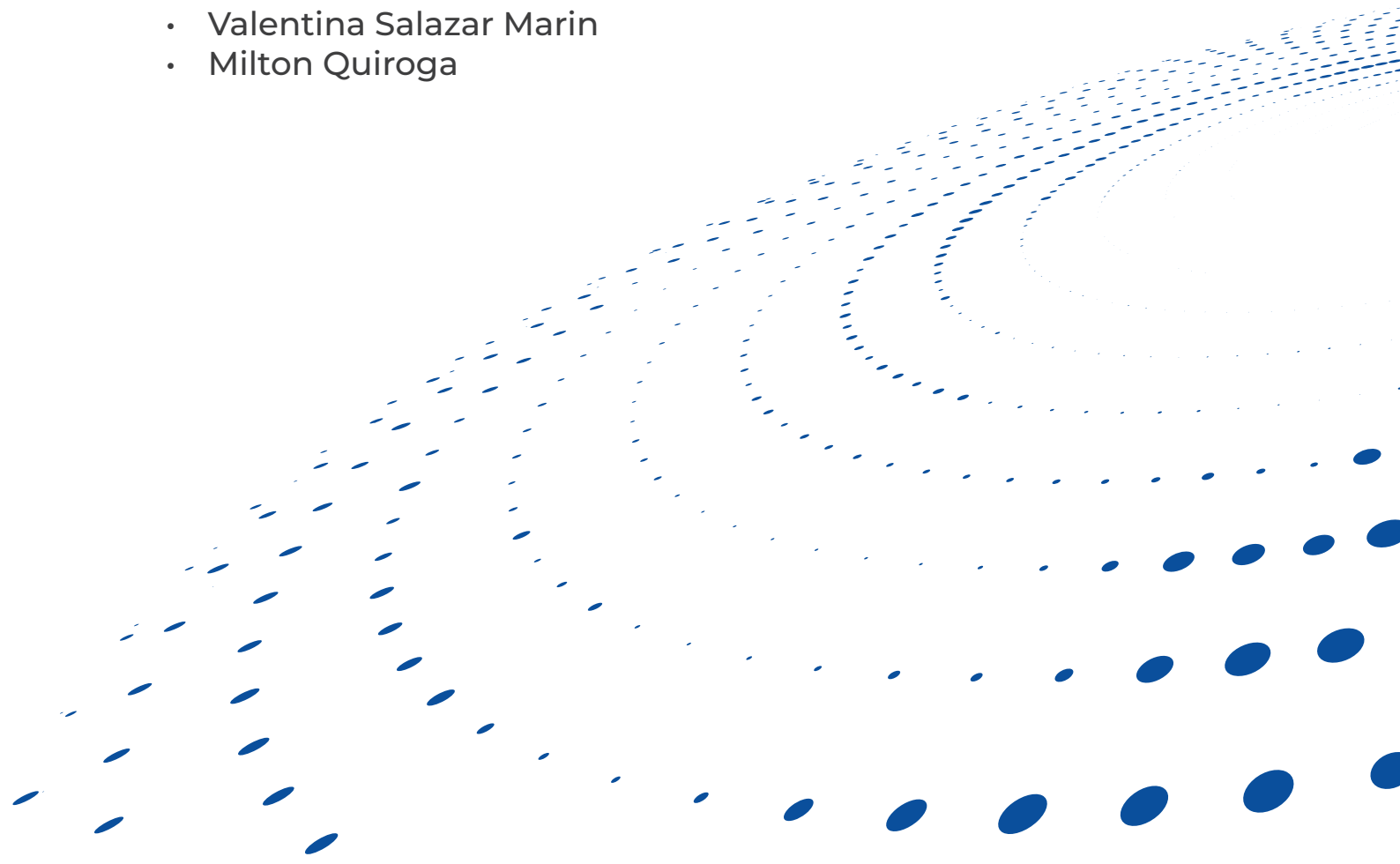
FLAR
FONDO LATINOAMERICANO DE RESERVAS

Computación en la nube: del diagnóstico al despliegue seguro

Gobernanza, controles y hoja de ruta para arquitecturas híbridas resilientes

Autores:

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



Índice general

Índice de tablas

Introducción

En un panorama donde la inclusión de capacidades en la nube crece con celeridad en el sistema financiero, los bancos centrales requieren un compendio que armonice salvaguardas de seguridad, resiliencia operativa y observancia regulatoria, sin menoscabar la agilidad inherente a entornos bajo demanda. El presente documento constituye una guía técnica y estratégica para que cada institución examine su nivel de madurez, refine políticas internas, despliegue controles de forma escalonada y consolide un ciclo de aprendizaje compartido.

Los objetivos se articulan en tres planos. En primera instancia, se proporciona un marco coherente de gobierno para ecosistemas en la nube, enlazando los estándares de referencia más aceptados con las exigencias normativas propias del sector. En segundo término, se detallan lineamientos prácticos para la incorporación segura de modelos IaaS, PaaS y SaaS, abarcando procesos de migración e integración, delimitación de responsabilidades y despliegue de controles especializados. Finalmente, se traza un itinerario de progreso sostenido que contemple métricas de eficacia e indicadores de riesgo, de tal manera que el avance pueda cuantificarse y supervisarse.

La obra se organiza en seis capítulos complementarios. El Capítulo 1 aborda gobernanza, riesgo y cumplimiento, con énfasis en órganos decisorios y criterios de debida diligencia para proveedores de servicios en la nube . El Capítulo 2 desarrolla rutas de adopción amparadas en modelos de servicio (IaaS/PaaS/SaaS) y en el modelo de responsabilidad compartida, precisando fronteras de mando entre el cliente y la plataforma. El Capítulo 3 examina la protección de datos y criptografía, profundizando en clasificación, soberanía/residencia, gobierno de llaves y mecanismos avanzados —desde cifrado homomórfico hasta preparación poscuántica. El Capítulo 4 sistematiza controles por dominios críticos y prácticas DevSecOps, con foco en microsegmentación, confianza cero y CI/CD. El Capítulo 5 desarrolla la respuesta a incidentes y la robustez operacional, abarcando telemetría centralizada, análisis forense y planes de recuperación con objetivos RTO/RPO verificables. El Capítulo 6 propone fases de implementación y un cuadro de KPI/KRI para orientar las inversiones y priorizar los cierres. En conjunto, el documento ofrece una brújula para que cada banco central avance hacia entornos de nube robustos, auditables y alineados con directrices internacionales.

1 Gobernanza, riesgo y cumplimiento para la nube

El presente capítulo articula los pilares esenciales para la gobernanza de ciberseguridad, la gestión integral de riesgos y la observancia normativa en despliegues sobre la nube, aspectos de vital importancia para mantener la operación de los bancos centrales en su rol de clientes (*Cloud Service Customer*, CSC) y en su interacción con el proveedor del servicio (*Cloud Service Provider*, CSP). Su finalidad es ofrecer un marco coherente que oriente la toma de decisiones estratégicas, refuerce la resiliencia operativa y preserve la confianza del público en la estabilidad financiera.

1.1 Marcos de referencia

Un análisis comparativo de los marcos de ciberseguridad líderes —NIST SP 800-61, CSA Cloud Incident Response Framework (CIRF) y MITRE ATT&CK for Cloud— es esencial para que los bancos centrales seleccionen y adapten los controles, métricas y procedimientos que se alineen con su apetito de riesgo, su arquitectura tecnológica y las exigencias de sus organismos supervisores. A grandes rasgos,

- **NIST SP 800-61 Rev. 3 (*Incident Response Recommendations and Considerations for Cybersecurity Risk Management*)**: Esta publicación, armonizada con el Cybersecurity Framework (CSF) 2.0, trasciende la mera reacción ante eventos y promueve un ciclo continuo de anticipación, detección, contención, recuperación y mejora. El documento enfatiza la integración vertical de la respuesta a incidentes dentro de la gestión corporativa del riesgo: los indicadores de impacto, los planes de continuidad y los presupuestos de ciberseguridad se interrelacionan para facilitar decisiones sustentadas en datos [1]. Asimismo, recomienda desplegar registros granulares, monitoreo en tiempo real y capacidades forenses, tanto en cargas locales como en nubes públicas, con el fin de acortar el tiempo medio de detección y minimizar la superficie vulnerable [1]. Para un banco central, lo anterior implica que la respuesta ante ciberincidentes se eleve a un nivel estratégico,

involucrando a la alta dirección, a los comités de auditoría y a los departamentos jurídicos, de modo que cualquier incidente sea tratado como un riesgo sistémico capaz de afectar la estabilidad macroeconómica.

- **CSA Cloud Incident Response Framework (CIRF)**: El CIRF presenta una visión esquematizada y articulada de los principales enfoques empleados para abordar incidentes en entornos de computación en la nube. Describe de forma clara las causas más frecuentes de disrupciones —tanto aquellas asociadas a la seguridad informática como las derivadas de otras fuentes— y propone esquemas de contención y mitigación acordes con su origen [2]. Este marco conceptual se construye a partir de referentes consolidados, entre ellos el NIST SP 800-61, la norma ISO/IEC 27035-1:2016 y la evaluación de riesgos publicada por ENISA sobre despliegues en la nube [3]. Su estructura metodológica se articula en cinco etapas secuenciales: preparación; detección y análisis; contención, erradicación y recuperación; revisión posincidente; y una fase transversal de coordinación e intercambio de información [2].

  El esquema del CIRF destaca por su amplitud temática, al incluir incidentes provocados por intenciones no maliciosas —como fallos de infraestructura, caídas de sistemas, desastres naturales o errores humanos— junto con ataques deliberados, como denegación de servicios distribuidos (DDoS) o campañas de ingeniería social [2]. Tal espectro resulta especialmente relevante para los bancos centrales, dado que la continuidad de funciones financieras esenciales puede verse afectada por un abanico de eventos mucho más extenso que los ciberataques convencionales. Desde esta óptica, el concepto tradicional de seguridad evoluciona hacia una estrategia centrada en la resiliencia operacional de todo el ecosistema tecnológico.

