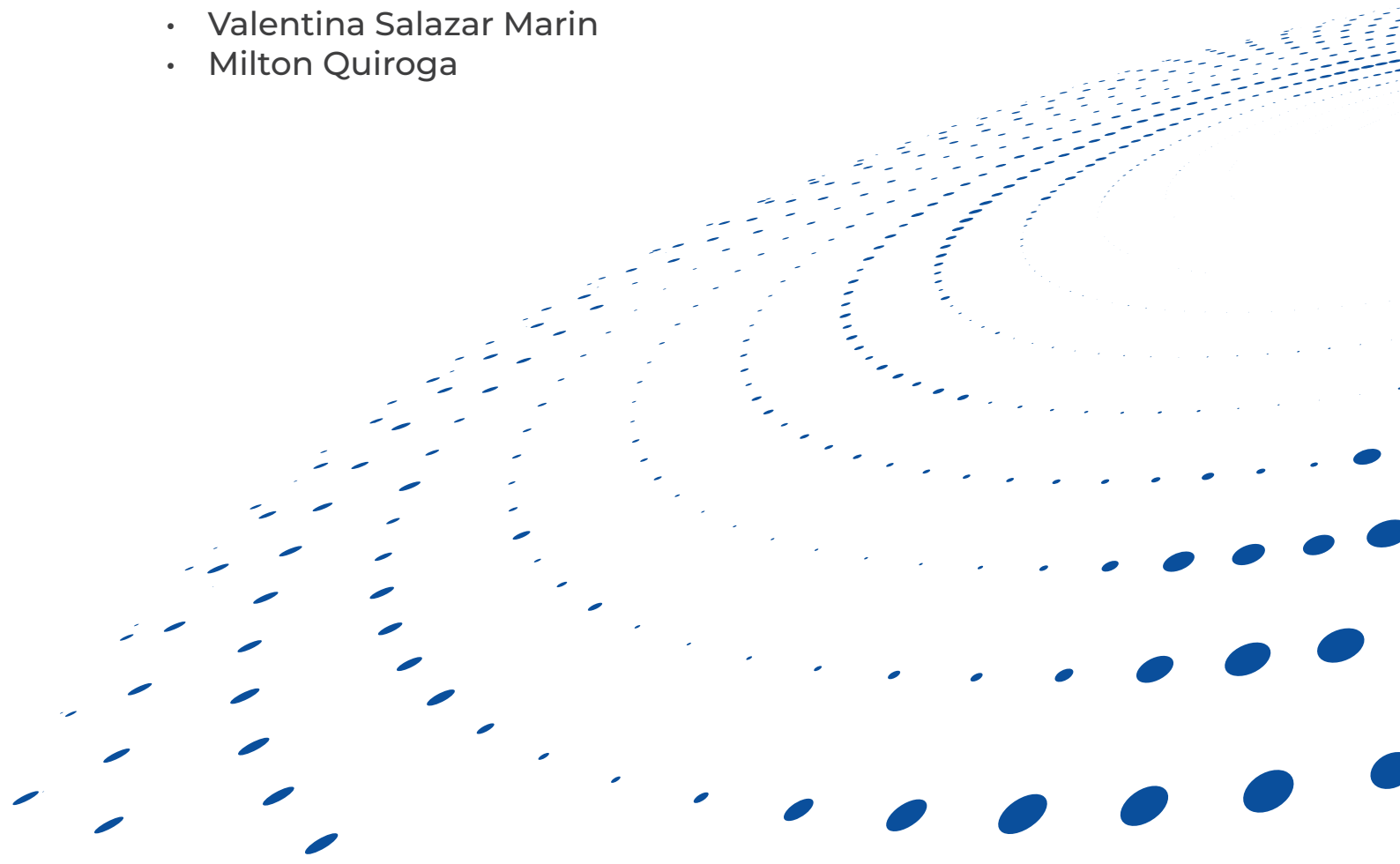
FLAR
FONDO LATINOAMERICANO DE RESERVAS

Automatización de la gestión de vulnerabilidades en bancos centrales

Del inventario inteligente a la remediación orquestada con métricas verificables

Autores:

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



Índice general

Índice de tablas

1 Introducción

La presente guía surge de un esfuerzo conjunto entre bancos centrales para ofrecer un marco integral de gestión de vulnerabilidades acorde con la interdependencia del sistema financiero y la sofisticación del panorama de amenazas. Su finalidad principal es proponer un referente común que posibilite diagnosticar la madurez institucional, identificar brechas de protección, inventariar activos esenciales, automatizar la detección de fallas, orquestar la remediación y fortalecer el aprendizaje organizacional. Con ello, se busca afianzar la resiliencia cibernética, proteger la confianza pública y resguardar la estabilidad macroeconómica en la región.

La obra se estructura en cinco dominios. El Dominio 1 compara marcos de madurez —con énfasis en CERT-RMM (*Resilience Management Model* del Software Engineering Institute)— y los contrasta con NIST CSF, ISO/IEC 27002 y OWASP SAMM, aportando una matriz que guía la autoevaluación institucional. El Dominio 2 aborda el inventario de activos críticos, su caracterización mediante RACI y una metodología de puntuación de riesgo que combina CVSS v4.0, EPSS y el catálogo CISA KEV (*Known Exploited Vulnerabilities*), culminando en una matriz de prioridad técnica; además, incorpora CAASM (Cyber Asset Attack Surface Management) como capa de visibilidad y correlación. El Dominio 3 reúne motores de descubrimiento y fuentes de inteligencia para detección automatizada, precisa lineamientos de integración y propone acciones para eliminar puntos ciegos. El Dominio 4 traslada la calificación técnica a ejecución mediante matrices operativas (vista por activo y por vulnerabilidad), SOAR, microsegmentación e integración continua con parcheo automatizado, alineando ventanas de servicio con RTO/RPO y la gobernanza del cambio. El Dominio 5 introduce análisis de causa raíz, fija indicadores para seguimiento longitudinal y plantea estrategias de mejora continua con apoyo en capacidades tecnológicas emergentes.

Cada dominio incorpora plantillas, listas de verificación y guías de buenas prácticas, de modo que las entidades puedan acoplar los lineamientos a su realidad operativa sin incurrir en desarrollos redundantes. El documento se concibe, por tanto, como un instrumento vivo: sus recomendaciones deberán revisarse periódicamente a la luz de nuevas vulnerabilidades, actualizaciones de estándares y lecciones derivadas de incidentes reales, consolidando así un ciclo de mejora y colaboración regional.

2 Marcos de madurez y prácticas líderes para gestión de vulnerabilidades

2.1 Comparativa de marcos de madurez

En el contexto actual, múltiples estándares y referentes ofrecen modelos específicos para fortalecer la gestión de vulnerabilidades y robustecer la postura de seguridad cibernética de las organizaciones. Uno de los esquemas más relevantes es el ***Resilience Management Model*** **(CERT-RMM)**, propuesto por el Software Engineering Institute (SEI) y dirigido principalmente a fortalecer la resiliencia institucional [1]. El CERT-RMM integra de manera sistemática las dimensiones de seguridad, continuidad del negocio y operaciones de tecnología informática (TI), sintetizando décadas de investigación sobre mejores prácticas relacionadas con la protección y la continuidad operativa de las personas, datos, tecnologías e infraestructuras [1]. Este modelo aplica un enfoque estructurado basado en niveles de madurez que permite a las organizaciones evitar acciones fragmentadas, favoreciendo una alineación efectiva con objetivos estratégicos relacionados con el manejo adaptable frente a crisis [1]. Además, constituye el fundamento de la *Cyber Resilience Review* (CRR), una metodología de autoevaluación para medir la eficacia de las prácticas adoptadas [2].

Por otro lado, el ***NIST Cybersecurity Framework*** **(CSF) 2.0** propone un abordaje integral para mejorar la postura global de seguridad de las organizaciones mediante seis funciones principales: gobernar, identificar, proteger, detectar, responder y recuperar [3]. Particularmente, la versión 2.0 destaca la primera de ellas, subrayando la importancia crítica de una gobernanza robusta que garantice la coherencia de la ciberseguridad con las metas comerciales y las exigencias regulatorias vigentes. En este sentido, el manejo de vulnerabilidades se encuentra inmerso transversalmente en todas sus fases, desde la identificación preliminar hasta la recuperación posterior a un incidente [3].

La norma **ISO/IEC 27002:2022** suministra un conjunto de controles de seguridad de la información, ciberseguridad y protección de la privacidad [4]. En su versión de 2022, agrupa 93 controles bajo cuatro temas principales, destacando el control 8.8, dedicado

puntualmente al abordaje técnico de vulnerabilidades, y el 8.16, orientado al monitoreo continuo de actividades críticas [4]. ISO/IEC 27002 complementa esquemas como CERT-RMM al apoyarse en modelos de referencia ampliamente difundidos en el ámbito internacional.

Asimismo, el ***Software Assurance Maturity Model* (OWASP SAMM 2.1)** representa una herramienta relevante en la revisión y ajuste evolutivo de la seguridad del software. Se organiza en cinco dimensiones de negocio (gobernanza, diseño, implementación, verificación y operaciones), cada una con lineamientos y niveles de madurez delimitados (fundacional, maduro, avanzado), simplificando la adopción sistemática de directrices reconocidas en seguridad durante todo el ciclo de vida del desarrollo de aplicaciones (SDLC) [5]. OWASP SAMM recalca la importancia de emprender acciones de acuerdo con su impacto real y concreto en las aplicaciones.

Adicionalmente, la **CISA Cyber Security Evaluation Tool (CSET)** es una plataforma de software de escritorio gratuita que orienta paso a paso a las organizaciones propietarias de infraestructuras críticas para evaluar sistemáticamente la postura de seguridad de sus sistemas industriales y redes TI [6]. La CSET posibilita aplicar metodologías reconocidas para efectuar diagnósticos y afianzar continuamente la seguridad [6].

Finalmente, los **Cybersecurity Performance Goals (CPG)** formulados por la Agencia de Ciberseguridad y Seguridad de Infraestructuras (CISA) de Estados Unidos abarcan prácticas voluntarias que buscan reducir significativamente la probabilidad de explotación de vulnerabilidades conocidas. Dichos objetivos se alinean directamente con las funciones del NIST CSF, determinando una jerarquía de atención centrada en los activos más críticos y proporcionando un enfoque pragmático y accionable para la mitigación de riesgos cibernéticos [7].

La coexistencia y la interrelación entre estos marcos —como los mapeos cruzados entre la CRR y el NIST CSF v1.1, la complementariedad entre ISO/IEC 27002 y CERT-RMM, o la sinergia entre NIST CSF y OWASP SAMM para potenciar su repercusión [8]— evidencian que los bancos centrales no deben restringirse a la instauración de un único modelo. Por el contrario, se recomienda un planteamiento híbrido y sinérgico. Cada uno de los estándares aporta una perspectiva única —ya sea en resiliencia operativa, administración general de riesgos cibernéticos, controles de seguridad de la información, seguridad de aplicaciones, evaluación de postura o establecimiento de objetivos de rendimiento— que, al combinarse, ofrece una visión más completa y una estrategia más robusta para la gestión de vulnerabilidades. Lo anterior resulta indispensable para abordar de manera integral la complejidad inherente a la ciberseguridad en el sector financiero.

La Tabla 2.1 sintetiza las características y la relevancia de las guías descritas.

Tabla 2.1: Comparativa de marcos de gestión de vulnerabilidades y medición de madurez organizacional.

Aspecto	CERT-RMM	NIST CSF 2.0	ISO/IEC 27002:2022	OWASP SAMM 2.1
Enfoque general	Modelo de madurez de resiliencia operacional (convergencia de seguridad, TI y continuidad). Incluye un proceso específico de análisis y resolución de vulnerabilidades *(VAR)*.	Marco de gestión de riesgos cibernéticos amplio y flexible que describe resultados de seguridad deseados.	Norma de controles de seguridad de la información. Es prescriptiva en *qué* hacer (por ejemplo, parches y configuraciones), no en *cómo*.	Modelo de madurez para aseguramiento de software, centrado en ciclo de vida y endurecimiento de aplicaciones. Complementa *frameworks* generales.
Cobertura de vulnerabilidades	El proceso VAR define pasos para identificar, analizar, jerarquizar y resolver vulnerabilidades en activos y servicios críticos como parte de la resiliencia.	Incluye subcategorías relevantes: ID.RA-2 (recibir información de vulnerabilidades de fuentes externas); PR.IP-12 (gestión de vulnerabilidades); DE.CM (monitoreo continuo de activos). No elabora un proceso detallado, pero mapea las prácticas CERT-RMM VAR.	Contempla explícitamente la gestión técnica de vulnerabilidades (control 8.8), integrándola en la seguridad operativa. Recomienda obtener inteligencia acerca de vulnerabilidades para luego evaluarlas y remediarlas.	Define prácticas de *testing* y *defect management* para asegurar que las vulnerabilidades de aplicaciones sean detectadas (p.ej. mediante análisis estático o dinámico) y organizadas en el *backlog* de desarrollo.

Medición de madurez	Cinco niveles de capacidad (0-Incompleto a 5-Optimizado). Define un escala de niveles de madurez y permite autoevaluación de prácticas. La madurez se mide por grado de implementación en áreas como VAR.	Cuatro *Implementation Tiers* (parcial, informado por riesgo, repetible y adaptativo) que indican integración del riesgo cibernético en funciones organizacionales. No son estrictamente niveles de madurez, pero se usan como tal para trazar el progreso.	No cuenta con niveles de madurez por diseño. La certificación ISO 27001 implica implementar controles 27002 apropiados al contexto. La mejora en la gestión se mide vía escrutinios periódicos y ciclo PHVA (planear, hacer, verificar y actuar) de ISO.	Tres niveles de madurez por cada práctica de seguridad. Cada nivel define actividades más avanzadas (el 0 para un proceso *ad hoc* o no existente hasta el 3 para medidas de seguridad totalmente optimizadas y en permanente evolución). Permite calificar la madurez actual de las aplicaciones e instaurar ciclos de mejora sostenida.
Fortalezas	Visión holística de resiliencia; enfocado en procesos y gobernanza, no solo en tecnologías; y útil para autoevaluación (ej. método CRR que deriva de CERT-RMM).	Amplio reconocimiento global, lenguaje sencillo para comunicarse con alta dirección o terceros, centrado en los riesgos, adaptable a cualquier sector, facilita el reconocimiento de brechas y la priorización de mejoras.	Concreto y accionable en controles; alineado a certificación ISO 27001 (marco regulatorio común); actualizado a 2022 con controles modernos (vulnerabilidades y amenazas emergentes); y entrega una guía para diseñar un programa de parches y monitoreo.	Profundiza en seguridad de software, un área crítica que frecuentemente se encuentra fuera del alcance de directrices generales; proporciona una ruta clara a favor de un SDLC seguro; se integra con *OWASP resources* (Top 10, MASVS, etc.); y permite comparar el estado de una aplicación con los referentes de la industria.

