy for Cybersecurity*. CSFaaS. 2025. URL: https://medium.com/@csfaas/veris-a-powerful-taxonomy-for-cybersecurity-8e83db1bba10 (vid. pág. 80).

[74] *STIX Version 2.1 Errata 01*. OASIS. 2025. URL: https://docs.oasis-open.org/cti/stix/v2.1/stix-v2.1.html (vid. pág. 81).



FLAR
FONDO LATINOAMERICANO DE RESERVAS

Fondo Latinoamericano de Reservas | FLAR
Calle 84A No. 12-18 Piso 7 | Bogotá, Colombia
Correo electrónico: flar@flar.net
Tel: (571) 634 4360