  El CIRF subraya la necesidad de establecer canales de comunicación entre proveedores y usuarios, contemplando actualizaciones periódicas y flujos formales de intercambio de información sobre incidentes con otras organizaciones a fin de protegerse contra amenazas similares [2]. Esta recomendación responde directamente al modelo de responsabilidad compartida que caracteriza a los entornos de nube. En consecuencia, una respuesta oportuna y coordinada por parte de un banco central requiere acuerdos sólidos con el CSP, cláusulas contractuales explícitas, procedimientos de notificación predefinidos y ejercicios conjuntos que comprueben distintos escenarios de disrupción.

- **MITRE ATT&CK for Cloud**: Es un subconjunto de la matriz *ATT&CK for Enterprise*, que se centra en el comportamiento de los adversarios en entornos de nube y clasifica las tácticas (objetivos del adversario) y las técnicas (medios para lograr esos objetivos), proporcionando una taxonomía común para la ciberseguridad ofensiva y defensiva [4]. El propio marco subraya que los métodos empleados en

un ataque a la nube no replican aquellos aplicados a entornos empresariales tradicionales; en su lugar, con frecuencia, los adversarios aprovechan las características nativas del proveedor para alcanzar sus fines [4]. Esta observación adquiere implicaciones significativas para los bancos centrales: las herramientas heredadas de seguridad perimetral o las arquitecturas *on-premise* clásicas resultan, por sí solas, insuficientes frente al modelo de amenaza en nube. Por ende, se vuelve imperativo instalar dispositivos de monitoreo orientados a configuraciones, API, flujos de identidad y dependencias propias del entorno de cada CSP.

Más allá de su función descriptiva, el marco ATT&CK for Cloud posee aplicaciones concretas en múltiples disciplinas: detección de intrusiones, cacería de amenazas, ingeniería defensiva, *red teaming*, análisis de inteligencia y ponderación de riesgos [4]. Al mapear las técnicas adversarias, las organizaciones pueden localizar con precisión los puntos ciegos en las defensas y protecciones instaladas, caracterizar sus áreas de exposición, evidenciar parametrizaciones frágiles o sin supervisión y encauzar inversiones de manera más eficaz. Para un banco central, esto habilita la simulación de escenarios realistas de ataque a la nube, el fortalecimiento de capacidades defensivas mediante ejercicios avanzados y una transición desde una seguridad centrada en el cumplimiento hacia una postura dinámica, resiliente y dirigida a la inteligencia contextualizada de amenazas.

Los bancos centrales enfrentan, por tanto, el desafío de fortalecer su estrategia de ciberdefensa mediante un enfoque escalonado que articule marcos complementarios. La combinación adecuada de los referentes descritos no solo incrementa el potencial de las acciones correctivas o preventivas, sino que además compagina los procesos de defensa con los objetivos institucionales de estabilidad, continuidad y gobernanza informada por el riesgo. A continuación, se listan algunas recomendaciones claras y accionables para acoger los componentes más relevantes de cada documento:

- **NIST SP 800-61 Rev. 3**: Conlleva integrar la respuesta a incidentes dentro del ecosistema más amplio de la gestión de riesgo empresarial (*Enterprise Risk Management*, ERM), efectuando una correlación explícita con el apetito de riesgo institucional. Este encaje exige que las acciones de respuesta no se limiten a lo técnico y operativo, sino que se inscriban en las prioridades del negocio. Además, resulta indispensable utilizar mecanismos de revisión posincidente que retroalimenten las decisiones tácticas, sirvan como base para rediseñar políticas de seguridad y se incorporen sistemáticamente en los procesos de formación del personal y en las renovaciones tecnológicas [5].
- **CSA CIRF**: Se deben elaborar planes de respuesta a incidentes (IRP) dirigidos a escenarios de nube, abarcando tanto eventos cibernéticos como factores no intencionales [2]. Tales planes deben formalizar esquemas de comunicación previamente definidos con los CSP, incluyendo roles, tiempos de respuesta y canales

de escalamiento. La efectividad de dichos protocolos depende, en buena medida, de su validación a través de simulacros frecuentes, así como del aprovechamiento coordinado de las funcionalidades nativas de continuidad y restauración que ofrecen los CSP [2].

- **MITRE ATT&CK for Cloud**: Aporta una base rigurosa para llevar a cabo una inteligencia de amenazas contextualizada. Su adopción implica centrar la atención en técnicas que explotan capacidades legítimas de la nube, lo que obliga a redefinir las prioridades defensivas más allá del perímetro tradicional. Para ello, se recomienda conducir evaluaciones de brechas que revelen deficiencias en la cobertura de monitoreo o carencias en el levantamiento de barreras de contención clave. Además, la integración de la matriz ATT&CK en soluciones como SIEM y EDR contribuye a enriquecer la correlación de eventos y la detección proactiva [4]. Adicionalmente, emerge la necesidad de aplicar medidas concretas frente a técnicas como la manipulación de políticas de acceso condicional o el secuestro de servicios en la nube, las cuales representan vectores de ataque altamente eficaces si no se mitigan con anticipación [4].

1.2 Marco de gobernanza corporativa en la nube

El establecimiento de un esquema sólido de gobernanza corporativa es primordial para que los bancos centrales aborden eficazmente las implicaciones estratégicas, operativas y de seguridad de la transición a la nube. En términos de jerarquía, el marco que proporciona las directrices para las prácticas de ciberseguridad se posiciona en el nivel superior; a continuación, le siguen las políticas (descripción de los requisitos de seguridad), los objetivos de control (resultados deseados de los controles) y las especificaciones de control (lineamientos de implementación) [6]. Tales componentes serán abordados en las siguientes secciones.

1.2.1 Roles, responsabilidades y órganos decisorios

El primer pilar consiste en establecer un **organigrama** nítido, donde cada función —desde TI y operaciones hasta finanzas, seguridad y cumplimiento regulatorio— reconozca con precisión su ámbito de actuación, autoridad y responsabilidad [7]. El *Cloud Adoption Framework* de AWS, por ejemplo, aconseja plasmar dicho reparto de obligaciones mediante matrices RACI («Responsable», «Aprobador», «Consultado» e «Informado») que consignen quién responde, quién ejecuta, quién consulta y quién recibe información [8]. Independiente del modelo de servicio contratado (IaaS, PaaS o SaaS), la entidad

financiera conserva la tutela última sobre la confidencialidad y solidez de la información sensible de sus clientes [9]. La Tabla 1.1 delimita, capa por capa, la participación de cada actor en un despliegue de nube genérico. Dependiendo del nivel de servicio adquirido, este recurso debe ser refinado y ampliado.

Tabla 1.1: Matriz RACI para actividades de gestión de arquitecturas en la nube.

Actividad	CSP	Comité *cloud*	SOC	Área de infraestructura y operaciones tecnológicas	Propietario de la aplicación o dominio de negocio	Oficina de Riesgo y Cumplimiento	Audito-ría interna
Hardware físico y energía	R	I	I	I	–	I	C
***Firmware* y proceso de arranque**	R	I	C	I	–	I	C
Hipervisor y aislamiento de *tenants*	R	I	C	I	–	I	C
Red troncal, balanceo y defensa DDoS	R	C	C	I	–	I	C
Segmentación virtual y filtros	C	C	R	A	–	I	I
Almacenamiento con cifrado en reposo	C	C	R	A	–	I	I
Sistema operativo invitado y parches	–	I	C	R / A	–	I	C
Administración de identidades	–	A	R	C	–	C	I
Supervisión, telemetría y alertas	C	I	R / A	C	–	I	C
Bitácoras y retención	C	C	R	A	–	C	I

Clasificación de información	–	C	C	C	R / A	C	I
Configuración de la aplicación	–	I	C	C	R / A	C	I
Respuesta ante incidentes	C	C	R	A	–	C	I
Continuidad y restauración	C	C	R	A	–	C	I
Revisión de cumplimiento	C	I	C	I	–	R / A	C

El segundo pilar es la **adaptabilidad**. La gobernanza de la nube se concibe como un esfuerzo continuo, en permanente sintonía con los requerimientos del negocio y el cambiante panorama de amenazas [8]. En consecuencia, los procedimientos y los instrumentos de ciberdefensa deben someterse a revisiones periódicas que aborden avances tecnológicos, lecciones aprendidas tras incidentes y nuevas normativas, al tiempo que promueven la formación permanente del personal [10].

El éxito de la gobernanza de la nube depende del **patrocinio ejecutivo**. Cuando los niveles más altos de liderazgo —CIO, CTO, CFO, CISO y CRO— otorgan legitimidad y respaldo explícito al equipo de gobierno de la nube [7], se robustece la alineación con los objetivos macroeconómicos de la institución y se dispone de un canal formal para resolver tensiones interdepartamentales. Para los bancos centrales, esto significa que la seguridad en la nube no es únicamente una preocupación de un área, sino un imperativo estratégico que requiere la participación y el compromiso transversal [7]. Una gobernanza eficaz exige la colaboración permanente entre todos los departamentos, incluidas las áreas jurídicas y de negocio, para asegurar que las políticas minimicen el riesgo sin obstaculizar la innovación [7].

1.2.2 Políticas institucionales para adopción y uso de servicios

Las directrices internas respecto al despliegue en la nube representan un componente cardinal de la gobernanza tecnológica en los bancos centrales [11], dado que orquestan la convergencia entre parámetros normativos, salvaguardas criptográficas e instrumentos de auditoría [10]. Tales lineamientos deben contemplar, entre otras disposiciones, protección extremo a extremo de la información sensible; bitácoras inmutables que documenten cada transacción relevante; y esquemas de control de acceso o consulta basados en privilegio mínimo, autenticación multifactor (MFA) y revisiones periódicas de permisos [11]. Dicho nivel de detalle sustenta la trazabilidad y confiere a los órganos de supervisión plena confianza en la custodia de los activos de información.

La incorporación de herramientas de inspección continua introduce, además, un paradigma orientado a «política como código». En esta modalidad, las reglas corporativas se expresan por medio de artefactos declarativos que los motores de cumplimiento examinan de forma permanente en el ecosistema de nube [11]. De este modo, se obtiene comprobación constante de la postura de seguridad, superando la perspectiva de auditoría puntual y reduciendo el esfuerzo manual requerido en las verificaciones de cumplimiento [8]. Al codificar tanto restricciones como umbrales de alerta, la institución gana inmediatez para detectar desviaciones y aplicar correcciones antes de que deriven en una exposición significativa.