Limitaciones	Es extenso y complejo de implementar en su totalidad; exige acoplar el modelo a la realidad de cada organización; y es menos conocido fuera de comunidades especializadas.	No prescribe controles ni métodos puntuales, por lo que su eficacia se halla supeditada a cómo se implementa; puede requerir mapear a estándares concretos (ISO o COBIT) para trazar acciones; y cobertura limitada en aplicaciones (depende de usar NIST SSDF aparte).	Enfocado en cumplimiento; no indica *cómo* determinar relevancia; puede convertirse en una lista de comprobación sin asegurar efectividad; y la implementación homogénea en países latinoamericanos requiere considerar el contexto socioeconómico de cada organización.	Alcance limitado a desarrollo/ aplicaciones, por lo que otras áreas (infraestructura, redes, etc.) no son contempladas; y no es un estándar de cumplimiento regulatorio, sino voluntario, por lo que su instauración en instituciones financieras tradicionales puede demandar esfuerzos de sensibilización interna.

2.2 Diagnóstico de madurez institucional

Para que un banco central pueda ubicarse en las categorías de madurez propuestas por el CERT-RMM, resulta esencial contar con un cuestionario de autodiagnóstico que oriente el análisis interno de sus capacidades de resiliencia cibernética. El CERT-RMM emplea indicadores de madurez (MIL) que describen el grado de consolidación obtenido, desde MIL0 (incompleto) hasta MIL5 (definido), tal que una organización debe alcanzar de forma progresiva cada etapa antes de aspirar a una superior [2].

La CRR, derivada del CERT-RMM, constituye una herramienta ligera compuesta por 299 ítems organizados en diez dominios clave —entre ellos, vulnerabilidades (VM), activos (AM), controles (CM), incidentes (IM) y riesgos (RM)— [2], los cuales pueden ser utilizados como base para un ejercicio introspectivo. Lo anterior dado que un instrumento correctamente diseñado debe contener preguntas que examinen el grado de formalización, consistencia y trazabilidad en cada una de las áreas consideradas.

De acuerdo con los criterios para valorar cada objetivo y práctica del CRR [2] [9], los niveles se examinan mediante interrogantes como:

Nivel inicial (MIL0 - Incompleto / MIL1 - Realizado)

- ¿Se han identificado y priorizado formalmente los servicios críticos que el banco central presta a la economía y al sistema financiero?
- ¿Se mantiene un inventario básico de los activos (tecnología, información, personas e instalaciones) que soportan directamente estos servicios críticos?
- ¿Se llevan a cabo acciones básicas y *ad hoc* para gestionar la exposición a vulnerabilidades técnicas identificadas, aunque no de manera sistemática?

Nivel gestionado (MIL2 - Planificado / MIL3 - Gestionado)

- ¿Existe una estrategia documentada y aprobada para el análisis y la resolución de vulnerabilidades, aclarando roles y responsabilidades?
- ¿Se han establecido y se mantienen procesos formales para identificar y analizar vulnerabilidades, incluyendo el uso de fuentes de información de vulnerabilidades, descubrimiento activo y categorización/jerarquización?
- ¿Se asignan los recursos humanos y financieros adecuados para la gestión de las vulnerabilidades, reconociendo y moderando los riesgos relacionados con estas actividades?

Nivel medido (MIL4 - Medido)

- ¿Se evalúa periódicamente la efectividad de las prácticas de gestión de vulnerabilidades (por ejemplo, a través de métricas o auditorías internas)?

- ¿Se revisan los resultados de tales evaluaciones con la alta dirección para informar la toma de decisiones y la mejora continua?
- ¿Se aprovechan datos cuantitativos para comprender y controlar el rendimiento de los procesos de gestión de vulnerabilidades?

Nivel optimizado (MIL5 - Definido)

- ¿Se han estandarizado y optimizado las tareas de gestión de vulnerabilidades, con un enfoque en la mejora continua y la adaptación proactiva a la evolución del panorama de amenazas?
- ¿Se recopila y comparte información sobre las lecciones aprendidas y las oportunidades de mejora de manera consistente en toda la organización para impulsar la innovación en personas, procesos y tecnología?

Este tipo de autodiagnóstico trasciende la simple recolección de datos técnicos: se convierte en un catalizador para reconfigurar la cultura organizacional y los patrones de coordinación existentes. Al apoyarse en un modelo que entrelaza personas, procesos y tecnología, su puesta en práctica exige una revisión profunda de los procesos institucionales desde una óptica global. Tal ejercicio revela posibles disonancias entre unidades funcionales —como seguridad, operaciones de TI y continuidad del negocio—, inaugurando oportunidades para lograr una articulación más armónica y transversal. Así, al evidenciar los puntos débiles en la concertación de los flujos operativos y en la cooperación interdepartamental, la autoevaluación se transforma en un recurso valioso para entender y abordar la fragmentación interna, solventando la existencia de esquemas de trabajo desconectados o «silos» organizacionales que obstaculizan una respuesta coordinada y resiliente. Por consiguiente, su mayor virtud no radica en los puntajes obtenidos, sino en el diálogo que suscita y en su capacidad para propiciar el discernimiento compartido del estado actual, junto con la construcción coherente de una trayectoria de consolidación futura.

3 Inventario y priorización de activos

3.1 Caracterización de activos críticos

3.1.1 Construcción del inventario

Un inventario exhaustivo y actualizado de activos es un componente indispensable para sostener cualquier programa de ciberseguridad en un banco central. Constituye un elemento esencial no solo para mantener una adecuada postura defensiva frente a las ciberamenazas, sino también para cumplir eficientemente con regulaciones financieras y mitigar riesgos operacionales inherentes [10]. Por tanto, el registro debe cubrir a cabalidad todos los activos que sustentan las funciones críticas de la institución, tales como equipos físicos (servidores, estaciones de trabajo e infraestructura de red), infraestructura de seguridad informática, sistemas operativos y aplicaciones de software, recursos virtualizados, plataformas desplegadas en la nube, bases de datos sensibles, flujos de información estratégica y procesos de negocio subyacentes [10].

En un entorno caracterizado por una transformación tecnológica constante, la precisión y dinamismo en la enumeración de activos son fundamentales para anticipar y neutralizar posibles vulnerabilidades emergentes. Las innovaciones recientes en el sector financiero, como la incorporación de monedas digitales emitidas por bancos centrales y la consolidación de mecanismos de pagos inmediatos, ejemplifican claramente este reto, a razón de que extienden considerablemente la superficie susceptible a ataques informáticos a través de nuevas arquitecturas de red y aplicaciones expuestas a diversos vectores de amenaza [11] [12]. Frente a tal escenario, mantener un inventario estático se convierte en una vulnerabilidad latente, dado que fomenta la proliferación inadvertida de activos tecnológicos no autorizados o no identificados, fenómeno conocido como *shadow IT*, los cuales se convierten en puntos ciegos explotables por los adversarios [10]. En consecuencia, la capacidad de llevar a cabo un descubrimiento continuo y automatizado en tiempo real es una necesidad para conservar una postura de seguridad relevante y vigente.

Como se expone en la Tabla 3.1, los grandes proveedores de nube y los principales

fabricantes de soluciones de seguridad ofrecen mecanismos de detección que abarcan centros de datos, servicios SaaS, contenedores, terminales móviles y entornos híbridos, aplicando distintos métodos de descubrimiento [13].

Tabla 3.1. Herramientas automatizadas para descubrimiento de activos: panorama de mercado.

Ámbito	Capacidades distintivas	Ejemplos de soluciones
On-premises / redes corporativas	Buscan exponer cada nodo visible (servidores, estaciones de trabajo, sensores IoT o hipervisores) y enriquecerlos con atributos como sistema operativo, puertos expuestos, software instalado y controles de seguridad vigentes [14] [15].	Qualys CyberSecurity Asset Management, Rapid7 InsightVM y Tenable Nessus
Nube pública	Interrogan directamente a las API administrativas del servicio de nube, suscriben flujos de eventos (como CloudTrail o Cloud Logging) y consumen metadatos de configuración para detectar deriva, revisar políticas y calcular métricas de postura de seguridad [16] [17].	AWS Config, Azure Resource Graph con Defender for Cloud y Google Cloud Asset Inventory
Entornos híbridos y contenedores	Se instalan directamente en sistemas físicos, máquinas virtuales y contenedores, donde recogen de forma continua huellas hardware, listas de software, configuración del kernel y metadatos de la capa orquestadora (Docker Engine o Kubernetes) [18].	Qualys Cloud Agent y Rapid7 Agents
Dispositivos móviles y teletrabajo	Obtienen identificadores de hardware, versión de sistema operativo, aplicaciones instaladas, estado de cifrado, IMEI/UDID y otros metadatos que se envían hacia un servicio en la nube que consolida la información en una base de activos unificada, aplica etiquetas de riesgo y compara la configuración con políticas corporativas [19] [20].	Microsoft Intune y VMware Workspace ONE Unified Endpoint Management

Complementariamente, la realización de auditorías frecuentes contribuye a garantizar la exactitud y actualidad del inventario, permitiendo detectar proactivamente inconsistencias o discrepancias. En adición a ello, la integración fluida del sistema con plataformas auxiliares, como aquellas destinadas a supervisar vulnerabilidades o proteger los *endpoints*, es indispensable para agilizar la respuesta ante incidentes [10]. El va-

lor del inventario reside también en la posibilidad de asignar perfiles de riesgo a cada activo, atendiendo tanto a su relevancia operacional como a las amenazas potenciales vinculadas. Tal segmentación informada favorece el diseño de medidas defensivas adecuadas y focaliza los esfuerzos de seguridad en aquellas áreas donde la exposición al riesgo es más significativa, optimizando recursos y reforzando la resiliencia global de la institución [10].

3.1.2 Plantilla RACI para el inventario de activos

Con el propósito de garantizar claridad organizacional y responsabilidad efectiva en la administración de activos críticos, se recomienda la creación de una matriz RACI («Responsable», «Aprobador», «Consultado» e «Informado»). Este recurso es imprescindible para delimitar con precisión las funciones, fortalecer la comunicación interna y acelerar la toma de decisiones a través del ciclo completo de vida de los activos tecnológicos [13]. Tal instrumento define los siguientes roles para cada entregable:

- **Responsable (*reponsible*)**: Es el individuo o grupo que ejecuta directamente la tarea asignada. Puede haber múltiples responsables simultáneamente en función de las necesidades de la actividad.
- **Aprobador (*accountable*)**: Persona que asume la responsabilidad última sobre el resultado y aprueba formalmente la culminación de la tarea. Idealmente, solo una figura ocupa dicha posición para evitar ambigüedades.
- **Consultado (*consulted*)**: Son aquellas personas o equipos cuyo conocimiento especializado o perspectiva debe constatarse antes de concretar la tarea. Su participación es clave para validar propuestas técnicas o estratégicas.
- **Informado (*informed*)**: Quienes deben mantenerse al tanto sobre los avances significativos y los resultados finales, procurando transparencia y alineación.

Las recomendaciones más contundentes al emplear esta herramienta incluyen mantener la matriz sencilla y accesible, promover la participación activa del personal en su elaboración para aumentar el sentido de compromiso, así como revisar y actualizar periódicamente su contenido a fin de reflejar modificaciones en roles, responsabilidades o incorporación de nuevos activos [13]. Asimismo, la documentación detallada de cada cambio promueve la trazabilidad y rendición de cuentas.

En el ámbito de los bancos centrales, quienes ostentan exigentes lineamientos de gobernanza y altos criterios de responsabilidad [11], el uso riguroso de una matriz RACI conlleva la adjudicación clara de responsables para cada activo primordial. Tal concepción busca evitar la proliferación de recursos no mapeados, fomentando una administración coherente. Procediendo así, al asignar deberes y distribuir tareas, se promueve

una interacción más fluida entre las distintas unidades implicadas, lo que se traduce en una articulación más cohesionada y consistente de los procesos vinculados con la seguridad digital y los componentes tecnológicos que la sustentan. La Tabla 3.2 presenta una plantilla que puede ser ajustada por los bancos centrales de acuerdo con su organigrama.

Tabla 3.2. Plantilla RACI para inventario de activos.

Actividad	Propietario del activo	Equipo de TI o de infraestructura	Equipo de seguridad	Equipo de riesgos	Cumplimiento	Auditoría interna	Alta dirección
Descubrimiento de activos	I	C	R	I	I	I	I
Clasificación de activos	A	R	C	C	C	I	I
Asignación de propietarios	A	R	I	I	I	I	I
Mantenimiento del inventario	C	R	A	I	I	I	I
Revisión de criticidad	A	C	R	C	C	I	I
Gestión de cambios en activos	C	R	A	C	I	I	I
Retiro de activos	A	R	C	I	I	I	I

3.2 Metodología de puntuación de riesgo

La clasificación de riesgo para los bancos centrales debe ir más allá de las consideraciones tradicionales de confidencialidad, integridad y disponibilidad (CIA), incorporan-

do explícitamente el impacto macroeconómico y reputacional. En virtud de ello, esta metodología de puntuación de riesgo busca plasmar la criticidad única de las operaciones en la industria financiera [12].

Respecto a la tríada para calificar la criticidad de un recurso, se toma en cuenta:

- **Confidencialidad**: ¿El activo maneja información sensible cuyo acceso no autorizado acarrea graves consecuencias (como filtración de datos de mercado o información de política monetaria confidencial)?
- **Integridad**: ¿Una alteración no detectada de este activo podría provocar decisiones o transacciones erróneas (por ejemplo, manipulación de tasas, de registros contables o de reservas internacionales)?
- **Disponibilidad**: ¿La indisponibilidad del activo impacta significativamente operaciones críticas o servicios al sistema financiero (como caída del sistema de pagos o imposibilidad de iniciar transferencias interbancarias)?

Según lo anterior, son pertinentes las escalas introducidas en la publicación FIPS 199 del NIST, donde se categorizan los impactos potenciales en tres magnitudes [21]:

- **Bajo**: Se refiere a situaciones donde la alteración prevista es limitada y se deriva de una degradación mínima que repercute sobre la capacidad del banco para cumplir funciones esenciales, con un desempeño notablemente disminuido. Lo anterior podría implicar daños menores sobre activos físicos o virtuales, pérdidas financieras leves o inconvenientes mínimos para los individuos.
- **Moderado**: Alude a consecuencias de intensidad significativa que afectan de forma apreciable la aptitud técnica de una entidad para llevar a cabo tareas clave. Aunque dichas funciones aún pueden cumplirse, su ejecución se ve notablemente obstaculizada, con una marcada disminución en la eficiencia y en la calidad de los resultados. En este umbral, los perjuicios sobre los activos pueden alcanzar una escala elevada, traducida en afectaciones materiales o económicas de peso. Asimismo, pueden materializarse impactos nocivos sobre las personas, sin que estos lleguen a implicar lesiones severas o la pérdida de vidas.
- **Alto**: Denota efectos adversos extremos, que pueden producir una degradación severa o pérdida completa de la competencia para desempeñar funciones esenciales, impidiendo al banco llevar a cabo una o varias de sus responsabilidades primarias. Tal escenario podría conllevar daños extensos o irreparables a activos físicos o digitales, pérdidas económicas de gran magnitud o catastróficas, así como repercusiones devastadoras sobre las personas implicadas, inclusive con lesiones graves o pérdida de vidas humanas.