Por último, las políticas deben reflejar un planteamiento centrado en los datos. Esto im-

plica clasificar la información financiera según la criticidad, aplicar las defensas acordes al nivel de sensibilidad y respetar las exigencias de soberanía, independientemente de la ubicación física del recurso [11]. Así, el banco central refuerza la confidencialidad y minimiza los riesgos regulatorios, manteniendo coherencia entre marcos normativos y prácticas operativas.

1.3 Evaluación formal de proveedores de servicios en la nube (CSP)

El estudio de los prestadores de servicios de computación remota constituye un pilar crítico para que un banco central mitigue la exposición a terceros, preserve la conformidad con los lineamientos vigentes y sostenga la resiliencia operativa. Este escrutinio abarca componentes jurídicos, técnicos y financieros, además de certificar el veredicto en revisiones independientes (auditorías externas, pruebas de penetración y evaluaciones de vulnerabilidad), en estudios sobre la efectividad de las acciones correctivas y en informes de cumplimiento de los acuerdos de nivel de servicio (SLA) [9]. Luego, los contratos deben definir claramente las responsabilidades para la configuración de los mecanismos de seguridad, los derechos de acceso, la administración de claves, la supervisión continua, la gestión de parches, las obligaciones de respuesta a incidentes (informes, comunicación y análisis forense), el uso de subcontratistas, la propiedad/-devolución de datos, las restricciones geográficas y la destrucción de la información al término de la relación comercial [9].

El Banco Central Europeo (BCE) advierte que la oferta de servicios remotos se concentra en un número reducido de corporaciones globales [12], lo que ocasiona un riesgo de dependencia y dificulta la sustitución inmediata en caso de disfunción. Frente a esta situación, el CSC necesita elaborar estrategias de salida sólidas, recurrir a arquitecturas multinube o híbridas6 y solicitar cláusulas que contemplen la portabilidad de datos, la interoperabilidad y los protocolos precisos para la eliminación de activos digitales [9]. Dichas disposiciones reducen el impacto de posibles fallas y contrarrestan el llamado *vendor lock-in*.

Documentos legales como DORA (*Digital Operational Resilience Act*) y CRD (*Capital Requirements Directive*) imponen a los bancos instaurar una gobernanza eficaz del riesgo derivado de la subcontratación [12]. Asimismo, el *Cloud Executive Steering Group* del Departamento del Tesoro de los Estados Unidos alude a problemas y consideraciones de subcontratación en la nube, enfatizando la necesidad de transparencia, las potenciales deficiencias en los recursos aprovisionados, las dificultades en la resolución de incidentes operativos y la delicada dinámica de negociación de contratos [13]. En con-

secuencia, la evaluación de los prestadores no puede concebirse como un evento puntual, sino que debe evolucionar conforme lo hagan los mandatos regulatorios [12] y fomentar el intercambio de información entre supervisores y entidades [13], de modo que el panorama de riesgos compartidos se mantenga siempre actualizado.

En concordancia con lo anterior, la Tabla 1.2 desglosa y organiza los criterios a tener en cuenta, los cuales se aplican en dos planos que se complementan bajo el modelo de responsabilidad compartida: al entorno interno del proveedor (controles que el CSP diseña y opera en su plataforma); y a la configuración del cliente sobre su propia arquitectura en la nube (controles que el CSC puede consumir, ajustar y administrar con las capacidades expuestas por el CSP).

Además, existe un tercer eje contractual que depende de si es factible pactar compromisos legales, auditoría y salidas.

Tabla 1.2. Criterios para la evaluación formal de proveedores de servicios en la nube.

Categoría	Aspectos	Detalles/ejemplos
Legal y contractual	Responsabilidades contractuales	Definición clara de roles en configuración, acceso, gestión de claves y monitoreo de seguridad.
	Obligaciones de respuesta a incidentes	Reporte, comunicación, análisis forense y uso de subcontratistas.
	Propiedad y retorno de datos	Delimitación de la propiedad de datos, expectativas de eliminación y retorno al finalizar contrato.
	Restricciones geográficas	Especificación de ubicaciones geográficas donde residen los datos.
Seguridad técnica	Configuración y aprovisionamiento	Uso de herramientas para configurar sistemas de forma segura y aprovisionamiento de acceso.
	IAM y salvaguardas de red	Principio de mínimo privilegio, MFA, revisión de acceso, VPN, WAF e IDS.
	Controles de datos sensibles	Cifrado, tokenización, DLP y administración del ciclo de vida de las claves de cifrado.
	Seguridad de microservicios/contenedores	Evaluación de las opciones de implementación y gestión de la superficie de ataque.

Continúa en la página siguiente

Tabla 1.2. Criterios para la evaluación formal de proveedores de servicios en la nube. (Continuación)

Certificaciones y garantías	Debida diligencia y supervisión continua	Evaluación de informes de auditoría independientes y pruebas de penetración.
	Informes de cumplimiento de SLA	Revisión de reportes de cumplimiento.
Cumplimiento normativo	Adherencia a marcos regulatorios	Conformidad con FFIEC, DORA, CRD, estándares globales de seguridad de la información o lineamientos nacionales acerca del manejo de terceros.
	Responsabilidad general	La institución financiera mantiene la responsabilidad final por la seguridad y solidez.
Resiliencia operativa	Capacidades de resiliencia y recuperación	Evaluación de las capacidades de resiliencia del CSP y opciones de servicio.
	Planes de continuidad del negocio (BCP) y de recuperación ante desastres (DRP)	Diagnóstico del impacto de las operaciones en la nube y pruebas regulares de planes.

1.3.1 Transferencia de riesgo y pólizas de ciberseguridad

Las pólizas de ciberseguridad proporcionan un mecanismo robusto para la transferencia financiera del riesgo derivado de incidentes tecnológicos, robusteciendo así la resiliencia operativa de las organizaciones. Dichos instrumentos permiten mitigar las consecuencias económicas relacionadas con ciberataques, fugas o corrupción de información [14], ataques de extorsión digital y fallos imputables tanto al cliente como al proveedor del servicio en la nube. A diferencia de las pólizas convencionales, esta modalidad contempla explícitamente eventos asociados a infraestructuras gestionadas externamente, distinguiendo entre las responsabilidades del CSP y las del asegurado en concordancia con el modelo de servicio elegido (IaaS, PaaS y SaaS).

Entre las coberturas más destacadas en este ámbito se encuentra la denominada *Contingent Business Interruption* (CBI), que indemniza pérdidas operativas ocasionadas por la indisponibilidad o interrupción prolongada en las operaciones de un tercero clave [15], así como la cobertura paramétrica que facilita un pago automático y sin necesidad de evaluación pericial cuando se registran caídas en AWS, Azure o Google Cloud que

superan los umbrales contratados [16]. También existen cláusulas puntuales que protegen contra errores y omisiones cometidos por el CSP, indemnizando daños directos cuando las brechas tienen su origen en la negligencia o fallo operacional de este.

En paralelo, los principales proveedores de nube (AWS, Microsoft Azure y Google Cloud) han creado alianzas estratégicas con reconocidas aseguradoras, como Allianz Global, Munich Re, Chubb, Beazley y Marsh, desarrollando programas específicos que incentivan la mejora continua de la postura de ciberseguridad. Dichos programas emplean métricas técnicas obtenidas directamente de las consolas de gestión, como *AWS Security Hub* [17] o *Google Cloud Risk Manager* [18], para evaluar la madurez en seguridad del cliente y determinar condiciones ventajosas en los contratos aseguradores.

Al contratar una póliza de esta naturaleza, resulta imperativo considerar ciertos aspectos críticos, como la sincronización entre los SLA pactados con el CSP y las disposiciones fijadas por la aseguradora, incluyendo la deducción de créditos compensatorios otorgados por fallas del proveedor. Asimismo, conviene revisar con atención las exclusiones habituales relativas a errores de configuración imputables al cliente, solicitar cláusulas claras sobre la disponibilidad inmediata de registros forenses por parte del proveedor y asegurar que los términos de notificación temprana sean compatibles con las exigencias contractuales.

2 Adopción segura y modelos de servicio: IaaS, PaaS y SaaS

Este capítulo explora las consideraciones estratégicas para que los bancos centrales adquieran servicios en la nube, incluyendo la comprensión de los beneficios y costos, la navegación de las vías de migración, la seguridad de los entornos híbridos y la clarificación de las responsabilidades bajo el modelo compartido.

2.1 Claves del paradigma cloud y sus implicaciones

Entre las ventajas señaladas por la literatura especializada, figuran una orquestación más eficiente de los procesos interdepartamentales, menores inversiones operativas gracias al modelo de pago por uso y a la reducción en la infraestructura física, refuerzo de la protección de datos mediante criptografía administrada por el proveedor, obtención de indicadores sobre tendencias del mercado, mejor experiencia para el usuario final a través de plataformas web o móviles y, en último término, diferenciación competitiva por la rapidez en la puesta en marcha de nuevos productos [10]. Algunos informes estiman reducciones cercanas al 20 % en el gasto de TI y un incremento aproximado del 30 % en la agilidad [19].

No obstante, el *Azure Well-Architected Framework* advierte que optimizar costos no equivale a minimizarlos, sino a conciliarlos con factores críticos como solidez, escalabilidad y continuidad [20]. En ese sentido, priorizar exclusivamente el ahorro podría traducirse en brechas inaceptables de seguridad o resiliencia. El verdadero objetivo consiste en equilibrar el presupuesto con inversiones iniciales en controles robustos que preserven la confiabilidad del ecosistema digital [20], pero sin sacrificar la flexibilidad presupuestaria a largo plazo.

La computación en la nube, además, se erige como catalizador de la banca contemporánea al habilitar herramientas de inteligencia artificial y aprendizaje automático (*Machine Learning*, ML) proporcionadas por los grandes proveedores [10]. Las soluciones

de nube híbridas también ofrecen motores cognitivos capaces de examinar transacciones en tiempo real y señalar patrones anómalos [21]. Para un banco central, tales funcionalidades significan ir más allá de la mera modernización de infraestructura: aportan soporte para la supervisión regulatoria, la detección temprana de fraudes y la entrega de servicios digitales. Sin embargo, este salto tecnológico incorpora retos adicionales relacionados con la custodia de los datos que alimentan los modelos y la veracidad de los resultados algorítmicos.