En el caso de un banco central, se añade una dimensión adicional conocida como **efec-**

to macroeconómico. En virtud del papel que desempeñan estas entidades en la arquitectura financiera de un país, un incidente cibernético que impacte procesos esenciales —como la operatividad de los sistemas de pago mayoristas— podría provocar alteraciones de carácter sistémico, con el potencial de interrumpir gravemente la dinámica de los mercados y erosionar la estabilidad económica en su conjunto [12]. Particularmente alarmante es la posibilidad de que se vea comprometida la integridad de datos sensibles, como libros contables, algoritmos utilizados en operaciones monetarias o registros de transacciones clave. Este tipo de afectaciones no solo presenta una alta complejidad técnica para su contención y recuperación, sino que, además, puede minar de manera profunda y prolongada la credibilidad tanto de la red financiera como de la institución emisora ante los actores del mercado y la ciudadanía [22]. De hecho, casos reales ilustran tal situación: un ciberataque al Banco Central de Lesoto en 2023 detuvo el sistema nacional de pagos, bloqueando las transacciones bancarias y demostrando cómo un evento cibernético puede incidir sobre el equilibrio económico de un país [22]. Además, el FMI advierte que la creciente dependencia de proveedores externos de tecnología incrementa la posibilidad de disrupciones simultáneas [22].

La **reputación y confianza pública** actúan como pilares intangibles de valor incalculable para un banco central, cuya legitimidad se sustenta no solo en su aptitud técnica, sino en la percepción sostenida de su autoridad, integridad y competencia. Cualquier evento de naturaleza cibernética que comprometa el funcionamiento de mecanismos clave —como las plataformas de pago o las monedas digitales emitidas—, o que resulte en actividades fraudulentas, puede desencadenar consecuencias duraderas sobre la credibilidad institucional. Esta clase de afectaciones no solo pone en entredicho la imagen de la entidad emisora, sino que también proyecta dudas sobre la fiabilidad de la moneda y del entramado normativo que la respalda [11].

Para un banco central, el efecto macroeconómico y la reputación no son simplemente factores adicionales, sino que actúan como multiplicadores decisivos del riesgo. Situaciones que, desde un punto de vista puramente técnico, podrían considerarse moderadas, adquieren automáticamente una clasificación de alto impacto debido a la naturaleza intrínseca de las tareas del banco, como la emisión de moneda, la salvaguarda de la estabilidad financiera o la gestión de reservas.

La denominada «densidad de valor» (*value density*) de los activos, una métrica suplementaria introducida en CVSS v4.0 y que calibra cuánta «riqueza digital» obtiene un adversario con una sola explotación [23], alcanza una concentración excepcionalmente elevada en este tipo de entidades, como consecuencia directa de su rol estratégico en la infraestructura económica del país. No obstante, múltiples debilidades aún no se encuentran valoradas con dicha versión, por lo que este atributo puede no estar disponible; en tales casos conviene inferirlo a través de indicadores sustitutos (criticidad del proceso, concentración de datos sensibles, interdependencias tecnológicas y alcance

transaccional). Cuando se aplica, las secuelas de una brecha de seguridad pueden adquirir una magnitud drásticamente mayor en contraste con aquellas que competerían a una empresa comercial convencional. La ausencia de métodos estandarizados para cuantificar los costos económicos de los ciberincidentes subraya el requerimiento de involucrar criterios especializados y un proceso de revisión robusto para ponderar adecuadamente estos factores técnicos y no técnicos [12].

La metodología general para la valoración de riesgo debe seguir guías como NIST SP 800-30 Rev. 1. Este proceso inicia al definir el alcance y los activos, tipificar amenazas y vulnerabilidades, inspeccionar los controles existentes, determinar la probabilidad de ocurrencia y estimar el impacto potencial para así precisar los niveles de riesgo globales. En este proceso, la integración de las escalas del FIPS 199 con una evaluación cualitativa/cuantitativa de las repercusiones macroeconómicas y reputacionales otorgará una puntuación de riesgo más exacta y relevante para el ecosistema de un banco central.

3.3 Matriz de prioridad técnica

La matriz traduce el diagnóstico de riesgos en un plan de acción escalonado. La estructura empleada en este caso (Tabla **??**) sitúa en el eje horizontal la explotabilidad informada por EPSS (*Exploit Prediction Scoring System*) y listados como el CISA *Known Exploited Vulnerabilities* (KEV) [24], mientras que el eje vertical refleja la severidad. Esta último se valora mediante un indicador agregado que pondera superficie de ataque, deficiencias sin parchear y tendencia histórica a incidentes, o bien recurriendo a las categorías de crítica, alta, media y baja derivadas de la versión más reciente del CVSS. La intersección de ambos ejes sitúa cada componente en un cuadrante de atención inmediata, diferida o simplemente monitorizada.

Tabla 3.3. Matriz de prioridad técnica por severidad (CVSS) y explotabilidad (EPSS/-KEV)

Prioridad		Explotabilidad (EPSS/KEV)			
		Baja	**Media**	**Alta**	**Muy alta**
Severidad (CVSS)	**Crítica**	Alta	Máxima	Máxima	Máxima
	Alta	Alta	Alta	Máxima	Máxima
	Media	Baja	Media	Media	Media
	Baja	Baja	Baja	Baja	Media

En prioridad máxima se ubican componentes esenciales o expuestos al exterior con fallas críticas y alta explotabilidad —por ejemplo, *core* bancario, pasarelas SWIFT, API públicas, módulos de autenticación o servidores con CVE listadas en CISA KEV y probabilidad elevada según EPSS— cuyo compromiso adquiriría un efecto sistémico. La prioridad alta agrupa recursos relevantes con brechas severas, pero de menor probabilidad, o bien con debilidades altas en entornos particularmente sensibles: bases de datos que sostienen liquidaciones, portales internos de alto tráfico o *middleware* que integra cámaras de compensación. Para tales recursos, el tratamiento se programa a corto plazo y con controles de cambio estrictos. La prioridad media corresponde a plataformas de apoyo sin exposición directa, donde existen barreras efectivas y la indisponibilidad no interrumpe procesos esenciales, por lo que los parches siguen el ciclo habitual. Finalmente, el nivel bajo abarca elementos periféricos o aislados con baja probabilidad de explotación y mitigaciones suficientes; en estos casos, se opta por vigilancia continua y ventanas de mantenimiento amplias. Tal lógica encarna el principio de manejo basado en riesgo, puesto que la puntuación CVSS cuantifica la gravedad técnica, pero el riesgo surge del contexto: ubicación del activo, criticidad de la función y probabilidad real de explotación [25].

Al final del proceso, el banco central dispone de un instrumento transparente con el que fundamentar ante la alta dirección y los supervisores la razón por la que un parche se aplica de inmediato en ciertos sistemas y se difiere en otros. De tal forma, los recursos se orientan primero hacia los componentes que concentran una mayor densidad de valor, minimizando la posibilidad de disrupciones con efectos sistémicos o daños reputacionales irreversibles.

3.4 Plataformas CAASM para potenciar la visibilidad y el manejo de activos

En ecosistemas complejos, una plataforma CAASM (*Cyber Asset Attack Surface Management*) emerge como una capa de integración y correlación que consolida inventarios heterogéneos, depura duplicidades y vincula cada elemento tecnológico con su contexto de negocio. Su objetivo radica en elevar la fidelidad del inventario y exponer la verdadera huella del riesgo mediante un modelo consolidado que combina fuentes internas, telemetrías de seguridad y metadatos nativos de nube, aportando una vista transversal de dispositivos, software, identidades y servicios críticos [26] [27].

La ingesta se apoya en conectores hacia CMDB (base de datos de la gestión de configuración), EDR/XDR (detección y respuesta en *endpoints*/extendida), MDM (gestión de dispositivos móviles)/UEM (gestión unificada de terminales), CSPM (gestión de la postura de seguridad en la nube), hipervisores, controladores de dominio, SaaS, soluciones de protección de puntos finales, registros de configuración y catálogos de identidades (IAM). Con fundamento en ello, la herramienta normaliza esquemas, reconcilia identificadores (hostname, número de serie, etiquetas, huellas de red, ID de instancia, entre otros) y aplica resolución de entidades para agrupar evidencias que describen el mismo activo. A la par, aplica controles de calidad de datos (completitud, unicidad y latencia) con alertas de deriva cuando surgen inconsistencias entre fuentes [28] [29].

Tras la consolidación, la plataforma enriquece cada registro con la criticidad del servicio, la propiedad funcional (acorde al responsable que consigne la matriz RACI), los controles (agentes activos, parches pendientes o *hardening*), la exposición externa y las relaciones con aplicaciones, bases de datos y flujos de información. De forma complementaria, descubre activos huérfanos, tecnología no sancionada por el área de TI, fallos en agentes, sistemas fuera de soporte y parametrizaciones que amplifican el radio de explosión de un incidente. La representación como grafo de dependencias habilita una visión de 360° que organiza no solo en función de la severidad técnica, sino también del impacto operativo sobre funciones misionales y procesos de pago [30].

En la práctica diaria, la capa CAASM concentra consultas y tableros de control que nutren la metodología de puntuación de riesgo y la matriz de prioridad (Tabla 3.3). Al unir inventario, contramedidas e interacciones entre entidades, ascienden en la cola de remediación aquellos elementos con mayor exposición en el ámbito operativo.

Las herramientas CAASM contemporáneas incorporan automatizaciones basadas en eventos —como *webhooks*— que activan flujos y acciones de remediación en plataformas colindantes; por ejemplo, Axonius Action Center admite políticas y secuencias que aíslan equipos en la red, despliegan software o ejecutan comandos remotos, conser-

vando el historial de ejecuciones para brindar una trazabilidad integral. Estas señales pueden encadenarse con SOAR y con NAC/*firewalls* encargados de segmentación o cuarentena [28].

El gobierno de la información se robustece mediante métricas longitudinales y estadísticas acerca de la cobertura de las defensas: porcentaje de activos sin agente de seguridad, MTTR por dominio tecnológico, proporción de sistemas con parches críticos aplicados, reducción de la exposición perimetral y el perfilamiento del catálogo vigente. Tales indicadores sostienen OKR/KPI de mejora continua (Capítulo 6), respaldan auditorías y contribuyen a programas de CTEM (*Continuous Threat Exposure Management*), que protegen la superficie de ataque con base en el impacto y el entorno de actuación [26]. Así, una solución de CAASM transforma el listado de recursos en conocimiento accionable al señalar con precisión quién se encuentra a cargo de cada activo, qué salvaguardas lo cubren, dónde se concentra la exposición y cómo evolucionan las dependencias que soportan los procesos críticos del banco central [30].

En el mercado destacan Axonius, con conectividad extensa y deduplicación rigurosa; JupiterOne, que modela un grafo relacional para estimar el impacto de un incidente de seguridad; Rapid7/Noetic, orientado a la visibilidad contextual y al cierre de brechas de cobertura; Armis Centrix, fuerte en entornos TI/TO/*Internet of Things*/5G mediante un enfoque sin agentes; runZero, experto en descubrimiento sin credenciales y *fingerprinting* preciso; y Panaseer, centrado en el monitoreo continuo de controles (*Continuous Controls Monitoring*, CCM) y en la construcción de tableros ejecutivos [31].

4 Motores de descubrimiento e inteligencia para detección automatizada

4.1 Catálogo de fuentes automatizadas

En la detección contemporánea de vulnerabilidades, convergen diversos motores automatizados cuya finalidad consiste en descubrir, clasificar y situar debilidades técnicas con la celeridad que exige el entorno digital. Particularmente,

- **Escáneres de red/host (VM)**. Recorren sistemas operativos, dispositivos y servicios expuestos para descubrir configuraciones débiles, binarios sin parche y protocolos inseguros mediante sondeo autenticado/no autenticado y fingerprinting. Ejemplos prominentes son Tenable Nessus, OpenVAS y Qualys VMDR [32].
- **Seguridad de aplicaciones — DAST/SAST/IAST/SCA**. Los analizadores dinámicos (DAST) —Invicti y Burp Scanner [32]— reproducen vectores ofensivos como inyección SQL o XSS en aplicaciones en ejecución, mientras que los revisores estáticos (SAST) exploran código fuente, bytes o binarios en repositorios o *pipelines* con miras a detectar patrones inseguros antes de la compilación. Por su lado, IAST (*Interactive Application Security Testing*) observa flujos internos durante pruebas funcionales/automatizadas y SCA (*Software Composition Analysis*) lleva a cabo un inventario de dependencias para examinar los riesgos en la cadena de suministro [33].
- **CSPM/CNAPP para nube**: CSPM (*Cloud Security Posture Management*) supervisa las configuraciones en IaaS/PaaS/SaaS. CNAPP (*Cloud-Native Application Protection Platform*) integra CSPM, CWPP, CIEM, escaneo de infraestructura como código (IaC) y protección *runtime* en arquitecturas nativas de nube [34].
- **Contenedores, Kubernetes e IaC**. Escaneo de imágenes (Docker), revisión de manifiestos YAML y políticas de Kubernetes [32], en conjunto con la inspección de IaC en el pipeline para frenar desviaciones antes de producción [35]. Esto se alinea con NIST SP 800-190 y CIS Kubernetes Benchmark.

- **Motores de base de datos**. Revisión de parámetros críticos, cifrado en reposo/-tránsito, privilegios, contraseñas y parches; validación contra guías de endurecimiento por familia de motor [32].
- **Seguridad de API**. Descubrimiento e inspección de interfaces, pruebas de autorización a nivel de objeto/función y fuzzing dirigido; ejemplos incluyen plataformas como Pynt orientadas a pruebas dinámicas en CI/CD [36].
- **EASM (*External Attack Surface Management*)**. Observación de afuera hacia adentro para inventariar dominios, IP públicas, certificados, recursos expuestos y *shadow IT*. Algunos referentes son Microsoft Defender EASM [37].

Lo anterior se nutre de plataformas de inteligencia de amenazas, las cuales son cruciales para contextualizar y ponderar las vulnerabilidades [38]. En concreto, se encargan de ingerir, agregar y organizar datos de múltiples fuentes como *feeds* de amenazas comerciales, foros en la internet oscura, OSINT y catálogos como CISA KEV, etiquetando cada CVE según prevalencia, nivel de explotación y severidad potencial [39]. Soluciones tales como Recorded Future, Cyble Vision, CloudSEK XVigil, SOCRadar o Google Threat Intelligence ofrecen esta curaduría en tiempo casi real [40].