2.2 Rutas de migración y efectos en la seguridad

La estrategia de migración a entornos de nube constituye una decisión crucial que condiciona la postura de seguridad, la resiliencia operativa y la rentabilidad futura de un banco central. Elegir el enfoque correcto exige ponderar con rigor las características de cada aplicación, su nivel de criticidad y los requisitos de cumplimiento normativo que la rodean. A continuación, se describen modalidades comunes [22]:

- **Reubicación (*lift-and-shift*)**: Traslada las aplicaciones sin alteraciones significativas. Este enfoque posibilita una migración rápida y un desembolso inicial moderado; sin embargo, tiende a obstaculizar la escalabilidad a mediano plazo [19] y mantiene intactos los mecanismos de identidad, seguridad y cumplimiento ya existentes, de modo que la deuda técnica —especialmente la relativa a la protección— permanece sin depurar.
- **Replataformización (*lift, tinker and shift*)**: Introduce ajustes mínimos en el código y actualiza el sistema operativo subyacente. Su objetivo consiste en aprovechar parte de las ventajas nativas de la nube —como autoservicio, elasticidad automática o facturación granular— sin incurrir en el esfuerzo considerable que implica una refactorización completa.
- **Refactorización**: Implica mejorar el código existente para potenciar los atributos no funcionales y la estructura de los componentes, con cambios en la pila tecnológica. Aunque demanda mayor dedicación de recursos y tiempo, desbloquea el potencial de escalabilidad, rendimiento y optimización de costos [19]. Además, mejora las características de seguridad, cumplimiento y gobernanza.
- **Reconstrucción**: Arranca de cero con un diseño modernizado, integra microservicios, contenedores y arquitecturas *serverless*, asumiendo planes avanzados de gobernanza y defensa. Esta ruta maximiza la resiliencia y el cumplimiento, pero implica la inversión más considerable de todas.

Para un banco central, el atractivo temporal de una migración acelerada pierde relevancia frente a la obligación de resguardar datos altamente sensibles y conservar, sin inte-

rrupciones, el funcionamiento de procesos financieros fundamentales para la estabilidad sistémica. Así, aun cuando la reubicación pueda funcionar como fase transitoria, la refactorización o la reconstrucción ofrecen beneficios perdurables al reforzar la protección de los datos, optimizar la elasticidad y facilitar el alineamiento con normativas progresivamente más estrictas. La decisión debe calibrarse de acuerdo con la sensibilidad y criticidad de cada carga de trabajo, con la premisa de que una planificación apropiada, pese a su coste inicial, propicia un entorno más robusto y sostenible.

2.3 Seguridad en infraestructuras híbridas: integración y gobierno unificado

La arquitectura híbrida fusiona capacidades on-premise con recursos de nube privada y pública, otorgando una plataforma flexible donde la información estrictamente confidencial reside en instalaciones internas mientras los datos con menores restricciones regulatorias se alojan en infraestructuras elásticas externas [21]. Así, sus beneficios incluyen una gestión de identidades reforzada, reducción de la superficie expuesta mediante *zero trust* y restauración ágil de servicios [23].

Este modelo demanda una vigilancia unificada que abarque visibilidad, control de acceso, detección oportuna de amenazas, cumplimiento normativo y recuperación ante desastres [23]. Adicionalmente, en ecosistemas de esta naturaleza, un esquema de autenticación federada resulta primordial para aplicar de forma coherente el principio de privilegio mínimo sobre activos locales, plataformas privadas y servicios públicos. Sin una administración centralizada de cuentas, funciones y permisos, la asignación de credenciales se vuelve compleja y proclive a errores; esto amplía la superficie vulnerable y dificulta la conformidad con marcos regulatorios. El alcance de la identidad abarca, además, la conexión segura con aplicaciones SaaS y la protección de interfaces API, componentes que suelen intensificar la exposición [23].

Finalmente, un despliegue híbrido concede la posibilidad de mantener cargas sensibles en dominios vigilados, cumpliendo los mandatos de soberanía establecidos por GDPR, HIPAA, PCI-DSS o lineamientos locales, mientras se aprovechan la escalabilidad y la innovación disponibles en servicios públicos para entornos de prueba o procesos menos regulados. Tal combinación brinda a los bancos centrales una herramienta para equilibrar robustez regulatoria y modernización tecnológica, navegando con solvencia panoramas reglamentarios cada vez más exigentes sin sacrificar agilidad ni capacidad de expansión.

2.4 Modelo de responsabilidad compartida en IaaS, PaaS y SaaS

El modelo aclara que los CSP garantizan la seguridad de la nube (infraestructura física, capa de virtualización), mientras que los clientes son responsables de la seguridad en la nube (datos, aplicaciones, identidades y sistema operativo) [9]. Por ejemplo, Google Cloud expone la relación en las obligaciones cliente-proveedor mediante un modelo de estratificación profunda que desciende hasta el nivel de *firmware* y se extiende hasta la capa de contenidos. La Figura 2.1 revela cómo dicha asignación varía al transitar de una arquitectura local a servicios IaaS, PaaS y SaaS [2] [10] .

Tabla 2.1. Responsabilidad compartida en IaaS, PaaS y SaaS para bancos centrales

Modelo	**Responsabilidad del proveedor de la nube (seguridad de la nube)**	**Responsabilidad del banco central (seguridad en la nube)**	**Implicaciones clave**
IaaS	Instalaciones físicas, infraestructura de red, hardware y capa de virtualización.	Datos, aplicaciones, sistema operativo, configuración de red, IAM, cifrado, datos del lado del cliente, tráfico de red, configuración de la plataforma y máquinas virtuales.	Endurecimiento de imágenes base y SO; *logging* central; segmentación; KMS/HSM con control criptográfico; criterios de residencia de datos y salida contractual para cargas críticas; vigilancia del riesgo de concentración en un único CSP conforme a lineamientos prudenciales.
PaaS	Instalaciones físicas, infraestructura de red, hardware, capa de virtualización, sistema operativo y entorno de ejecución o*middleware*.	Datos, APIs, código, capas de acceso, IAM, cifrado, datos del lado del cliente, tráfico de red y configuración de la plataforma.	Control de credenciales de servicio y secretos en *pipelines*; cifrado lógico por defecto; pruebas de restauración para servicios administrados; debida diligencia sobre terceros TIC y cláusulas de auditoría, reporte de incidentes y terminación ordenada conforme a DORA/estándares supervisorios.

Continúa en la página siguiente

Tabla 2.1. Responsabilidad compartida en IaaS, PaaS y SaaS para bancos centrales (Continuación)

SaaS	Instalaciones físicas, infraestructura de red, hardware, capa de virtualización, sistema operativo, entorno de ejecución o *middleware* y aplicación.	Gestión de acceso de usuarios, seguridad de datos/cuentas, clasificación de datos, cifrado y datos del lado del cliente.	Enfoque en IAM federado y MFA; exportación/retorno de información en formatos abiertos; métricas de desempeño/alerta y derechos de inspección; atención a dependencias sistémicas y reportes periódicos del proveedor.

En general, se presentan las diferencias descritas a continuación [6] [10]:

- **IaaS (infraestructura como servicio)**: La entidad conserva la administración del sistema operativo, las aplicaciones, los datos y los parches, mientras que el proveedor administra la red física, los centros de datos y la virtualización.
- **PaaS (plataforma como servicio)**: El operador de nube hospeda la plataforma de ejecución y los componentes intermedios, quedando en manos del cliente el código, las interfaces de programación y la custodia de la información.
- **SaaS (software como servicio)**: La carga operativa se traslada casi por completo al prestador, de modo que la institución únicamente gobierna las credenciales y aplica criterios de confidencialidad y clasificación sobre los registros que allí residen.

Persiste, sin embargo, la falsa impresión de que el proveedor de la nube se ocupa de todo. No obstante, a medida que la organización se desplaza de IaaS hacia PaaS y finalmente a SaaS, la carga técnica se reduce, pero la atención se orienta con mayor fuerza hacia la gobernanza de la identidad y la coherencia de los datos. Mientras IaaS impone protecciones minuciosas al nivel del sistema operativo y del software desplegado, SaaS traslada la atención hacia la administración del ingreso de los usuarios, la clasificación de la información y la salvaguarda de su integridad dentro de la propia aplicación.

Lo anterior obliga a los equipos de protección a reorientar sus competencias: de una perspectiva centrada en la infraestructura deben pasar a otra focalizada en la identidad y en el tratamiento de la información, interiorizando los matices propios de cada modalidad de servicio junto con los instrumentos de ciberdefensa que les corresponden. Si bien el concepto de *shared fate* (destino compartido) promovido por Google introduce

valores predeterminados en los servicios de acuerdo con buenas prácticas de los usuarios [24], la vigilancia del cliente continúa siendo el factor determinante para mantener la confianza y la estabilidad operativa.