4.2 Integración y aprovechamiento de fuentes

La detección automatizada alcanza su máximo potencial cuando los hallazgos de las distintas sondas técnicas se incorporan a una arquitectura de orquestación que unifique la captura, normalización, correlación y reacción. En tal entramado, toda pieza de información debe fluir sin fricciones hacia los dominios de desarrollo, operaciones y respuesta, evitando silos de datos y duplicación de esfuerzos.

En primera instancia, los artefactos producidos a través de la inteligencia de amenazas (por ejemplo, CISA KEV y *feeds comerciales*) no deben quedar en informes aislados. Es crucial que se aprovechen como insumo directo para otros procesos clave, como la priorización de vulnerabilidades [39], la gestión de incidentes y las iniciativas de mejora continua.

Dentro del ciclo de vida del software,la filosofía DevSecOps exige que los motores de SAST/DAST, de inspección de dependencias y de escaneo IaC se acoplen como etapas obligatorias del pipeline de integración y despliegue continuo (CI/CD) [33]. Los plugins nativos para Jenkins, GitLab CI, GitHub Actions o Azure DevOps, algunos de ellos potenciados por inteligencia artificial [41], insertan controles de conformidad automáticos que rechazan *builds* con vulnerabilidades por encima de umbrales establecidos, acoplando el concepto de seguridad hacia la izquierda e introduciendo correcciones cuando el costo de remediar aún es marginal [38].

Por otro lado, para mitigar la fatiga operativa derivada de múltiples consolas, los datos resultantes deben converger en plataformas unificadas, donde se procesen mediante formatos normalizados (CEF, JSON o STIX/TAXII) y se enriquezcan con taxonomías MITRE ATT&CK y catálogos KEV. Este tejido de integración ofrece una vista panorámica de exposición sin alternar entre interfaces heterogéneas, además de entregar contexto de táctica/técnica y estado de explotación real.

Finalmente, la interconexión por API con soluciones SOAR permite encadenar playbooks sin intervención humana: ingestión de indicadores de compromiso, ejecución en *sandbox*, apertura de caso, aplicación de parches o endurecimiento de reglas en firewalls [42]. La automatización de estos circuitos no solo reduce el tiempo medio de respuesta, sino que consolida un ciclo de retroalimentación continuo donde cada detección refina la postura defensiva y el aparato de cumplimiento normativo en igual medida.

4.3 Acciones para cerrar brechas de cobertura

La detección de vulnerabilidades no concluye al desplegar escáneres; mantener una cobertura plena exige medir de forma continua qué activos se revisan, con qué profundidad y qué vacíos persisten, ajustar la cartera de herramientas con criterios de costo-beneficio, cultivar competencias internas que automaticen tareas repetitivas y, cuando la magnitud lo imponga, delegar funciones en proveedores especializados sin perder la gobernanza técnica ni el control de los datos.

Un programa maduro comienza por contrastar, activo por activo, el inventario consolidado en CAASM con los registros de cada motor de descubrimiento; cualquier host, contenedor o microservicio que no figure en ambos listados constituye un punto ciego. Esto podría incluir entornos de tecnología operativa (OT), dispositivos IoT, API no documentadas, despliegues contenerizados o aplicaciones legado [10].

Respecto a la adquisición de tecnologías que aborden puntualmente las brechas descubiertas (p. ej., IAST para defectos en ejecución, EASM para perímetro o sondas OT/IoT para plantas), se debe equilibrar el alcance funcional, la integración con el ecosistema de seguridad existente y el horizonte de soporte, tal que los nuevos datos y capacidades se incorporen fluidamente al flujo de trabajo [43].

Asimismo, cuando los plazos de parcheo son muy estrictos o la superficie de ataque se expande a múltiples zonas geográficas, un proveedor de servicios de seguridad administrados (*Managed Security Service Providers*, MSSP) aporta vigilancia 24 horas al día y 7 días a la semana, junto con personal especializado y centros de operaciones distribuidos, además de contribuir con la integración de feeds de amenazas, el monitoreo

de la *dark web* y la realización de pruebas de intrusión [44].

Aun contando con productos de terceros, los equipos pueden recurrir a una automatización ligera mediante *scripting* interno. En concreto, es factible escribir *scripts* en Python, PowerShell o Bash para acelerar la ingesta de resultados, unificación de formatos,enriquecimiento con ATT&CK y envío a paneles de riesgo. Estas capacidades internas aportan flexibilidad, reducen costes,y suplen carencias de funcionalidades *out-of-the-box* y posibilitan una adaptación rápida a cambios de fuentes.

Por último, las auditorías periódicas son el mecanismo de control que garantiza que el inventario de activos refleje con precisión la realidad organizacional, confirmando que cada activo se halla debidamente registrado, categorizado y protegido [43].

La Tabla 4.1 presenta una guía escalonada y técnicamente fundamentada para eliminar puntos ciegos en el descubrimiento de vulnerabilidades en infraestructuras críticas. Se halla alineada con los hitos de madurez definidos por el modelo CERT-RMM y contempla desde escenarios iniciales con recursos limitados hasta arquitecturas avanzadas con visibilidad continua, automatización y manejo integral. Además, incluye metas estratégicas, acciones técnicas, herramientas recomendadas, indicadores clave y requisitos presupuestales, trazando una trayectoria progresivo y realista para consolidar capacidades de detección y respuesta frente a un panorama de amenazas cada vez más sofisticado.

Tabla 4.1: Trayectoria de madurez para ampliar la cobertura en la detección de vulnerabilidades.

Escalón de madurez	Objetivo operativo	Cobertura (ámbito y método)	Acciones técnicas clave	Esfuerzo y recursos
MIL-1: Realizado (Visibilidad incipiente)	Obtener una fotografía básica de la superficie de ataque.	- Subredes internas y DMZ - Servidores críticos *on-premise*. - Puestos de usuario más expuestos.	1. Despliegue de OpenVAS y Nmap para descubrimiento de hosts, puertos y servicios. 2. Activación de alertas del catálogo CISA KEV. 3. Inventario manual en hojas de cálculo y etiquetado de criticidad básica (CIA).	**Bajo**: Software de código abierto, personal interno y horas extra limitadas.
MIL-2/3: Planificado y gestionado (Cobertura ampliada y normalizada)	Sustituir la exploración *ad hoc* por un ciclo de descubrimiento regular y mayor profundidad.	- Infraestructura on-premise completa (servidores, red, bases de datos, etc.). - Aplicaciones web críticas. - Instancias IaaS/PaaS en nubes públicas.	1. Licenciar Nessus, Qualys VMDR o Rapid7 InsightVM; programar escaneos mensuales. 2. Añadir SAST/DAST/IAST en *pipeline* CI/CD para portales de banca y CBDC piloto. 3. Suscribirse a FS-ISAC y contratar un proveedor externo de inteligencia de amenazas. 4. Enviar resultados al SIEM y correlacionar con autenticaciones y logs de firewall.	**Moderado**: Licencias comerciales, formación del personal y horas de integración.

MIL-4/5: Medido y definido (Visibilidad continua, orquestada y predictiva)	Descubrimiento en tiempo real, priorización en función del contexto y reacción automatizada.	- Todo el espectro híbrido: *on-premise*, multinube, contenedores, dispositivos móviles, etc. - Superficie externa (EASM) y SaaS ofertados por terceros.	1. Agentes ligeros (Qualys Cloud Agent, Rapid7, Tanium, etc.) desplegados en servidores y *endpoints* para telemetría continua. 2. Plataformas de inteligencia de amenazas y EASM para enriquecer CVE. 3. SOAR para ejecutar *playbooks* que lleven a cabo el aislamiento de host, la carga tiquete a Jira, la actualización de CMDB o la activación de parches. 4. Análisis de brechas de cobertura trimestral, comparando CMDB, logs de red, cuentas cloud y dispositivos MDM. 5. Machine Learning/UEBA en el SIEM para examinar anomalías de comportamiento.	**Alto**: Suites integradas, IA y MSSP/hunters. El ROI es soportado por la reducción de riesgo sistémico.

5 Estrategias de decisión y automatización en la remediación

5.1 Matrices operativas para acción y orquestación de la remediación

La priorización de vulnerabilidades es un pilar de la estrategia de ciberseguridad debido a que posibilita una gestión preventiva del riesgo y reduce la probabilidad de brechas. En el caso de un banco central, tal proceso debe superar la mera severidad técnica y apoyarse en un marco de decisión multicriterio que integre métricas de riesgo, evidencias de explotabilidad en el entorno, exposición y criticidad del activo, impacto operativo y dependencias, en conjunto con el contexto de negocio y las obligaciones regulatorias, como se describió en el Capítulo 3. En lugar de remediar de acuerdo con el orden de descubrimiento, se ponderan tales variables para intervenir primero aquello que materializa un riesgo real y significativo para la misión y la continuidad operativa. Entre los determinantes habituales destacan:

1. **Puntaje CVSS (Common Vulnerability Scoring System)**: Proporciona una evaluación estandarizada de la severidad de las vulnerabilidades. Incluye métricas base que describen las cualidades intrínsecas de una vulnerabilidad (vector de ataque, complejidad, requisitos previos, privilegios requeridos e interacción del usuario) y estiman su impacto sobre la confidencialidad, integridad y disponibilidad tanto del sistema afectado como, cuando procede, de sistemas subsiguientes [23]. Asimismo, CVSS v4.0 introduce métricas de amenaza (como la madurez de explotación) y suplementarias; estas últimas añaden contexto sin modificar la puntuación: *safety* (seguridad, impacto en personas), automatizable, recuperación, densidad de valor, esfuerzo de respuesta ante la vulnerabilidad y urgencia del proveedor [23]. En conjunto, estas dimensiones favorecen decisiones más acertadas: ayudan a discernir qué hallazgos requieren tratamiento inmediato por su probabilidad real de explotación, su efecto cascada o la concentración de activos críticos.

2. **Explotabilidad y amenaza activa**: Estima la propensión de una debilidad a ser aprovechada en el corto plazo a partir de señales observables: existencia de *exploits* públicos (por ejemplo, registrados en el CISA KEV) o códigos de prueba de concepto, referencias en fuentes de inteligencia y evidencia de uso por actores maliciosos [24]. Estas pistas elevan de inmediato la urgencia de tratamiento. En esta línea, modelos contemporáneos como EPSS asignan un puntaje probabilístico de explotación que complementa a CVSS, al incorporar componentes de prevalencia y dinamismo adversario que no se reflejan en la severidad técnica pura.

3. **Impacto operativo y contexto del negocio**: Valora las consecuencias sobre operaciones, continuidad del servicio, reputación y cumplimiento normativo si la vulnerabilidad llegara a materializarse. Resulta clave integrar un análisis de impacto del negocio (*Business Impact Analysis*, BIA), el cual constituye un proceso sistemático que evalúa los efectos potenciales de las interrupciones en las funciones esenciales, consolidándose como un componente vital de la planificación de la continuidad del negocio (BCP) [45]. En concreto, ayuda a identificar los flujos de trabajo y activos primordiales, así como a comprender el impacto del tiempo de inactividad en los ingresos, las operaciones y la reputación. Adicionalmente, el BIA establece los objetivos de tiempo de recuperación (RTO) y los de punto de recuperación (RPO), que son métricas cruciales para determinar la tolerancia a la interrupción y la pérdida de datos [45]. Dado que el CVSS no contempla el marco organizacional, conviene asignar mayor peso a debilidades que inciden en procesos núcleo o datos sensibles. El BIA localiza dichos componentes y ordena la atención conforme a potenciales pérdidas monetarias, indisponibilidad operativa, deterioro reputacional o implicaciones legales y regulatorias [45].

4. **Exposición del activo**: Examina la accesibilidad del sistema desde dominios externos o segmentos internos. Un servicio expuesto a Internet revela una superficie de ataque ampliada y un radio de descubrimiento masivo mediante barridos programados. En consecuencia, el riesgo relativo aumenta y su tratamiento se antepone en la cola de remediación [46]. Por el contrario, debilidades en plataformas confinadas a redes internas adquieren menor urgencia, salvo que existan vectores ya confirmados que habiliten movimiento lateral y eleven de inmediato la prioridad.

5. **Obligaciones regulatorias y cumplimiento**: En el ámbito financiero, los supervisores fijan plazos y criterios para corregir debilidades según su criticidad; en Estados Unidos, diversas guías recomiendan subsanar fallas críticas en sistemas expuestos a Internet en un máximo de quince días [47]. A su vez, el reglamento europeo DORA exige procedimientos documentados para la administración de vulnerabilidades y el ciclo de parches, con calendarios definidos y rutas de esca-

lamiento cuando no sea posible atenderlos a tiempo [48]. El incumplimiento de tales parámetros suele traducirse en hallazgos de auditoría, sanciones o medidas correctivas impuestas por la autoridad. Integrar estas exigencias en la matriz de priorización refuerza la trazabilidad, disciplina y coherencia entre riesgo técnico y obligaciones de cumplimiento.

De este modo, el proceso se erige como un instrumento decisorio para equipos técnicos, alta dirección y organismos supervisores, debido a que articula tanto la urgencia como la justificación de cada medida correctiva y respalda la asignación de recursos finitos allí donde el riesgo es más grave [45].

Mientras la Tabla 3.3 del Capítulo 3 determina la jerarquía de atención por vulnerabilidad (cruce CVSS con explotabilidad EPSS/KEV), el presente apartado traslada esa calificación al terreno operativo. Aquí se consolida, por un lado, el perfil del activo —criticidad, exposición, RTO/RPO y propietario— como entrada a flujos delegados a procesos tecnológicos; y, por otro, se asocia cada CVE a una acción concreta, con SLA y responsable. De esta manera, la jerarquía técnica se convierte en remediación programada, contención o control compensatorio, con seguimiento y gobernanza del cambio.

Con tal propósito, se sugieren dos instrumentos complementarios: la matriz sobre perfil de criticidad del activo, que consolida atributos intrínsecos del recurso (servicio que soporta, ventanas de recuperación, visibilidad externa y propietario) para guiar las decisiones sobre cuándo, dónde y cómo ejecutar parches, aislamientos o ajustes de configuración, respetando RTO/RPO y dependencias; y la matriz de acción por vulnerabilidad, la cual asocia cada CVE con su orden de atención, categoría de resolución (corrección inmediata, contención temporal, endurecimiento o excepción controlada), SLA y equipo a cargo.

Ejemplos conceptuales de ambos recursos pueden ser consultados en la Tabla 5.1 y la Tabla 5.2.

Tabla 5.1: Perfil de criticidad del activo para orquestación de respuesta (vista por activo).

ID activo	Activo crítico (nombre)	Proceso/servicio que soporta	Impacto macroeconómico o reputacional	RTO	RPO	Exposición (Internet/Interno)	Propietario/Área
A-001	RTGS-Core (LBTR)	Pagos mayoristas / liquidación bruta en tiempo real	USD 5,000,000	1 h	5 min	Internet (a través de pasarela)	Plataforma de Pagos

Tabla 5.2: Matriz de acción por vulnerabilidad (vista operativa).

ID activo	Vulnerabilidades identificadas	Afectación confidencialidad	Afectación integridad	Afectación disponibilidad	Explotabilidad	Priorización	Categoría de acción	Responsable remediación
A-001	CVE-2024-12345 (OpenSSL 1.x) – Ejecución remota	V	V	V	KEV: Sí · EPSS: 0.86 · PoC: Sí	Máxima	Crítico inmediato (≤72 h)	Equipo infraestructura
A-001	CVE-2023-45678 (Servicio SSH) – Configuración débil	F	V	F	KEV: No · EPSS: 0.22 · PoC: No	Media	Prioridad normal (≤45 días)	Seguridad de plataforma /DevOps

5.2 Guía técnica para automatización progresiva

5.2.1 Orquestación y respuesta automatizada (SOAR)

Las plataformas de orquestación y respuesta (SOAR) consolidan las operaciones del centro de seguridad mediante flujos programables que ejecutan tareas recurrentes y coordinan acciones entre herramientas heterogéneas [49]. Sus playbooks —secuencias declarativas con validaciones, ramificaciones y puntos de aprobación— estructuran el triaje de alertas, el enriquecimiento con información de SIEM, CTI y CMDB, la correlación con marcos como MITRE ATT&CK, además del lanzamiento de escaneos y la programación de parches, con lo que disminuyen errores operativos y liberan a los analistas para investigaciones de mayor complejidad [49]. Adicionalmente, un SOAR integra escáneres de vulnerabilidades, gestores de parches (p. ej., Microsoft SCCM/Intune o IBM BigFix) y sistemas de tiquetes (como Jira o ServiceNow), creando un circuito continuo desde la detección hasta la corrección [42].

Procediendo así, ante un boletín crítico, el playbook puede vigilar fuentes de avisos, identificar versiones expuestas cotejando el inventario, ponderar explotabilidad (EPSS y KEV) y criticidad de negocio, abrir casos con SLA definidos, calendarizar despliegues escalonados dentro de ventanas de servicio, llevar a cabo pruebas de verificación, aislar de forma temporal nodos vulnerables, entre otros [42]. Asimismo, toda acción queda registrada con rigor documental —quién, qué y cuándo—, lo que refuerza auditorías, métricas de desempeño (MTTD/MTTR) y otros KPIs.

Prerrequisitos: Disponer de un catálogo vivo de activos (CMDB reconciliada con descubrimiento continuo local, en nube y endpoints), herramientas interoperables, playbooks versionados con trazabilidad y procedimientos de gobierno correctamente formulados. Asimismo, es indispensable definir criterios de decisión ante cada tipo de hallazgo y garantizar un registro auditable de las acciones emprendidas.

Riesgos: Derivados de una calibración incorrecta se tienen: acciones inapropiadas, despliegues incompatibles, bloqueos involuntarios o degradaciones de disponibilidad. Por ello, es prudente mantener puntos de decisión humana en hitos críticos [42], por ejemplo, exigiendo aprobación previa por analista o comité responsable antes del paso a producción.

5.2.2 Aislamiento automático mediante microsegmentación

La microsegmentación consiste en dividirla red en dominios de muy alta granularidad y aplicar políticas de control de tráfico estrictas que gobiernan comunicaciones este-

oeste, es decir, entre sistemas en el interior del centro de datos. Con tal diseño, ante una debilidad grave o un indicio de intrusión, es posible aislar de forma automática el componente comprometido y confinar la amenaza [50]: por ejemplo, trasladarlo a una zona de cuarentena o imponer reglas de denegación que impidan el movimiento lateral del adversario. Lo anterior reduce de manera drástica la superficie de exposición [50], limita la propagación de ataques y actúa como control compensatorio en entornos donde coexisten plataformas legadas difíciles de parchear [51], lo cual constituye un escenario habitual en el sector bancario.

Prerrequisitos: Se requiere infraestructura definida por software o soluciones bajo el principio de confianza cero (*Zero Trust*) capaces de imponer reglas dinámicas en distintos puntos de aplicación (por ejemplo, VMware NSX, Illumio, además de arquitecturas SDN y NAC avanzadas). Resulta igualmente imprescindible contar con visibilidad de dependencias y una clasificación precisa de qué cargas deben comunicarse entre sí. Idealmente, tales políticas se expresan como etiquetas vinculadas al inventario (CMDB) para evitar ambigüedades [52].

Riesgos: Reglas erróneamente concebidas pueden aislar servicios legítimos, interrumpiendo servicios esenciales inesperadamente, mientras que el exceso de granularidad puede derivar en complejidad de gobierno. Además, si la automatización no se sustenta o justifica por detecciones fiables, correlación de múltiples señales y umbrales conservadores, es probable que la tasa de falsos positivos aumente considerablemente. Por ello, se recomienda comprobar el funcionamiento de las políticas en entornos de ensayo, incorporar métricas de salud posteriores al cambio y documentar procedimientos de reversión y protocolos *break-glass* para reintegrar rápidamente sistemas aislados una vez saneados [53].

5.2.3 Parches automáticos e integración continua

La instalación de parches sin intervención del personal acorta el intervalo entre la publicación de una corrección y su implementación efectiva [38], reduciendo la ventana de exposición y homogeneizando la postura defensiva. Respecto a la estrategia, las plataformas de administración centralizada permiten programar actualizaciones periódicas, aprobaciones y grupos piloto, mientras que las buenas prácticas apuntan a iniciar en entornos controlados o en flotas de baja criticidad antes de avanzar hacia componentes clave [46].

Prerequisitos: Es indispensable contar con un manejador de parches y repositorios confiables (por ejemplo, Microsoft Endpoint Manager/Intune, IBM BigFix, Red Hat Satellite o gestores nativos de paquetes), en conjunto con un inventario fidedigno (CMDB) y bases de configuración estandarizadas [46]. Se requiere, asimismo, un ecosistema

previo a producción donde se lleven a cabo pruebas exhaustivas y seguimiento del funcionamiento posterior a la actualización.

Riesgos: El principal riesgo es operativo: incompatibilidades, dependencias no previstas o reinicios no coordinados pueden degradar servicios críticos. A fin de mitigar, conviene aplicar despliegues graduales y mantener planes de reversión listos (instantáneas, desinstalación o conmutación a la versión anterior). Por último, la programación debe respetar ventanas de mantenimiento aprobadas y registrar trazabilidad completa para auditoría y análisis forense.

5.2.4 Requisitos transversales de automatización

La automatización exige una planificación minuciosa y una valoración explícita de las condiciones habilitantes y riesgos operativos, de modo que los flujos orquestados eleven la postura defensiva sin introducir fragilidades nuevas. Los siguientes prerrequisitos y consideraciones son transversales a diversas estrategias e iniciativas que se desenvuelven en este ámbito:

Prerrequisitos:

- **Inventario de activos completo y en tiempo real**: La orquestación depende de una visibilidad exhaustiva de sistemas, dependencias y propietarios. La carencia de un inventario preciso conduce a que las acciones programadas no se desplieguen correctamente o a que activos críticos permanezcan sin protección [43].
- **Políticas y procedimientos claros**: Es fundamental disponer de normativa documentada para la identificación, priorización y tratamiento. Las políticas deben establecer roles y responsabilidades, así como criterios para atender excepciones y aprobaciones [38]. La trazabilidad de cada decisión sostiene la realización de auditorías y la disciplina operativa.
- **Madurez de procesos de seguridad**: Los procesos deben estar bien definidos, ser consistentes y acoplarse a umbrales comparables con MIL3-Managed o MIL4-Measured del CERT-RMM4 antes de intentar una optimización a gran escala. De lo contrario, orquestar tareas defectuosas amplificará las ineficiencias existentes. Métricas como MTTD/MTTR, cumplimiento de SLA y calidad del inventario actúan como barómetro de preparación.
- **Interoperabilidad**: Las plataformas de deben ser capaces de integrarse sin problemas con los sistemas existentes del banco, incluyendo SIEM, herramientas de administración de servicios de TI (ITSM), escáneres de vulnerabilidades y plataformas de inteligencia de amenazas.

- **Personal capacitado**: Pese a que aminora la carga de trabajo manual, se exige personal con habilidades avanzadas para diseñar, parametrizar, mantener y supervisar flujos automatizados. Asimismo, es crucial contar con expertos para atender excepciones, falsos positivos y situaciones complejas que la plataforma de orquestación no puede resolver.

Riesgos:

- **Falsos positivos y fatiga de alertas**: Reglas mal calibradas y correlaciones escasas pueden disparar volúmenes masivos de eventos legítimos, provocando sobrecarga cognitiva en los analistas, desensibilización ante señales críticas y paulatina pérdida de confianza en los playbooks y paneles de monitoreo [41].
- **Impacto operacional no deseado**: Acciones automáticas, si no se validan en entornos de prueba y con criterios de *go/no-go*, pueden ocasionar interrupciones imprevistas [54]. Un *hotfix* defectuoso o una política errónea puede desencadenar efectos en cascada sobre recursos esencialmente, especialmente en un banco central.
- **Complejidad de configuración y mantenimiento**: Orquestaciones extensas y políticas de microsegmentación resultan difíciles de versionar, auditar y probar minuciosamente. Por ende, una parametrización defectuosa puede introducir nuevas superficies de riesgo, desde denegaciones a flujos válidos hasta exposiciones inadvertidas.
- **Dependencia excesiva y puntos ciegos**: La sobreconfianza en decisiones automáticas sin supervisión humana favorece el sesgo: campañas sigilosas pueden eludir la telemetría instrumentada, mientras respuestas inadecuadas se ejecutan sin vigilancia del personal capacitado. La automatización es una herramienta, no un sustituto del juicio experto.

Se sugiere ampliar de forma controlada el alcance de las acciones sistematizadas: primero tareas de bajo riesgo (como la recolección de datos, las notificaciones o la apertura de tiquetes), después respuestas semiautónomas con validación humana y, únicamente donde resulte seguro, acciones plenamente automáticas (por ejemplo, aislar un segmento de red o desplegar un parche rutinario). Tal esquema exige gobernanza rigurosa: mantener un catálogo de playbooks, examinar resultados con periodicidad fija y ajustar a partir de lecciones aprendidas.

En bancos centrales, la adopción debe ser aun más prudente dada la sensibilidad de sus misiones, razón por la que conviene empezar por entornos administrativos antes de intervenir plataformas de pagos de alto valor. En suma a ello, el despliegue ha de sustentarse en una comprensión profunda de los riesgos operativos, preservando un *human in the loop* (humano en el circuito) para las decisiones críticas. El objetivo es

alcanzar operaciones de seguridad con alto grado de autonomía, pero siempre bajo dirección estratégica humana.

5.3 Ventanas de servicio y gobernanza del cambio

La NIST SP 800-40 Rev. 4 propone un marco integral para la orquestación del ciclo de parchado y provee criterios para fijar y gobernar las ventanas de servicio. El documento subraya que el parchado es crucial para la continuidad del negocio: invertir en procesos y capacidades de actualización reduce la probabilidad de compromisos, acota vectores de explotación y mitiga interrupciones en servicios esenciales [55].

Cada banco debe fijar, mediante una política formal, las franjas horarias autorizadas para desplegar parches en producción. Tales intervenciones se programan en periodos de baja demanda [54] (madrugada, fines de semana o interrupciones planificadas) con el fin de sincronizar el calendario técnico con el calendario de negocio e impedir modificaciones durante actividades sensibles, como el cierre contable mensual o la compensación interbancaria. Conforme a las buenas prácticas, los ciclos de actualización se alinean con el perfil de riesgo de cada sistema y consignan plazos máximos de atención por severidad de la vulnerabilidad [55]. A modo orientativo, para sistemas expuestos se adoptan horizontes de 15 días para debilidades de máxima severidad, 30 a 45 días para alta severidad y periodos mayores para casos medios o bajos, ajustando en concordancia con la sensibilidad del servicio [46]. Dichas reglas deben incorporarse a procedimientos internos, en coherencia con marcos regulatorios aplicables (como DORA en la Unión Europea).

Para cada intervención de parchado, la entidad debe elaborar un documento que identifique los sistemas implicados, el horario exacto de ejecución y los controles de verificación previa y posterior [55]. Adicionalmente, ha de incorporar un plan de reversión con medidas concretas como copias de seguridad, instantáneas y disponibilidad de versiones anteriores. Se exige, asimismo, aprobación previa por el comité de cambios o el responsable del proceso, comunicación a las partes interesadas sobre el impacto esperado, soporte durante la franja de mantenimiento y contingencias preparadas [55]. Finalmente, conviene reservar intervalos de reversión dentro de la misma ventana para deshacer la actualización si los indicadores posteriores no resultan satisfactorios [46], evitando prolongar la indisponibilidad en servicios sensibles como cajeros o transferencias electrónicas. En aplicaciones de alta sensibilidad resulta idóneo el *blue-green deployment* (donde se utilizan dos ambientes idénticos, *blue* para la versión estable de la aplicación y *green* para la nueva versión, con conmutación inmediata ante fallos) [56]. Por otro lado, los parches de emergencia fuera del calendario regular exigen mecanismos de *rollback* ágiles, puesto que el margen de pruebas suele ser limitado.

En consonancia con lo anterior, las ventanas de servicio funcionan como válvulas de seguridad que equilibran celeridad de protección y continuidad, siempre que cada vulnerabilidad priorizada se agende en el intervalo apropiado y la actualización se documente con análisis de impacto, inactividad prevista, responsables, criterios de éxito y plan de retorno. Así, el ciclo de actualización permanece previsible, transparente y seguro, en consonancia con el control de cambios y la continuidad del negocio exigidos por los supervisores.

6 Causa raíz, métricas y mejora continua

6.1 Dificultades en el cierre de vulnerabilidades

Los ciclos de atención y remediación de vulnerabilidades tropiezan con obstáculos recurrentes que erosionan la eficacia del programa de seguridad, como:

- **Arquitecturas complejas y activos no inventariados**: La expansión de entornos locales, nubes públicas/privadas y despliegues híbridos, junto con una flota heterogénea de dispositivos, introduce interdependencias que dificultan el descubrimiento continuo y la trazabilidad de vulnerabilidades a lo largo de todo el ciclo de vida [10]. En particular, el *shadow IT* genera superficies de ataque ocultas que evaden controles formales, impidiendo una visión integral del riesgo y degradando la eficacia de los mecanismos de protección [10].
- **Sobrecarga de hallazgos**: El caudal diario de debilidades reportadas puede saturar a los equipos, diluyendo la atención sobre exposiciones con probabilidad real de explotación [57].
- **Parcheo y control de cambios en producción**: La aplicación de correcciones de seguridad exige ventanas de mantenimiento, pruebas de regresión y validaciones de compatibilidad. La gestión irregular o tardía de parches debilita la seguridad general y puede derivar en interrupciones del servicio o fallos colaterales [54].
- **Comunicación y coordinación multidisciplinar**: En organizaciones complejas confluyen funciones con mandatos distintos (seguridad, TI, propietarios de aplicaciones, respuesta a incidentes, arquitectura, entre otras). Ambigüedades en responsabilidades, acuerdos de nivel de servicio poco precisos o flujos de trabajo fragmentados introducen latencias en la remediación [38]. Adicionalmente, suelen presentarse prioridades desalineadas: el equipo de seguridad puede calificar un hallazgo como crítico, mientras desarrollo u operaciones priorizan otras tareas, dilatando la atención de riesgos severos [38].
- **Proliferación de herramientas y fatiga de alertas**: La coexistencia de múltiples plataformas con interfaces heterogéneas obliga a cambios continuos de contex-

to, eleva la complejidad operativa y ralentiza la toma de decisiones [58]. Adicionalmente, un volumen elevado de falsos positivos precipita fatiga de alertas, fenómeno que reduce la atención del analista y aumenta la probabilidad de pasar por alto señales críticas.