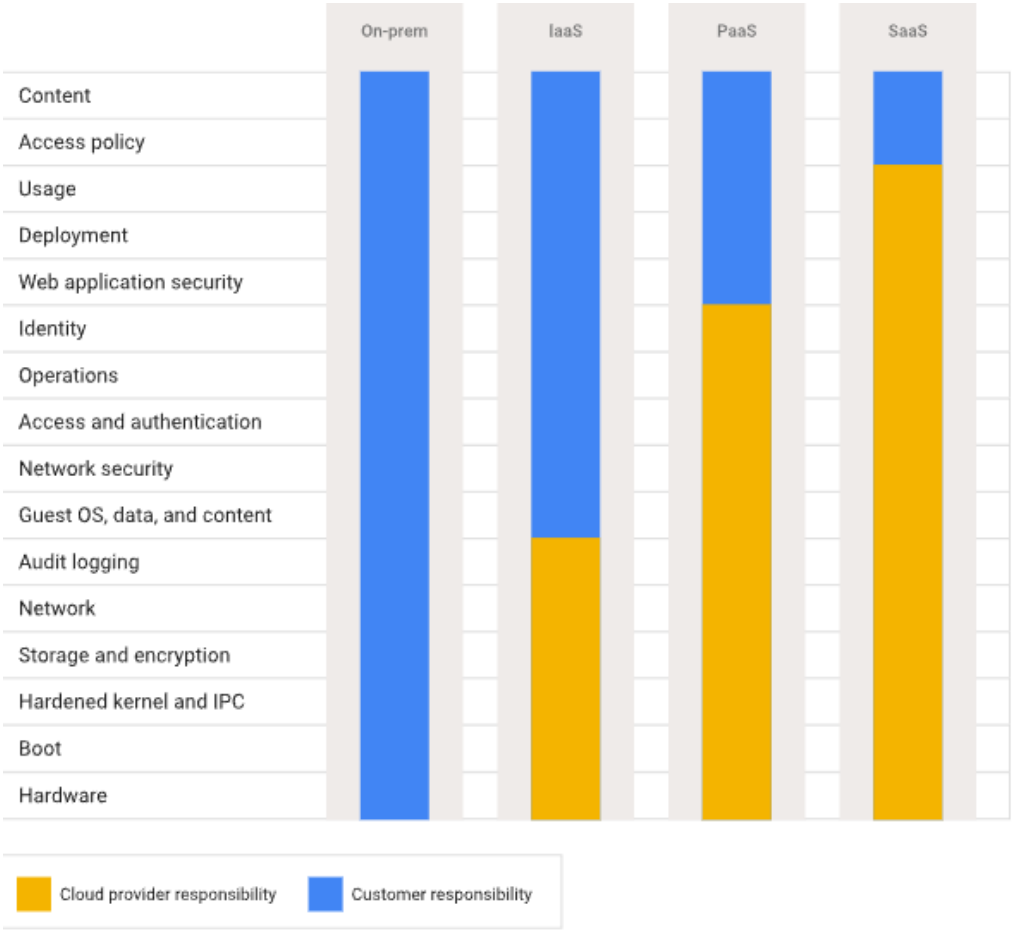


Figura 2.1: Distribución de responsabilidades en Google Cloud Platform. Fuente: *Responsabilidades compartidas y destino compartido en Google Cloud* [24].

3 Protección de datos y criptografía en la nube

3.1 Clasificación de datos sensibles

La gobernanza de la información en entornos de nube descansa sobre un pilar doble: catalogar cada activo digital conforme a su sensibilidad y dictar normas que rijan su tratamiento durante todo el ciclo de vida. Sin esa taxonomía previa, cualquier iniciativa orientada a protección o conservación se vuelve imprecisa y, por consiguiente, vulnerable a fisuras regulatorias.

El primer paso consiste en clasificar los registros de acuerdo con criterios predeterminados como confidencialidad, impacto en caso de divulgación y valor para la institución [25]. Así, la organización puede delimitar con precisión qué estrategias de contención aplicar en cada caso y cómo demostrar diligencia frente a las auditorías o revisiones por parte de terceros.

Una política de etiquetado rigurosa identifica primero los campos que contienen información personal, registros financieros, claves criptográficas o secretos industriales; a continuación, vincula instrumentos proporcionales (cifrado robusto, MFA, registro inmutable y períodos específicos de retención) con cada familia de activos [25]. De este modo, el banco central conoce en todo momento qué posee, dónde reside y bajo qué normativa se rige [26], lo que facilita la preparación de evidencias y reduce la superficie de exposición derivada del almacenamiento prolongado de recursos que ya no aportan valor operativo [27].

El dominio 9 de la guía de seguridad de la CSA [6] propone cuatro niveles:

Tabla 3.1. Clasificación de datos y activos por sensibilidad, criticidad e impacto por pérdida o compromiso.

Nivel	Descripción
Altamente confidencial	Contenido cuya divulgación provocaría impacto financiero elevado o riesgo sistémico.
Confidencial	Información que ocasionaría perjuicio moderado en caso de fuga.
Privado	Material de uso interno que provocaría inconvenientes menores si trasciende.
Público	Contenido divulgable sin consecuencias.

Este entramado no solo respalda condicionamientos como los prescritos por PCI DSS, GDPR, CCPA o las directrices regionales de soberanía [25] [27], sino que también habilita un gobierno preciso sobre la información monetaria, estadística y de políticas públicas. El resultado es una arquitectura documental coherente con los mandatos de transparencia, resiliencia y control que rigen al sector financiero [26], capaz de evolucionar al ritmo de la innovación tecnológica sin relegar la responsabilidad fiduciaria que la institución ostenta ante la sociedad.

3.2 Soberanía y residencia de datos

Conviene destacar que la visión de los prestadores de servicios tecnológicos basados en la nube respecto a la soberanía digital se articula en torno a tres pilares complementarios: **soberanía operacional, soberanía del software y soberanía del dato** [28] [29]. El primero se refiere a la capacidad de las organizaciones para conservar visibilidad y ejercer gobernanza sobre las operaciones realizadas por la entidad proveedora, incluso mediante verificaciones ejecutadas por terceros de confianza o mediante ecosistemas completamente aislados, como es el caso de *Google Distributed Cloud Hosted* para procesos altamente sensibles. El segundo componente busca garantizar que las instituciones puedan ejecutar sus cargas de trabajo sin depender de software propietario o componentes que introduzcan vínculos técnicos irreversibles con el proveedor. Por su parte, la soberanía del dato conlleva a mantener dominio absoluto sobre el acceso, el cifrado, la colocación y la custodia de las claves, diferenciando entre datos regulados y aquellos de naturaleza menos restrictiva.

Esta última representa una dimensión jurídica central en los ecosistemas de nube contemporáneos, especialmente para instituciones financieras sujetas a obligaciones transfronterizas. Este principio establece que cualquier contenido digital preservado en una

determinada jurisdicción queda sujeto a las leyes de ese país [30], independientemente del origen de la organización que lo maneja. A su vez, es necesario distinguir entre tres conceptos clave: la residencia de datos, que remite a la ubicación física de los sistemas de almacenamiento; la soberanía, que determina qué legislación rige sobre dichos datos; y la localización, entendida como la exigencia legal de conservar información dentro de fronteras nacionales [31].

Para los bancos centrales, tales distinciones trascienden lo teórico: constituyen requisitos operativos ineludibles que afectan la forma en que se diseñan las arquitecturas, se seleccionan regiones y se redactan cláusulas contractuales con proveedores de servicios tecnológicos. La coexistencia de marcos regulatorios con enfoques divergentes —como el GDPR, que impone restricciones estrictas a la transferencia internacional, o la ley china de protección de información personal (PIPL), que demanda localización absoluta para ciertos tipos de datos— complica aún más la toma de decisiones sobre despliegues globales [30].

Frente a este panorama normativo fragmentado y en constante transformación, resulta imprescindible llevar a cabo un mapeo minucioso del flujo de información. Dicho ejercicio no debe limitarse a identificar qué contenido se recolecta o se procesa, sino que debe capturar con precisión su punto de origen, los canales por los que circula y las ubicaciones físicas y lógicas en las que se conserva. La cartografía resultante brinda a las entidades una base sólida para aplicar medidas proporcionales a la sensibilidad del contenido y, al mismo tiempo, evaluar con rigor si los acuerdos de nivel de servicio (SLA) firmados con los proveedores de nube estipulan cláusulas específicas y suficientes en materia de traslado y jurisdicción [31]. Ignorar este tipo de diligencia puede exponer a la institución a controversias legales, sanciones regulatorias o daños reputacionales.

Dado que la esfera legal evoluciona permanentemente, con reformas frecuentes en materia de protección transfronteriza, los bancos centrales deben contar con una función especializada que mantenga una vigilancia activa sobre los cambios normativos en términos de privacidad y custodia digital. Lo anterior implica ajustar políticas internas, capacitar equipos jurídicos y técnicos, así como llevar a cabo revisiones periódicas de contratos para garantizar su vigencia frente a nuevas disposiciones. La publicación *Global Data Sovereignty: A Comparative Overview* de la CSA ofrece un punto de partida para identificar las disparidades normativas y establecer criterios de gobernanza adaptativa frente a esta complejidad creciente [30].

En suma, abordar la soberanía de los datos no puede limitarse a una cláusula genérica en el contrato; reclama un marco institucional que conjugue precisión técnica, seguimiento normativo y negociaciones contractuales informadas, especialmente cuando se trata de custodiar activos de alto valor en el interior de una infraestructura distribuida globalmente.

A través de opciones como cifrado por defecto, residencias geográficas moderadas, transparencia en los registros de acceso y arquitecturas desconectadas, los principales CSP ofrecen un abanico progresivo de mecanismos que permiten configurar controles soberanos alineados con el nivel de sensibilidad de cada activo (Figura 3.1). Esta aproximación modular facilita que cada banco central module su despliegue conforme a las expectativas regulatorias y sus propias exigencias institucionales.

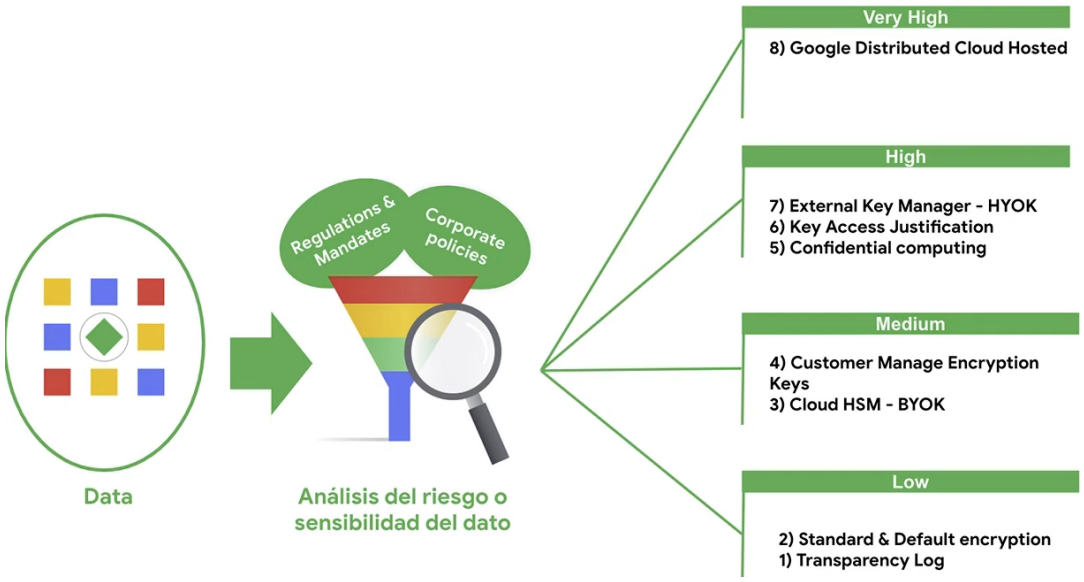


Figura 3.1: Estrategia de soberanía de datos de acuerdo con la clasificación del dato o activo. Fuente: *Soberanía digital y del dato en Google Cloud* [28].