- **Restricciones de recursos y capacidades**: Plantillas limitadas, brechas de talento en ciberseguridad y márgenes presupuestales acotados dificultan un ciclo integral de descubrimiento, priorización y tratamiento de vulnerabilidades en plazos prudentes [58].
- **Remediación irregular o diferida**: Ausencia de procedimientos consolidados, criterios de priorización débiles o dependencia de ventanas de mantenimiento excesivamente rígidas conduce a cierres tardíos e inconsistentes, manteniendo superficies de exposición innecesarias [57].
- **Vigilancia continua insuficiente**: Un incorrecto monitoreo y auditoría posterior a la corrección permite que determinadas debilidades persistan sin ser detectadas o que mitigaciones se apliquen de forma incompleta [57].

La mitigación efectiva de tales situaciones exige una estrategia convergente que, tal como se detalló en capítulos anteriores, articule inventariado integral de activos y detección de *shadow IT*, priorización sustentada en riesgo (con señales de explotación activa, criticidad del servicio y catálogos KEV/EPSS), así como consolidación de plataformas con orquestación/automatización de flujos (SOAR, tableros unificados, deduplicación y correlación) para reducir ruido y latencia. A su vez, conviene formalizar gobierno y responsabilidades, robustecer el control de cambios y el parcheo mediante pruebas de regresión y, cuando la actualización inmediata resulte inviable, aplicar controles compensatorios (segmentación, listas de control de acceso, hardening, etc.) que acoten la exposición. Además, la adopción de observabilidad continua —métricas, logs y trazas con validación posterior a la corrección— y el fortalecimiento de habilidades mediante capacitación avanzada, automatización de tareas repetitivas y racionalización presupuestal elevan la productividad sin sacrificar gobernanza del riesgo [57].

6.2 Metodología de análisis de causa raíz

Cuando ciertas vulnerabilidades tienden a reaparecer de forma recurrente (por ejemplo, la misma configuración débil en múltiples sistemas o fallos similares en código de distintas aplicaciones), es señal de factores subyacentes no resueltos. El análisis de causa raíz (RCA) constituye una metodología sistemática de investigación orientada a trascender los síntomas y a caracterizar el origen estructural de vulnerabilidades e incidentes [59].

Un marco integral para ejecutar una investigación de RCA exitosa incluye los siguientes pasos [59]:

- **Delimitación precisa del problema o de la vulnerabilidad recurrente**. En primer término conviene consignar, con rigor documental, qué debilidad reaparece, bajo qué condiciones operativas emerge, cuál es su efecto y por qué resulta especialmente preocupante para funciones esenciales del banco central.
- **Acopio de evidencias y cronología analítica**. Seguidamente, procede reunir todos los elementos probatorios: registros de escáneres, informes de pruebas de penetración, fragmentos de código y configuraciones involucradas, fechas de aparición, autoría de cambios y cualquier artefacto que aclare el entorno de ocurrencia. Con ello se construye una línea temporal que contextualiza cada episodio y revela relaciones causales. Además, resulta provechoso comprobar si los sistemas vulnerables comparten componentes comunes o si existió alguna excepción en el ciclo de parchado.
- **Hipótesis causales y factores contribuyentes**. A continuación, conviene aplicar técnicas estructuradas. «Los 5 ¿por qué?» (5 whys) indagan sucesivamente el «¿por qué ocurrió?» hasta alcanzar un punto sin respuestas lógicas adicionales, momento en que suele aflorar el núcleo causal. Resulta igualmente crucial involucrar a las partes relevantes (desarrollo, administración de sistemas, análisis de seguridad, etc.) en sesiones de lluvia de ideas. En ocasiones, el origen responde a tensiones organizacionales (por ejemplo, presión de negocio que pospone la instalación del parche), y solo un diálogo transversal revela tales condicionantes.
- **Evaluación de la causa raíz más plausible**. Con la lista de candidatas en la mano, procede depurarla mediante preguntas orientadas a evidencias: ¿qué hipótesis explica mejor todas las ocurrencias?, ¿qué pruebas la confirman o la refutan?, ¿existen factores concurrentes que actúen en conjunto? Tal validación puede requerir pruebas adicionales o revisión por pares. Con frecuencia aparece un origen organizacional o procedimental más que un fallo puntual, lo que obliga a orientar la atención más allá de lo estrictamente técnico.
- **Documentación de causas y escenarios no subsanables**. Pese a que el ideal apunta a una causa corregible, en determinadas circunstancias la evidencia resulta insuficiente o el origen se sitúa fuera del ámbito de control (por ejemplo, un componente de terceros opaco). Si, luego de un examen riguroso, no se alcanza una conclusión definitiva, conviene dejar constancia de las hipótesis revisadas y de los motivos que impidieron confirmarlas. No obstante, aun sin causa raíz definitiva, deben adoptarse medidas que eleven la visibilidad y aceleren la reacción.
- **Acciones correctivas y preventivas alineadas con la causa identificada**. Una vez aislado el origen —único o múltiple—, se formula un plan de respuesta que com-

pagine correcciones inmediatas con medidas de prevención a mediano y largo plazo. Por ejemplo, si el SCA revela carencias en seguridad de desarrollo, la corrección inmediata consistirá en parchear el código vulnerable, mientras que la prevención exigirá un programa de capacitación y la actualización de guías de codificación segura. Independientemente del escenario, la totalidad de las actuaciones debe consignarse a fin de consolidar el aprendizaje institucional y agilizar los procesos de clausura posteriores.

No obstante, persisten escenarios en los que no es factible detectar o inspeccionar dichas causas, por ejemplo:

1. **Insuficiencia de datos y telemetría**: La ausencia, pérdida o calidad deficiente de logs, métricas y evidencias forenses imposibilita reconstruir la secuencia causal con rigor.
2. **Complejidad sistémica extrema**: Arquitecturas densamente interconectadas, dependencias circulares y fallos concurrentes generan comportamientos que dificultan la caracterización de una causa única [59].
3. **Factores externos no controlables**: Campañas de amenazas persistentes avanzadas (APT) y operaciones ejecutadas por actores con capacidades estatales introducen obstáculos que limitan la atribución y entorpecen la identificación del origen.
4. **Restricciones de recursos y ventanas operativas**: Falta de tiempo, dotación especializada o herramientas de análisis reducen la profundidad de la investigación [59]. Si no se dispone de laboratorios para replicación, *sandboxes* instrumentados o cobertura de licencias adecuada, es posible que la causa subyacente no pueda confirmarse empíricamente.
5. **Cultura punitiva y silencios informativos**: En organizaciones que no priorizan el aprendizaje sin culpabilización individual, el temor a sanciones inhibe la revelación de errores, decisiones contingentes o señales tempranas [60].

6.2.1 Plantilla para vulnerabilidades recurrentes

La plantilla propuesta en la Tabla 6.1 se inspira en el formato *post mortem* de incidentes de Google [60] y se extrapola al análisis de causas raíz de vulnerabilidades recurrentes. Elaborada de tal forma, organiza la narrativa técnica, las evidencias y las decisiones que convierten hallazgos repetitivos en mejoras permanentes. Los autores indican que debe completarse con celeridad tras la detección de la recurrencia (idealmente en las primeras 24–72 horas), por un equipo multifuncional (seguridad, operaciones, desarrollo, riesgo y propietario del activo), manteniendo un enfoque sin atribución personal y

sustentando cada afirmación con pruebas constatables [60]. Su diligenciamiento se puede apoyar en insumos automatizados: escáneres de vulnerabilidades, SIEM para cronologías y correlaciones, CMDB/CAASM para inventario y dependencias, sistemas ITSM para trazabilidad de cambios o plataformas SOAR para extraer los artefactos derivados de playbooks.

Metodológicamente, la plantilla conduce desde la cronología y el mapeo causal hasta un plan de acción con criterios de aceptación, ventanas de mantenimiento, responsables nominados y métricas de cierre, lo que habilita el seguimiento ejecutivo y la auditoría. Tal estructura resulta idónea para el manejo de vulnerabilidades porque transforma correcciones *ad hoc* en cambios sistémicos (políticas, controles, capacitación, automatización, hardening, entre otros), reduce la reincidencia mediante prevención puntual y alinea las remediaciones con las prioridades del negocio, los plazos regulatorios y la resiliencia operativa.

Tabla 6.1. Plantilla de seguimiento para vulnerabilidades recurrentes (RCA y acciones).

Sección	Descripción y preguntas clave
Ficha maestra del caso	
ID del caso / versión	Identificador único y número de revisión del RCA.
Clasificación	Tipo (reincidencia de vulnerabilidad/configuración/proceso/proveedor).
Fecha de detección inicial	[AAAA-MM-DD]
Fecha(s) de recurrencia	[AAAA-MM-DD] (una o varias)
Activo(s) involucrado(s)	Nombre/ID, entorno, exposición, propietario funcional.
Descripción breve	CVE, tipo de vulnerabilidad, sistema/componente, síntesis del impacto inicial.
Impacto en negocio (recurrencia)	Efectos en procesos (pagos mayoristas, política monetaria o mercado).
1. Línea de tiempo y evidencias	
Cronología detallada	Secuencia desde la detección original hasta la recurrencia y primeras respuestas (fechas/hitos).
Evidencias adjuntas	Reportes de escáner, *pen-tests*, *logs*, *commits*, tiquetes de cambio, diagramas, capturas.
Condiciones de entorno	Cambios relevantes (parches, despliegues, proveedores o infraestructura) previos a la recaída.
2. Diagnóstico sin culpabilización	

Continúa en la página siguiente

Tabla 6.1. Plantilla de seguimiento para vulnerabilidades recurrentes (RCA y acciones). (Continuación)

Problema que reaparece	¿Qué volvió a ocurrir? ¿dónde y con qué síntomas?
Por qué falló la solución previa	Cobertura incompleta, excepciones, regresión, dependencia no cubierta, error de configuración, etc.
5 ¿Por qué? (5 Whys)	1º ¿Por qué…? → … / 2º ¿Por qué…? → … / 3º ¿Por qué…? → … / 4º ¿Por qué…? → … / 5º ¿Por qué…? → …
Mapa causal (Ishikawa)	Procesos / Personas / Tecnología / Proveedores / Entorno – causas potenciales clasificadas.
3. Causa raíz y verificaciones	
Hipótesis causal principal	Condición cuya eliminación prevendría la recurrencia.
Causas contribuyentes	Factores secundarios que amplifican la probabilidad o el impacto.
Riesgos si no se aborda	Efectos operativos, reputacionales y de cumplimiento.
Escenarios no resolubles	Evidencia insuficiente / componente opaco de tercero.
Registro de hipótesis evaluadas	Qué se consideró y por qué no se confirmó.
Plan de investigación continua	Qué datos faltan, cómo y cuándo obtenerlos.
4. Plan de acciones (correctivas y preventivas)	
Acciones inmediatas (contención/mitigación)	Por ejemplo: regla WAF, aislamiento y *hotfix*.
Acciones correctivas	Solución del caso actual.
Acciones preventivas	Evitar recurrencia: política, capacitación, automatización, *hardening*, mejora de escaneo.
Responsable(s)	Persona o rol asignado.
Recursos requeridos	Presupuesto, licencias y personal.
Dependencias	Interacciones con otras áreas o proveedores.
Fecha objetivo / ventana	Compromiso temporal.
5. Lecciones aprendidas	
Lo que funcionó	Decisiones, controles o coordinaciones que aportaron valor.

Continúa en la página siguiente

Tabla 6.1. Plantilla de seguimiento para vulnerabilidades recurrentes (RCA y acciones). (Continuación)

Lo que falló	Brechas de proceso, comunicación, coberturas técnicas o ventanas.
Cambios a institucionalizar	Actualizaciones a políticas, *playbooks*, estándares y *baselines*.
6. Seguimiento y métricas	
MTTR-RC (*Mean Time to Remediate – Root Cause*)	Tiempo entre la detección de recurrencia y eliminación de la causa raíz.
% acciones preventivas completadas	Acciones cerradas / acciones planificadas.
Reincidencias	Número de recurrencias del patrón tras el cierre.
Cobertura de control	% de activos afectados con control preventivo aplicado.
Cumplimiento de SLA	Casos cerrados dentro del plazo comprometido.
Gobernanza de seguimiento	Comité de seguridad examina avances, escalamiento a dirección si hay bloqueos y auditoría de evidencias.
7. Anexos	

6.3 Estrategias de mejora continua

El RCA constituye el punto de partida de un ciclo virtuoso de perfeccionamiento continuo en seguridad: una vez aislados los orígenes de vulnerabilidades —o eventos— recurrentes, deben emprenderse medidas preventivas y correctivas que afiancen procesos, reduzcan la probabilidad de recaída y eleven la disciplina operativa.

- **Eliminar o mitigar la causa raíz identificada**: Resulta imprescindible asegurar que el origen fundamental de la debilidad quede suprimido o, cuando ello no sea viable de inmediato, suficientemente atenuado [61]. Si la brecha proviene de un proceso, corresponde corregirlo e incorporar controles adicionales. Asimismo, si deriva de carencias de conocimiento, conviene diseñar capacitaciones orientadas.
- **Definir e implantar acciones correctivas y preventivas concretas**: Por cada hallazgo, se requiere establecer un plan con medidas tangibles, plazos, responsables y criterios de aceptación [60]. Ejemplos ilustrativos son «actualizar las pautas de aceptación en el despliegue para incluir la inspección de la configuración X», «habilitar la autenticación multifactor en el sistema Y antes de finalizar el año»

o «intervenir el código legado para erradicar el patrón de vulnerabilidad z». Dichas acciones deben orientarse a impedir recurrencias, por lo que la plantilla tipo *post mortem* adaptada a vulnerabilidades constituye un recurso útil para guiar la priorización, el seguimiento y la medición de la efectividad mediante indicadores claros.