3.3 Cifrado en reposo, en tránsito y en uso

El cifrado constituye la columna vertebral de la confidencialidad en entidades emisoras y reguladoras, dado que la información fluye por tres fases diferenciadas: reposo, tránsito y uso. En almacenamiento, se aplican algoritmos simétricos robustos (AES-256) y acople a los estándares FIPS, junto con copias de resguardo, segmentación de privilegios y parches regulares [32]. Durante la transmisión, los enlaces emplean canales autenticados que se se apoyan en TLS 1.3, protegiendo la integridad extremo a extremo frente a intercepciones o alteraciones [33]. El momento más delicado surge cuando el procesamiento se produce en memoria: allí se emplean credenciales temporales, aislamiento por hardware y técnicas avanzadas, como computación confidencial o, en escenarios de muy alta sensibilidad, cifrado homomórfico, para mantener la opacidad incluso mientras se efectúan los cálculos.

A lo largo del ecosistema, los proveedores más destacados aplican un esquema de cifrado en capas que abarca las tres fases descritas. GCP emplea cifrado obligatorio desde el momento en que la información se escribe: cada fragmento recibe una *data*

encryption key (AES-256) distinta y esa clave queda envuelta por una *key encryption key* alojada en *Cloud Key Managment Service* (KMS) o, si el cliente lo solicita, en *Cloud Hardware Security Module* (HSM)/External KMS [32].

Durante la transferencia se aplica TLS 1.3 por defecto [33], mientras que en fase de procesamiento las ofertas de computación confidencial (Confidential VMs, Confidential GKE Nodes, Confidential Dataflow, entre otras) mantienen la memoria cifrada con claves efímeras generadas dentro de la CPU, lo que aísla la información incluso frente a la plataforma anfitriona [34]. Las cargas que demanden aislamiento absoluto disponen de *Google Distributed Cloud*, un despliegue desconectado que no interactúa con la red pública de Google [35].

AWS adopta un patrón análogo: S3, EBS y el resto de los servicios gestionados activan cifrado automático del lado del servidor mediante claves simétricas, las cuales se encapsulan bajo una *customer managed key* o una *AWS managed key* administrada por AWS KMS [36]; quienes requieran hardware dedicado disponen de CloudHSM o de la modalidad *external key store* [37]. El tráfico se protege con TLS 1.2+ (opción 1.3), y el procesamiento confidencial se confía a *Nitro Enclaves* (dominios mínimos, sin red propia) [38] o a instancias AMD EPYC con *Secure Memory Encryption*/SEV-SNP que ofuscan la memoria de forma permanente [39].

3.4 Criptografía homomórfica: potencial y casos de uso

La criptografía homomórfica (*Homomorphic Encryption*, HE) constituye el santo grial del campo criptográfico. Durante decenas de años, especialistas de todo el mundo han explorado centenares de problemas matemáticos con la ambición de crear un mecanismo de cifrado capaz de satisfacer una aspiración muy deseable: ejecutar operaciones y cálculos directamente sobre material cifrado sin revelar nunca su contenido.

La HE posibilita dicho procesamiento opaco, elevando de manera sustancial la confidencialidad y blindando la información frente a filtraciones [40]. Su potencial para la banca resulta palpable: los laboratorios de IBM, por ejemplo, ya han entrenado modelos de ML sobre registros bancarios totalmente cifrados y obtenido predicciones de alta precisión [41]. Entre los casos de uso más prometedores figuran la supervisión de fraudes, la detección de actividades de blanqueo de capitales y la creación de motores de búsqueda que jamás exponen texto en claro [41].

Esta idea de «calcular sin ver», resulta particularmente útil en la era de la inteligencia artificial y, en términos más generales, del procesamiento en la nube. Hoy en día, con frecuencia, el dueño o custodio de la información entrega sus datasets sensibles a un tercero, que llamaremos genéricamente «el operador», y que bien puede ser un modelo

conversacional como ChatGPT o un proveedor, que los procesa mediante algoritmos propios antes de devolver un resultado elaborado. Nótese que en este esquema tercerizado existe un acuerdo tácito: el procesador accede al contenido sensible, pero solo con el fin legítimo solicitado por su propietario.

En la práctica, este pacto sustentado en la buena fe incomoda un poco. Usualmente, se firman SLA, que incluyen toda clase de penalizaciones por eventuales deslices en confidencialidad y protección, y se espera que sean honrados a cabalidad; sin embargo, persiste la idea que el dueño cedió su tesoro informático a manos ajenas.

La criptografía homomórfica, por el contrario, transforma al tercero en un operador ciego que procesa valores cifrados mediante algoritmos que producen resultados equivalentes (homomórficos) al que se obtendría trabajando sobre el texto en claro. Tradicionalmente, el tratamiento de contenido cifrado exigía descifrar, procesar y volver a cifrar, lo que incrementaba el tráfico de subida y de bajada de la nube. Además, exponía temporalmente los datos a vulnerabilidades durante su estado descifrado. El enfoque de la HE elimina ese intervalo de exposición al permitir que sumas, multiplicaciones y otras operaciones algebraicas se ejecuten directamente sobre los elementos cifrados. El resultado de estas operaciones, una vez descifrado, es idéntico al que se obtendría si se hubieran realizado sobre el material original.

Con el paso de los años y tras una labor investigativa rigurosa, se han encontrado varios tipos de esquemas criptográficos homomórficos. Se distinguen, por un lado, las construcciones parciales, limitadas a una sola operación matemática (suma o multiplicación), y, por otro, la familia «algo» homomórfica, que admite únicamente un subconjunto de transformaciones. A la vanguardia se sitúa el cifrado completamente homomórfico (*Fully Homomorphic Encryption*, FHE), capaz de admitir cualquier cálculo arbitrario sobre valores encriptados [42].

Este tipo de criptografía es atractiva en modelos de computación delegada, en los que un proveedor procesa material reservado en nombre de un tercero,rasgo común tanto en servicios de inteligencia artificial como en plataformas de nube. No obstante, el principal obstáculo reside en la demanda extraordinaria de recursos de procesamiento, que se traduce en latencias y consumo energético todavía notables, aun cuando se continúan registrando avances significativos en términos de desempeño.

3.4.1 Definición formal

La criptografía homomórfica inaugura una categoría de algoritmos capaz de ejecutar transformaciones directamente sobre material cifrado. De manera formal, si C denota el procedimiento de cifrado y f es una función que se aplica a los datos cifrados, se cumple la relación:

$$C(f(x_1)), C(f(x_2)), ..., C(f(x_n)) = HE(f(C(x_1), C(x_2), ..., C(x_n))) \tag{3.1}$$

Por tanto, procesar primero y cifrar después resulta indistinguible de cifrar primero y procesar después. Nótese que la función f es arbitraria, podría ser desde una fórmula de incentivos salariales hasta la métrica de similitud coseno de una aplicación de recuperación de información o incluso las ecuaciones matriciales de un algoritmo de entrenamiento de inteligencia artificial generativa. En la práctica, el operador delegado lleva a cabo los cálculos sobre valores que son incomprensibles para él debido a que no dispone de la llave correspondiente; por su parte, el dueño legítimo descifra el resultado y obtiene la misma salida que hubiera logrado al ejecutar la operación en sus propias instalaciones. De este modo, el prestador de servicios, actúa como un ejecutor completamente ciego a los contenidos con los que trabaja, puesto que en ningún momento tuvo acceso a la información en texto claro del propietario.

3.4.2 Recorrido histórico

Los primeros indicios sobre propiedades homomórficas se descubrieron de una manera casi que afortunada en la década de 1980: ciertas ejecuciones del algoritmo RSA resultaban multiplicativamente homomórficas. En términos prácticos, multiplicar dos textos cifrados con RSA y después descifrarlo arroja el mismo producto que se obtendría al multiplicar los mensajes originales. En la notación anteriormente usada:

$$C(x_1)C(x_2) = C(x_1x_2) \tag{3.2}$$

Desafortunadamente, las variantes de RSA que exhiben esta característica son inseguras y, además, solo cubren la operación multiplicación, por lo que se catalogan como homomorfismo parcial. Aun así, este hallazgo disparó una intensa actividad académica en búsqueda de otros algoritmos seguros que extendieran el repertorio operativo.

Un atributo análogo aparece en la versión estándar de ElGamal [43], un esquema basado en el intercambio de claves Diffie–Hellman, el cual es adoptado en criptosistemas muy populares como GNU Privacy Guard y PGP. Se trata así de productos criptográficos homomórficos, si bien solo para la multiplicación.

Posteriormente, en 1999, se publicó el cifrado Paillier [43], el cual destaca por ser aditivo. Es decir, la suma de dos textos cifrados con Paillier, una vez descifrada, coincide con la suma de los mensajes en claro. Pese a que es considerado seguro, nuevamente, se trata de un homomorfismo parcial limitado a una única operación.

Tiempo después, la investigación se volcó hacia una novedosa estructura algebraica:

las retículas (*lattices*). Así, aparecieron problemas computacionalmente complejos que buscaban introducir una pequeña cantidad de ruido en cada operación. Tal perturbación es perfectamente tolerable y subsanable por el destinatario legítimo, pero se vuelve imposible de manejar para un adversario, debido a que se acumula con cada cálculo que este intente aplicar y termina oscureciendo por completo el mensaje.

Sobre esta base se propusieron esquemas que combinan sumas y productos, denominados ligeramente homomórficos (*Somewhat Homomorphic Encryption*, SWHE), que permitieron vislumbrar una posibilidad real de lograr un cifrado completamente homomórfico. El advenimiento de SWHE marcó un punto de inflexión: a diferencia de los algoritmos parciales, estos permiten ejecutar tanto adiciones como multiplicaciones sobre textos cifrados. Sin embargo, su principal limitación radica en que el número de operaciones soportadas es finito y predeterminado por los parámetros del sistema. En concreto, cada paso incrementa el ruido embebido y, llegado cierto umbral, el descifrado resultaría impracticable incluso para el receptor autorizado.

De los problemas de aprendizaje con errores (*learning with errors*, LWE) sobre retículas se avanzó hacia su variante de anillos de aprendizaje con errores (*ring learning with errors*,o RLWE), donde la nueva estructura algebraica redujo de manera sustancial la carga computacional. Finalmente, en 2009, Craig Gentry alcanzó el «santo grial» de la criptografía con su tesis doctoral, presentando el primer esquema completamente homomórfico sustentado en retículas ideales (*ideal lattices*). El modelo de Gentry define operaciones elementales —suma y producto— que conservan la homomorfía y, por extensión, permiten construir cualquier función computable sobre datos cifrados, obteniendo un resultado idéntico al que se conseguiría en texto claro.

La técnica fundamental que utilizó Gentry se conoce como *bootstrapping*, la cual consiste en un proceso mediante el cual se «refresca» el cifrado saturado de ruido, atenuándolo a un nivel manejable sin revelar su contenido. De forma ingeniosa, el propio circuito de descifrado se evalúa homomórficamente sobre el mensaje alterado, de modo que la salida regresa a un estado «limpio» apto para continuar procesándose.

No obstante, el precio de tal proeza es considerable: cada paso de bootstrapping demanda recursos computacionales notables, traduciéndose en tiempos de ejecución de varios minutos sobre hardware convencional, y el esquema propuesto exige invocar el método con frecuencia. Así, la construcción de Gentry constituye una demostración teórica del concepto de HE, pero todavía distante de un despliegue pragmático debido a la demanda de cómputo.

3.4.3 Proyecciones y líneas de innovación

Aunque el esquema de Gentry es una concepción teórica, incentivó una gran actividad académica e industrial orientada a transformar la criptografía homomórfica en una solución con aplicaciones reales. Al respecto, se han venido desarrollando otros esquemas con diferentes características. Los más notables son [42]:

- **BGV** (por las iniciales de sus autores Brakerski-Gentry-Vaikuntanathan) introduce una mejora en la concepción del proceso de bootstraping que no requiere que sea usado con tanta frecuencia. Un avance sustancial, pero todavía insuficiente.
- **BFV** (por las iniciales de sus autores Brakerski/Fan-Vercauteren), publicado en el 2012, introdujo tiempos de respuesta ya aceptables. Incluye la posibilidad de trabajar con operaciones habituales de álgebra lineal: producto punto y similaridad coseno, así como también los vectores de números reales que son usuales en las aplicaciones de inteligencia artificial. El algoritmo abre la puerta a los primeros despliegues corporativos.
- **TFHE** (*Fast Fully Homomorphic Encryption over the Torus*), presentado en el año 2020, refinó aún más el proceso de refresco de ruido. Condujo a implementaciones populares (por ejemplo, la librería `https://tfhe.github.io/tfhe/`), acogidas por diversos fabricantes en sus productos,
- **CKKS** (por las iniciales de sus creadores Jung Hee Cheon, Andrey Kim, Miran Kim, and Yongsoo Song): optimiza la aritmética de números reales y complejos en punto flotante. Es especialmente útil para aplicaciones de inteligencia artificial (redes neuronales) y tareas avanzadas de análisis cuantitativo.

Tales avances perfilan un horizonte donde el procesamiento confidencial se vuelve cada vez más viable, mitigando la penalización de latencia y acercando la criptografía homomórfica a cargas de trabajo críticas en finanzas, sanidad y ML.

De hecho, la criptografía homomórfica ha alcanzado un nivel de madurez adecuado para ser incluida en aplicaciones corporativas de gran visibilidad. En efecto, Apple anunció en octubre del 2024 la versión Sequoia 15.15 del sistema operativo macOS, la cual integra esta tecnología en las funciones de inteligencia artificial [44]. La razón es simple: cada vez que un usuario recurre a un servicio de IA, sea Gemini o ChatGPT, entrega información sensible a un procesador tercero que podría desviarla de su finalidad, pese a las cláusulas contractuales que intentan acotar tal riesgo. Por tal razón, en el caso de Apple, toda la interacción entre el dispositivo y los servidores de IA se halla completamente cifrada desde la versión mencionada. De esta manera, los nodos de cómputo internos llevan a cabo los cálculos solicitados por los algoritmos de inteligencia artificial sobre los valores cifrados, sin conocer ni revelar el contenido original. Por consiguiente, la empresa actúa como un «operador ciego». El equipo de Apple ha liberado,

además, librerías de código abierto (véase https://github.com/apple/swift-homomorphic-encryption) que utilizan el algoritmo BFV y se benefician de su resistencia a ataques de computadores cuánticos.

Un caso ilustrativo lo otorga el paradigma PIR (Private Information Retrieval), donde el cliente envía cifrados los términos de búsqueda (palabras clave, una foto o un sonido), los servidores procesan la consulta sin descifrar y responden con resultados igualmente cifrados. El descifrado ocurre únicamente en el dispositivo local. Así, Apple®, como entidad prestadora, nunca llega a conocer el contenido de la petición. Tal modelo responde a la necesidad latente de privacidad en una Internet donde cada consulta se archiva y perfila.

Persisten, sin embargo, áreas de mejora. Por un lado, se busca mitigar la latencia derivada de las operaciones homomórficas mediante hardware especializado —*application-specific integrated circuit* (ASIC) o *field-programmable gate array* (FPGA)— o a través de parámetros criptográficos optimizados que reduzcan tanto el tamaño del texto cifrado como los ciclos de cálculo. Adicionalmente, es deseable disponer de librerías que permitan incorporar esta capacidad de una manera más amigable para el programador, sin profundizar en la complejidad matemática subyacente.

3.4.4 Aplicaciones para bancos centrales

El cifrado homomórfico se perfila como un catalizador para la analítica financiera al resguardar la confidencialidad incluso durante el procesamiento [40]; sin embargo, su despliegue efectivo exige ponderar múltiples limitaciones inherentes. La sobrecarga computacional continúa siendo elevada y el repertorio de transformaciones soportado depende del tipo de esquema —PHE, SWHE o FHE—, lo que obliga a diseñar casos de uso circunscritos: monitoreo de fraude, detección de comportamientos sospechosos en registros ya agregados o consultas de recuperación de información privada donde la latencia puede tolerarse.

En un banco central, las restricciones no invalidan la tecnología. Por el contrario, delinean el perímetro donde su adopción aporta valor. Por ejemplo, entidades emisoras pueden compartir indicadores financieros cifrados con organismos de supervisión regionales, posibilitando una vista colectiva de la exposición sistémica sin revelar datos transaccionales. Asimismo, la colaboración con departamentos de justicia [40] permitiría examinar patrones de lavado de dinero mediante modelos de ML que operan sobre paquetes cifrados, de modo que ni los analistas externos ni los proveedores de nube visualicen transferencias individuales. Tales escenarios requieren clústeres especializados —GPUs optimizadas o incluso ASIC dedicados a operaciones con retículas— además de personal con pericia en bibliotecas como Microsoft SEAL, CKKS o TFHE.

En perspectiva, la criptografía homomórfica no representa una solución universal, sino una herramienta costosa y sofisticada, pero insustituible cuando la confidencialidad absoluta es innegociable. Su utilización por parte de gigantes tecnológicos, la aparición de módulos aceleradores y la creciente presión regulatoria sobre la privacidad colocan a esta técnica en la senda de convertirse en un componente estándar para procesar información estratégica en el interior del ecosistema financiero global.

3.5 Gestión de llaves criptográficas y servicios de cifrado

Una administración criptográfica avanzada constituye el pilar sobre el que descansa la confiabilidad de cualquier esquema de cifrado, premisa especialmente relevante para bancos centrales que trabajan con activos digitales de máxima sensibilidad. En este contexto, los servicios de gestión de claves (KMS) centralizan el manejo de ciclos de vida, políticas y rotaciones automáticas [45], mientras que los módulos de seguridad de hardware (HSM) —alojados en la nube o instalados localmente— emplean un anclaje físico que resguarda material criptográfico fuera del alcance del plano lógico.

Los KMS ofrecidos por los CSP admiten que cada llave permanezca en la región escogida por la entidad [46] y delegan la custodia operativa en infraestructura escalable, reduciendo la complejidad que implicaría el aprovisionamiento físico. Los Cloud HSM, por su parte, agregan una capa adicional de aislamiento al encapsular las llaves raíz en dispositivos validados con FIPS 140-2 nivel 3, tal que el material de la clave no se expone ni siquiera al proveedor [46], cumpliendo así mandatos regulatorios donde la institución debe conservar dominio exclusivo sobre la raíz de confianza [47]. Frente a ellos, los HSM instalados on-premise otorgan soberanía plena, tanto lógica como física, pese a que exigen inversión en espacio, energía, mantenimiento especializado y ciclos de renovación de hardware [46].

Para elegir la opción idónea conviene equilibrar diversos vectores: la criticidad de la carga de trabajo, la jurisprudencia que restringe la localización de llaves, la elasticidad requerida por picos de demanda y el presupuesto disponible. Así, tareas rutinarias de cifrado de volúmenes o bases de datos quizá se beneficien del modelo KMS regional, mientras que operaciones de alta sensibilidad (por ejemplo, emisión monetaria digital o custodia de credenciales interbancarias) podrían demandar Cloud HSM o incluso artefactos locales. La ponderación del riesgo debe ponderar no solo el nivel de exposición residual, sino también la necesidad de integrarse con instrumentos de auditoría continua, registros inmutables y esquemas de rotación que resulten trazables ante cualquier autoridad supervisora.

3.5.1 Bring Your Own Key (BYOK) / Hold Your Own Key (HYOK)

Las arquitecturas *Bring Your Own Key* (BYOK) y *Hold Your Own Key* (HYOK) conforman un continuo de soberanía criptográfica. En la modalidad BYOK, la entidad genera la clave maestra dentro de su perímetro y, posteriormente, la importa al servicio de administración de claves del CSP [47]; con ello retiene la génesis del secreto y conserva una copia local. Pese a que otorga flexibilidad, gobernanza sobre datos sensibles, visibilidad sobre el uso de llaves y acople con requisitos de cumplimiento, la versión operativa se custodia en la infraestructura del proveedor bajo sus políticas internas [47].

En contraste, en HYOK (también denominada *External Key Management* o EKM), la clave nunca abandona el dominio institucional. Por ende, cada vez que la plataforma necesita ejecutar una operación criptográfica, invoca el componente externo mediante interfaces seguras, de modo que nunca observa el material en texto claro [46].