- **Refinamiento de políticas, estándares y documentación operativa**: La mejora continua reclama el estudio de marcos normativos, guías técnicas y catálogos de controles a la luz de las causas detectadas [59]. Cuando emergen lagunas procedimentales, debe desarrollarse la guía faltante, mientras que, ante ambigüedades en responsabilidades, corresponde alinear roles, autoridades y flujos en el ciclo de vida de las vulnerabilidades. Asimismo, es perentorio nutrir bases de conocimiento con las lecciones aprendidas.
- **Capacitación y concienciación focalizadas en debilidades detectadas**: Dado que numerosos orígenes se relacionan con el factor humano, resulta pertinente diseñar campañas formativas que eleven la competencia técnica y consoliden hábitos seguros [61]. Por ejemplo, entrenamientos de hardening y buenas prácticas si se trata de errores de configuración; o talleres de desarrollo seguro frente a fallas de programación. Asimismo, la difusión transversal de las lecciones aprendidas convierte el caso puntual en aprendizaje institucional, refuerza la preparación ante amenazas emergentes [59].
- **Mejoras en herramientas y tecnología de apoyo**: Conviene evaluar con rigor si la plataforma tecnológica vigente permitió detectar o prevenir el incidente y, en su defecto, definir cierres de brecha alineados con prioridades de riesgo. Ello puede traducirse en incorporar análisis de código estático cuando defectos de software pasaron inadvertidos, habilitar descubrimiento continuo de activos externos para visibilizar superficies expuestas fuera del radar o perfeccionar monitoreo y correlación cuando la intrusión no se advirtió oportunamente.
- **Fortalecimiento de la respuesta y la resiliencia**: Las lecciones aprendidas deben traducirse en ajustes tangibles de playbooks de remediación, criterios de priorización y ventanas de cambio correctamente definidas [61]. Resulta provechoso realizar simulacros orientados a CVE críticas que verifiquen tiempos de aplicación, compatibilidades y rutas de reversión.
- **Seguimiento reforzado y detección temprana**: Puesto que ciertos riesgos no se suprimen por completo, la mejora sostenida exige monitoreo proactivo para detectar señales de recaída y confirmar la efectividad de las correcciones [61]. Ello incluye escaneo recurrente de las mismas debilidades y comprobaciones automatizadas.

6.3.1 Capacidades tecnológicas emergentes

La madurez del ciclo de vulnerabilidades exige incorporar capacidades inteligentes que conviertan grandes volúmenes de CVE en decisiones trazables y accionables. En este marco, resultan especialmente prometedoras las arquitecturas RAG (*Retrieval-Augmented Generation*) combinadas con proveniencia verificable de cada afirmación [62], puesto que reducen al mínimo las lagunas informativas, acotan el ruido y ofrecen una explicación sustentada de cada recomendación. Estas capacidades no sustituyen la ingeniería de procesos ni la gobernanza, sino que las amplifican, aportando velocidad, consistencia documental y un rastro de auditoría que satisface tanto a órganos de control como a terceros revisores.

Entre las propuestas más sobresalientes se encuentra ProveRAG (*Provenance-Driven Vulnerability Analysis with Automated Retrieval-Augmented LLMs*), un marco que emula el flujo de trabajo de un analista de seguridad: recuperar fuentes de autoridad, sintetizar hallazgos pertinentes, responder con lenguaje preciso y autoverificarse contra la evidencia citada [62]. Técnicamente, ProveRAG articula dos planos:

1. **Recuperación dirigida**, el cual extrae de NVD (National Vulnerability Database), CWE (Common Weakness Enumeration) y referencias anexas los fragmentos estrictamente relevantes para dos preguntas esenciales: cómo se explota y cómo se mitiga. En lugar de «trocear y pegar» textos extensos, el sistema resume por intención (explotación o mitigación), lo que reduce el sesgo por ventana de contexto y eleva la pertinencia del insumo.
2. **Generación controlada**, encargado de producir respuestas deterministas (temperatura baja), enriquecidas con las parejas respuesta-evidencia que anclan cada afirmación a su fuente.

Anclado a tales elementos, un módulo de autocrítica compara la salida con la documentación recolectada y clasifica la validez (verdadero positivo, alucinación y omisión), obligando al modelo a justificar su diagnóstico con pasajes que pueden ser citados [62]. El resultado no es sólo un texto, sino una pieza auditada, con referencias cruzadas y razonamiento explícito.

Desde la perspectiva operativa de un banco central, dicha aproximación aporta valor inmediato en tres frentes. En primera instancia, priorización sustentada: al combinar severidad (CVSS), explotabilidad observada (EPSS y presencia en CISA KEV) y mitigaciones con respaldo documental, ProveRAG alimenta la matriz de decisión sin depender exclusivamente del puntaje técnico. Segundo, aceleración del ciclo: la síntesis automatizada de guías de remediación reduce tiempos de elaboración de bitácoras de cambios, acorta la preparación de ventanas de mantenimiento y mejora la coordinación con proveedores. Tercero, trazabilidad regulatoria: cada recomendación conserva

citas constatables, lo que simplifica auditorías, inspecciones de cumplimiento y *post mortems* que exigen evidencia concluyente.

Por otro lado, la arquitectura es extensible. La integración con inventarios dinámicos (CMDB/CAASM), catálogos de dependencias de software (SBOM), escáneres de contenedores e infraestructura en la nube posibilita cruzar la información del NVD/CWE con la existencia real de activos. A esto se suma la posibilidad de inyectar fuentes sectoriales (boletines del sector financiero, inteligencia de amenazas propietaria, repositorios de configuraciones endurecidas, etc.) para especializar la salida sin perder el anclaje a estándares abiertos. Asimismo, cuando se dispone de bases enriquecidas como Aqua Vulnerability DB, la calidad de las recomendaciones sobre mitigación se incrementa sustancialmente [62].

El potencial trasciende el ámbito público. Para instituciones privadas (bancos comerciales, infraestructura de mercados, procesadores de pagos o *fintechs*), soluciones como ProveRAG pueden actuar como multiplicadores de productividad para filtrar referencias redundantes, unificar criterios entre equipos heterogéneos y generar artefactos reutilizables listos para incorporarse a pipelines CI/CD. Asimismo, dada una vulnerabilidad, el sistema puede proponer alternativas de mitigación con distinta huella operativa y explicar la opción recomendada con fundamento en la restricción temporal, la compatibilidad o el impacto en la disponibilidad. Para áreas de riesgo y cumplimiento, la producción de explicaciones estructuradas con citas textuales —que demuestran que la vulnerabilidad ha sido reconocida por fuentes oficiales— y métricas de calidad de evidencia —que corroboran que la respuesta del modelo se encuentra respaldada por texto fidedigno— disminuye la fricción habitual entre seguridad, desarrollo y auditoría interna.

No obstante, la adopción responsable de inteligencia artificial en este ámbito exige una hoja de ruta rigurosa y metódica. En la capa de datos, resulta indispensable establecer conectores resilientes hacia fuentes oficiales (NVD y CWE), catálogos de vulnerabilidades explotadas (KEV), repositorios internos y proveedores comerciales, complementado con la normalización de taxonomías (CVE, CWE, MITRE ATT&CK y SBOM) y políticas coherentes de retención y depuración. En la capa de modelo, deben aplicarse mecanismos de *prompting* controlado, filtros semánticos, limitaciones de tasa y bitácoras de ejecución. En suma a ello, para información sensible, es imperativo optar por entornos aislados (procesamiento *on-premise* o nubes privadas) y salidas que omitan detalles operativos confidenciales [63]. En la capa de integración, conviene fijar puntos de decisión humana en fases críticas, asegurando que cada acción quede documentada con trazabilidad completa. Finalmente, en validación y métricas, debe medirse la precisión (TP/FP/FN por tipo de consulta), la completitud (cobertura de mitigaciones por familia de debilidad), el MTTR-RC (tiempo medio hasta la eliminación de la causa raíz) y el porcentaje de acciones preventivas concluidas [63]. En caso de que la salida automatizada

no alcance el estándar esperado, procede la activación de rutas de revisión por pares. En última instancia, el principio rector debe ser la explicabilidad [63]: toda salida debe apoyarse en evidencia verificable por un experto y mantenerse abierta a refutación con pruebas más sólidas.

Existen, naturalmente, riesgos y limitaciones: dependencia de la calidad de las fuentes (obsolescencia o enlaces inactivos), sesgos en la selección de evidencias, restricciones excesivas que omitan detalles técnicos esenciales o fugas de información en ausencia de aislamiento del plano de inferencia [63]. No obstante, la incorporación de herramientas como ProveRAG aporta una capacidad analítica inédita que convierte la sobrecarga de CVEs en decisiones sólidas y sustentadas, acelera la preparación de cambios, optimiza la coordinación interinstitucional y, lo más relevante, convierte correcciones puntuales en transformaciones estructurales. Para los bancos centrales, este paradigma supone un salto cualitativo hacia programas de vulnerabilidades más ágiles, trazables y alineados con los imperativos estratégicos, sin alterar el rigor técnico ni relegar la supervisión humana en los momentos de mayor sensibilidad.

7 Conclusión

El documento elabora una ruta práctica y rigurosa para bancos centrales que requieren una gestión de vulnerabilidades guiada por el riesgo y las evidencias. Parte de marcos de madurez reconocidos y de un diagnóstico institucional realista para alinear capacidades, procesos y métricas con las prioridades del negocio financiero. Fundamentada en tales referentes, la propuesta integra gobierno técnico, ingeniería de inventario y automatización, con una narrativa que conecta principios metodológicos con decisiones operativas reproducibles en infraestructuras críticas.

El capítulo 2 coloca los cimientos: un censo integral de activos críticos con responsabilidades claras (matriz RACI), una metodología de puntuación de riesgo sustentada en CVSS v4.0, enriquecida con EPSS y la lista de explotaciones conocidas, en conjunto con una matriz de prioridad técnica que combina severidad, explotabilidad y contexto operativo. La incorporación de CAASM (administración de la superficie de ataque de activos cibernéticos) como capa de visibilidad y correlación aporta una vista unificada del parque tecnológico, eleva la fidelidad del inventario y habilita decisiones basadas en la exposición real, la criticidad del servicio y las dependencias.

Posteriormente, se detallan los motores de descubrimiento y las fuentes de inteligencia que alimentan la detección automatizada. La guía de integración propone flujos con STIX/TAXII para el intercambio estructurado, formatos operativos (CEF/JSON), taxonomías MITRE ATT&CK y pipelines CI/CD que introducen salvaguardas tempranas (shift-left). Así, se busca reducir puntos ciegos por etapas, con indicadores de cobertura, latencia de hallazgos y brechas por dominio tecnológico.

A continuacion, se traslada la calificación técnica a la ejecución automatizada. Las matrices operativas —vista por activo y vista por hallazgo— vinculan cada CVE con una categoría de tratamiento, SLA y equipos responsables, mientras que la guía técnica describe SOAR para playbooks repetibles, microsegmentación para aislamiento dinámico y parcheo continuo acoplado a integración continua. Respecto a esto último, las ventanas de servicio se armonizan con los umbrales de recuperación (RTO/RPO) y con la administración de cambios, garantizando trazabilidad de punta a punta y mínima disrupción en procesos misionales como pagos mayoristas, cámaras de compensación o servicios API de alto tráfico.

El último capítulo cierra el ciclo con análisis de causa raíz, métricas longitudinales y mejora constante en torno a MTTR, cobertura efectiva por dominio, reducción de exposición perimetral, atención prioritaria a entradas KEV y evolución de la postura en nubes públicas e infraestructuras híbridas. Este andamiaje convierte la telemetría dispersa en conocimiento accionable, robustece la evidencia para auditoría y supervisión, y eleva la resiliencia cibernética mediante decisiones informadas, medibles y sustentadas en estándares abiertos. En suma, la obra ofrece una arquitectura de trabajo que interpela.

Referencias

[1] 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. 3).

[2] *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. págs. 3, 8).

[3] Barry Snow. *NIST CSF 2.0: A Winning Framework for Vulnerability Management*. SecurityBridge Group. 2024. URL: https://securitybridge.com/blog/nist-csf-2-0-for-vulnerability-management/ (vid. pág. 3).

[4] David Holloway. *The Ultimate Guide to ISO 27002*. isms online. 2025. URL: https://www.isms.online/iso-27002/ (vid. págs. 3, 4).

[5] *OWASP SAMM Software Assurance Maturity Model*. OWASP. 2020. URL: https://owaspsamm.org/model/ (vid. pág. 4).

[6] *Cyber Security Evaluation Tool (CSET)*. U.S. Department of Homeland Security Cybersecurity e Infrastructure Security Agency (CISA). n.d. URL: https://www.cisa.gov/resources-tools/services/cyber-security-evaluation-tool-cset (vid. pág. 4).

[7] *Cybersecurity Performance Goals (CPGs)*. U.S. Department of Homeland Security Cybersecurity e Infrastructure Security Agency (CISA). n.d. URL: https://www.cisa.gov/cybersecurity-performance-goals-cpgs (vid. pág. 4).

[8] Aram Hovsepyan. *A comparison of NIST CSF 2.0 and OWASP SAMM*. Codific. 2025. URL: https://codific.com/a-comparison-of-nist-csf-and-owasp-samm/ (vid. pág. 4).

[9] *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. pág. 8).

[10] *What Is Attack Surface and Attack Surface Management?* Palo Alto Networks. n.d.

URL: https://www.paloaltonetworks.com/cyberpedia/what-is-attack-surface-management (vid. págs. 10-12, 22, 36).

[11] Tarik Hansen y Katya Delak. *Security Considerations for a Central Bank Digital Currency*. Board of Governors of the Federal Reserve System. 2022. URL: https://doi.org/10.17016/2380-7172.2970 (vid. págs. 10, 12, 15).

[12] Thomas M. Eisenbach, Anna Kovner y Michael Junho Lee. *When It Rains, It Pours: Cyber Vulnerability and Financial Conditions*. Federal Reserve Bank of New York, 2023. URL: https://www.newyorkfed.org/medialibrary/media/research/staff_reports/sr1022.pdf (vid. págs. 10, 14-16).

[13] *Top Automated Network Asset Discovery Tools and Their Benefits*. Device Authority. n.d. URL: https://deviceauthority.com/top-automated-network-asset-discovery-tools-their-benefits (vid. págs. 11, 12).

[14] *Vulnerability Management (InsightVM)*. Palo Alto Networks. n.d. URL: https://docs.rapid7.com/insightvm/ (vid. pág. 11).

[15] *Qualys Global AssetView CyberSecurity Asset Management Quick Start Guide*. Qualys. 2022. URL: https://cdn2.qualys.com/docs/qualys-gav-csam-quick-start-guide.pdf (vid. pág. 11).

[16] *Microsoft Defender for Cloud documentation - Protect network resources*. Microsoft. 2025. URL: https://learn.microsoft.com/en-us/azure/defender-for-cloud/protect-network-resources (vid. pág. 11).

[17] *What Is AWS Config?* Amazon Web Services (AWS). n.d. URL: https://docs.aws.amazon.com/config/latest/developerguide/WhatIsConfig.html (vid. pág. 11).

[18] *Get Started with Cloud Agent*. Qualys. n.d. URL: https://docs.qualys.com/en/ca/portal/latest/agents/manage_agents.htm (vid. pág. 11).

[19] *Microsoft Intune securely manages identities, manages apps, and manages devices*. Microsoft. 2025. URL: https://learn.microsoft.com/en-us/intune/intune-service/fundamentals/what-is-intune (vid. pág. 11).

[20] Christina Minihan y Andreano Lanusse. *Introduction to Workspace ONE UEM device management modes*. VMware by Broadcom. 2022. URL: https://blogs.vmware.com/euc/2022/10/introduction-to-workspace-one-uem-device-management-modes.html (vid. pág. 11).

[21] Max Aulakh. *FIPS 199 and 200 Compliance: Comparing Security Standards*. Ignyte. 2024. URL: https://www.ignyteplatform.com/blog/compliance/fips-199-200-compliance/ (vid. pág. 14).

[22] Fabio Natalucci, Mahvash S. Qureshi y Felix Suntheim. *Rising Cyber Threats Pose Serious Concerns for Financial Stability*. International Monetary Fund (IMF). 2024. URL: https://www.imf.org/en/blogs/articles/2024/04/09/rising-cyber-threats-pose-serious-concerns-for-financial-stability (vid. pág. 15).

[23] *Common Vulnerability Scoring System version 4.0 Specification Document*. Forum

of Incident Response y Security Teams (FIRST). 2024. URL: https://www.first.org/cvss/v4-0/cvss-v40-specification.pdf (vid. págs. 15, 26).

[24] *BOD 22-01: Reducing the Significant Risk of Known Exploited Vulnerabilities*. U.S. Department of Homeland Security Cybersecurity e Infrastructure Security Agency (CISA). 2021. URL: https://www.cisa.gov/news-events/directives/bod-22-01-reducing-significant-risk-known-exploited-vulnerabilities (vid. págs. 16, 27).

[25] Judy Kelly. *Common Vulnerability Scoring System (CVSS) vs. Risk: Why are we still having this conversation?* Red Hat. 2025. URL: https://www.redhat.com/en/blog/common-vulnerability-scoring-system-cvss-vs-risk-why-are-we-still-having-conversation (vid. pág. 17).

[26] *Cyber Asset Attack Surface Management (CAASM)*. Rapid7. n.d. URL: https://www.rapid7.com/fundamentals/what-is-cyber-asset-attack-surface-management-caasm/ (vid. págs. 18, 19).

[27] David Bruce. *Guide to Cyber Asset Attack Surface Management (CAASM*. CrowdStrike. 2024. URL: https://www.crowdstrike.com/en-us/cybersecurity-101/exposure-management/cyber-asset-attack-surface-management-caasm/ (vid. pág. 18).

[28] *Axonius Platform Overview*. Axonius. 2025. URL: https://docs.axonius.com/docs/using-axonius-overview (vid. págs. 18, 19).

[29] *JupiterOne Documentation*. JupiterOne. n.d. URL: https://docs.jupiterone.io/ (vid. pág. 18).

[30] Jennie Duong. *The Ultimate CAASM Guide for 2022*. JupiterOne. 2022. URL: https://www.jupiterone.com/blog/the-ultimate-caasm-guide-2022 (vid. págs. 18, 19).

[31] *Cyber Asset Attack Surface Management (CAASM) Reviews and Ratings*. Gartner. n.d. URL: https://www.gartner.com/reviews/market/cyber-asset-attack-surface-management (vid. pág. 19).

[32] *12 popular vulnerability scanning tools in 2025*. Red Canary. 2025. URL: https://redcanary.com/cybersecurity-101/security-operations/vulnerability-scanning-tools/ (vid. págs. 20, 21).

[33] Zbigniew Banach. *SAST vs. DAST vs. IAST: Everything you always wanted to know but were afraid to AST*. Invicti Security. 2023. URL: https://www.invicti.com/blog/web-security/sast-vs-dast-vs-iast-everything-you-always-wanted-to-know (vid. págs. 20, 21).

[34] *What is a Cloud-Native Application Protection Platform (CNAPP)?* Cloud Security Alliance. 2021. URL: https://cloudsecurityalliance.org/blog/2021/10/25/what-is-a-cloud-native-application-protection-platform-cnapp (vid. pág. 20).

[35] Swaroop Sham. *IaC Security: How to Ensure Infrastructure as Code Is Secure*. Wiz.

2024. URL: https://www.wiz.io/academy/iac-security (vid. pág. 20).
[36] Ofer Hakimi. *10 Vulnerability Scanning Tools to Know in 2025*. Pynt. 2025. URL: https://www.pynt.io/learning-hub/application-security/10-vulnerability-scanning-tools-to-know-in-2025 (vid. pág. 21).
[37] *Microsoft Defender External Attack Surface Management overview*. Microsoft. n.d. URL: https://learn.microsoft.com/en-us/azure/external-attack-surface-management/overview (vid. pág. 21).
[38] *Top 10 Vulnerability Management Best Practices for 2024*. Sprocket Security. 2024. URL: https://www.sprocketsecurity.com/blog/vulnerability-management-best-practices (vid. págs. 21, 31, 32, 36).
[39] Subhojit Roy. *Vulnerability Prioritization: The Complete Guide*. Ivanti. 2025. URL: https://www.ivanti.com/blog/vulnerability-prioritization-guide (vid. pág. 21).
[40] *Security Threat Intelligence Products and Services (Transitioning to Cyber Threat Intelligence Technologies) Reviews and Ratings*. Gartner. n.d. URL: https://www.gartner.com/reviews/market/security-threat-intelligence-products-and-services (vid. pág. 21).
[41] *AI in DevSecOps: Automating Security Vulnerability Detection*. Datahub Analytics. 2025. URL: https://datahubanalytics.com/ai-in-devsecops-automating-security-vulnerability-detection/ (vid. págs. 21, 33).
[42] *Security Orchestration and Automation Playbook*. Rapid7, 2019. URL: https://www.rapid7.com/globalassets/_pdfs/whitepaperguide/rapid7-insightconnect-automation-playbook.pdf (vid. págs. 22, 30).
[43] Terry Olaes. *What is Asset Inventory Management?* Balbix. 2025. URL: https://www.balbix.com/insights/what-is-asset-inventory-management/ (vid. págs. 22, 23, 32).
[44] Matthew Finio y Amanda Downie. *What is a managed security service provider (MSSP)?* IBM. n.d. URL: https://www.ibm.com/think/topics/managed-security-service-provider (vid. pág. 23).
[45] Elle Tsivka. *The Crucial Role of Business Impact Analysis (BIA) in Cyber Resilience*. Mitratech. 2025. URL: https://mitratech.com/es/centro-de-recursos/blog/the-crucial-role-of-business-impact-analysis-bia-in-cyber-resilience/ (vid. págs. 27, 28).
[46] *Vulnerability and Patch Management in Financial Institutions*. NETBankAudit. n.d. URL: https://www.netbankaudit.com/resources/vulnerability-patch-management-in-financial-institutions (vid. págs. 27, 31, 34).
[47] *BOD 19-02: Vulnerability Remediation Requirements for Internet-Accessible Systems*. U.S. Department of Homeland Security Cybersecurity e Infrastructure Security Agency (CISA). 2019. URL: https://www.cisa.gov/news-events/directives/bod-19-02-vulnerability-remediation-requirements-internet-acc

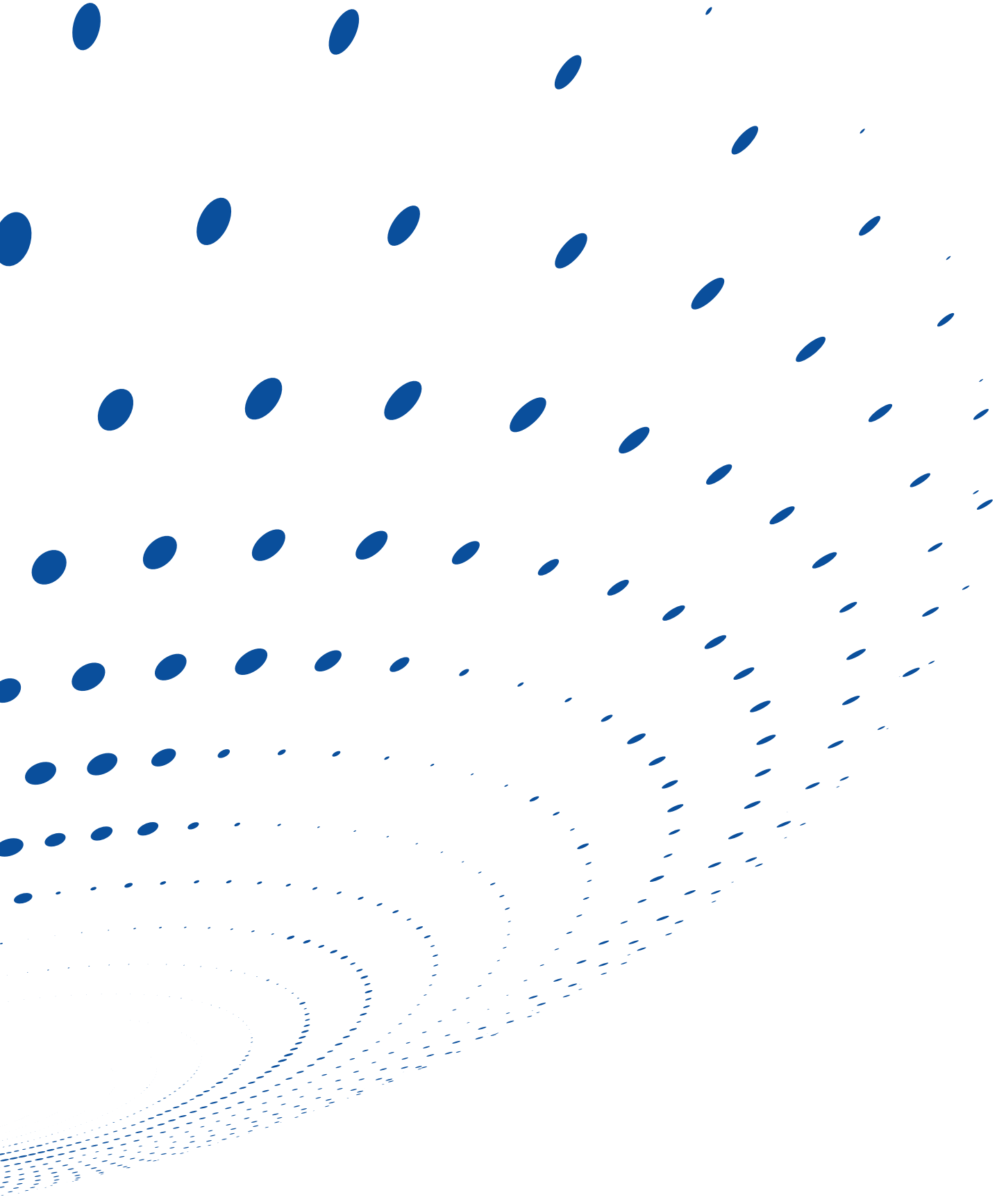
essible-systems (vid. pág. 27).
[48] *Article 10 Vulnerability and patch management*. Springflod AB. 2024. URL: https://www.springlex.eu/en/packages/dora/rts-rmf-regulation/article-10/ (vid. pág. 28).
[49] *SOAR Platforms: Key Features and 10 Solutions to Know in 2025*. Exabeam. n.d. URL: https://www.exabeam.com/explainers/soar/soar-platforms-key-features-and-10-solutions-to-know/ (vid. pág. 30).
[50] *Microsegmentation: The Key to Modern Cybersecurity*. Illumio. n.d. URL: https://www.illumio.com/cybersecurity-101/microsegmentation (vid. pág. 31).
[51] Devasmita Das. *Do Legacy Applications or Operating Systems Cause Gaps in Your Vulnerability Management Strategy? Microsegmentation Can Help*. ColorTokens. 2024. URL: https://colortokens.com/blogs/do-legacy-applications-or-operating-systems-cause-gaps-in-your-vulnerability-management-strategy-microsegmentation-can-help/ (vid. pág. 31).
[52] *Illumio App for ServiceNow*. Illumio. n.d. URL: https://www.illumio.com/es-mx/resource-center/illumio-app-for-servicenow (vid. pág. 31).
[53] *What is Break-Glass Access?* SSH. n.d. URL: https://www.ssh.com/academy/what-is-break-glass-access (vid. pág. 31).
[54] Phil Godfrey. *Managed Patch Management*. Park Place Technologies. 2025. URL: https://www.parkplacetechnologies.com/blog/managed-patch-management-best-practices-why-msps-smart-choice/ (vid. págs. 33, 34, 36).
[55] Murugiah Souppaya y Karen Scarfone. *NIST SP 800-40 Rev. 4 Guide to Enterprise Patch Management Planning: Preventive Maintenance for Technology*. National Institute of Standards y Technology (NIST), 2022. URL: https://csrc.nist.gov/pubs/sp/800/40/r4/final (vid. pág. 34).
[56] *Blue/Green Deployments on AWS*. Amazon Web Services. 2021. URL: https://docs.aws.amazon.com/whitepapers/latest/blue-green-deployments/welcome.html (vid. pág. 34).
[57] Shubham Jha. *What is Vulnerability Management? Compliance, Challenges, and Solutions*. Strobes. 2024. URL: https://strobes.co/blog/what-is-vulnerability-management-compliance-challenges-solutions/ (vid. págs. 36, 37).
[58] *Top 5 Vulnerability Management Challenges and How to Overcome Them*. ManageEngine. n.d. URL: https://www.manageengine.com/vulnerability-management/vulnerability-management-challenges.html (vid. pág. 37).
[59] *Root Cause Analysis*. proofpoint. n.d. URL: https://www.proofpoint.com/au/threat-reference/root-cause-analysis-rca (vid. págs. 37-39, 43).
[60] 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. 39,

40, 42).

[61] *Cybersecurity Incident and Vulnerability Response Playbooks*. U.S. Department of Homeland Security Cybersecurity e Infrastructure Security Agency (CISA), 2021. URL: https://www.cisa.gov/sites/default/files/2024-08/Federal_Government_Cybersecurity_Incident_and_Vulnerability_Response_Playbooks_508C.pdf (vid. págs. 42, 43).

[62] Reza Fayyazi, Stella Hoyos Trueba, Michael Zuzak y Shanchieh Jay Yang. «ProveRAG: Provenance-Driven Vulnerability Analysis with Automated Retrieval-Augmented LLMs». En: (2025). arXiv: 2410.17406 [cs.CR]. URL: https://arxiv.org/abs/2410.17406 (vid. págs. 44, 45).

[63] European Data Protection Board. *Training curriculum on AI and data protection Fundamentals of Secure AI Systems with Personal Data*. UNIDIR, 2025. URL: https://www.edpb.europa.eu/system/files/2025-06/spe-training-on-ai-and-data-protection-technical_en.pdf (vid. págs. 45, 46).



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