La escala de opciones resulta decisiva al calibrar la confianza depositada en terceros. BYOK ya suprime la dependencia de claves generadas por el operador de nube, pero HYOK/EKM eleva la salvaguardia requerida para activos de máxima sensibilidad, donde cualquier posible exposición —sea por personal interno del CSP o por requerimientos gubernamentales— deviene inaceptable. La elección entre ambos esquemas repercute de forma directa en la postura de riesgo y, por extensión, en la política institucional de soberanía sobre la información.

En el ecosistema de GCP [48], HYOK se concreta a través de Cloud EKM, donde cada versión de clave se compone de material externo residente en el gestor propio, una referencia única (URI o ruta) y un fragmento interno alojado en Cloud KMS que actúa como segunda envoltura durante la transacción. Para cifrar, KMS primero aplica su capa simétrica y el bloque resultante se remite al EKM, que lo encapsula otra vez con el material externo antes de retornarlo. Sin ambas capas —interna y externa— el descifrado resulta inviable. El mecanismo puede reforzarse mediante *key access justifications*, donde el sistema registra la motivación de cada solicitud y se atiende únicamente cuando coincide con los códigos autorizados por la política configurada, lo que añade trazabilidad e impide el ingreso de peticiones abusivas [48].

En conjunto, EKM aporta visibilidad sobre el origen, la ubicación y la replicación de las claves, al tiempo que habilita un modelo unificado para la administración de políticas y la imposición de restricciones en la consulta o uso. Tal centralización permite a las organizaciones ejercer un gobierno coherente tanto en entornos locales como en la nube pública [48], consolidando los flujos de autorización y reduciendo la exposición.

Adicionalmente, la elección también depende de la estrategia de despliegue [29]:

- **Saas**: Puesto que este modelo es limitado en opciones, BYOK y HYOK son las únicas opciones.

- **PaaS**: Admite tanto *Bring Your Own Encryption* (BYOE) como BYOK, dependiendo de las necesidades. Sin embargo, BYOE exige una mayor intervención, debido a que el CSC debe desarrollar el código para integrar las funciones de administración de criptografía y llaves en su aplicación.
- **IaaS**: Habilita BYOE, que a su vez implicaría HYOK dado que el cliente es quien se ocupa de gestionar los procesos de protección de datos en su totalidad. Esta es la única opción que permitiría la portabilidad de datos entre nubes.

El diagrama expuesto en la Figura 3.2 sintetiza las modalidades para resguardar los datos almacenados en la nube:

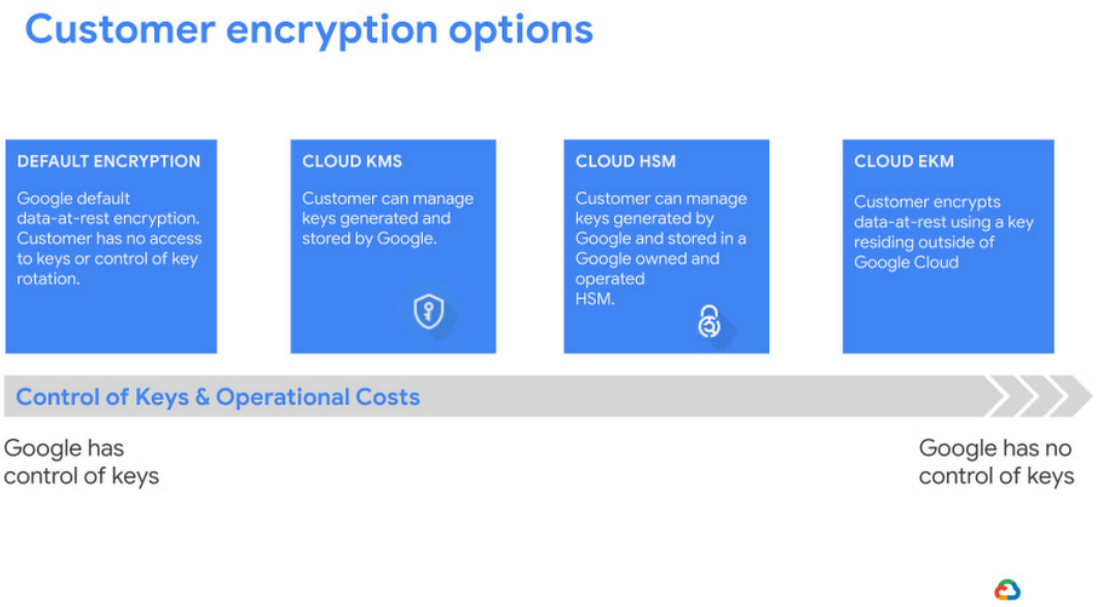


Figura 3.2: Opciones de cifrado en las bases de datos de Google Cloud. Fuente:*Architecting for database encryption on Google Cloud* [49].

Por último, la Tabla 3.2 recopila y organiza la explicación previa en un formato fácilmente comprensible.

Tabla 3.2. Esquemas de protección de datos y gobierno de llaves de cifrado.

Estrategia	Ubicación de la llave	Control	Aplicaciones típicas	Ventajas	Limitaciones
Cloud KMS	Almacenada y administrada por el proveedor de nube.	Limitado	Protección de datos generales en servicios en la nube.	Simplicidad operativa y escalabilidad incorporada.	Menor visibilidad y dependencia del proveedor.
Cloud HSM	Alojada en HSM dedicado en el entorno del proveedor.	Intermedio	Protección de datos sensibles bajo requisitos regulatorios estrictos.	Alta seguridad con menor esfuerzo que HSM local.	Costos elevados y menor control comparado con HSM local.
BYOK	Generada por el cliente y transferida al KMS del proveedor.	Elevado	Cumplimiento normativo con trazabilidad del origen de la llave.	Control sobre el ciclo de vida y trazabilidad de la llave.	Persistencia de la clave en el entorno del proveedor.
HYOK/ EKM	Residencia exclusiva en el sistema del cliente, fuera del proveedor.	Total	Soberanía total para cargas críticas o confidenciales.	Autonomía criptográfica completa; sin exposición al proveedor.	Complejidad técnica y operativa superior, junto con una inversión inicial considerable.

3.5.2 Ciclo de vida de las llaves

El ciclo de vida comprende desde la creación hasta la eliminación definitiva, contemplando la generación, distribución, almacenamiento, utilización, renovación, revocación y destrucción segura [45]. Tal secuencia garantiza que cada llave mantenga su vigencia a nivel funcional sin comprometer la confidencialidad o integridad de la información protegida. En particular, la automatización de estas etapas —como la rotación periódica y la atención a su expiración— por medio de servicios en la nube minimiza la exposición a errores humanos, fortalece la coherencia frente a las políticas de seguridad y reduce la carga operativa que implican los procesos manuales [45].

En la industria financiera, los bancos son responsables de custodiar activos de elevado valor y de trabajar con sistemas críticos, por lo que dicha automatización constituye no solo una mejora técnica, sino una condición esencial para sostener una arquitectura criptográfica robusta. La capacidad de revocar con inmediatez una clave comprometida o de suprimir de forma irrecuperable aquella que ha completado su propósito, utilidades que ofrecen los ecosistemas de nube, contribuye a consolidar una postura criptográfica resiliente y alineada con los estándares más exigentes en entornos de alta sensibilidad.

3.6 Preparación para criptografía poscuántica

A fin de que la infraestructura de seguridad de los bancos centrales responda adecuadamente a la próxima disrupción cuántica, es indispensable estudiar los nuevos estándares poscuánticos (PQC) seleccionados por el NIST [50] y optar por suites híbridas que combinen la criptografía actual con primitivas resistentes a Shor y Grover. Solo así, podrán neutralizar el riesgo del denominado *store now, decrypt later*, donde archivos retenidos durante décadas (balances de pagos, estrategias de inversión a largo plazo, indicadores macroprudenciales o historiales transaccionales) quedarían expuestos a las habilidades adversariales futuras que inaugura la computación cuántica [51].

En respuesta a este panorama, los grandes proveedores han comenzado a desplegar capacidades concretas. Por un lado, AWS ha integrado el mecanismo de encapsulación de claves basado en módulos y redes (ML-KEM) en su biblioteca criptográfica de código abierto (AWS-LC), convirtiéndola en el primer módulo que ofrece compatibilidad con algoritmos poscuánticos dentro de un marco validado por FIPS [52]. Esta implementación ha sido desplegada en diversos servicios de AWS; por ejemplo, el enfoque híbrido de intercambio de claves para el protocolo TLS en AWS KMS y AWS Secrets combina algoritmos clásicos y postcuánticos en las llamadas a la API [52].

De forma similar, todos los servicios de Google y algunos servicios nativos de GCP ya utilizan cifrado de red asegurado con ML-KEM [50]. Adicionalmente, la compañía planea ofrecer a sus clientes protección contra ataques de almacenamiento inmediato y descifrado posterior, proporcionando a los administradores herramientas que les permitan supervisar la adopción de PQC y el cumplimiento en toda su organización [53]. Además, el servicio Cloud KMS ahora soporta la generación y el uso de firmas digitales resistentes a capacidades cuánticas [53].

Desde la perspectiva del banco central, este paso le exige afianzar su agilidad criptográfica [50]: bibliotecas modulares, rotación de claves orquestada y ciclos continuos de actualización que favorezcan el intercambio de algoritmos a medida que emergen

vulnerabilidades o alteraciones normativas, preservando así la confidencialidad estructural de los datos que sustentan la estabilidad monetaria y la confianza sistémica. Lo anterior promueve un enfoque en el que las instituciones financieras, los reguladores y los líderes de la industria pueden alinear sus planes y hojas de ruta para procurar una transición eficaz y progresiva a arquitecturas *quantum-safe* [51].

4 Controles por dominios críticos y prácticas DevSecOps

4.1 Perímetro y red en la nube

4.1.1 Segmentación de redes y microsegmentación

En entornos de nube, la segmentación clásica se apoya en redes virtuales y subredes para aislar flujos de norte a sur (tránsito cliente-servidor) por dominios lógicos —por ejemplo, *front end*, servicios y datos—. La microsegmentación profundiza el aislamiento al regular con precisión los flujos de este a oeste entre cargas de trabajo internas, de modo que cada una solo intercambie información con contrapartes autorizadas. Al perfilar tanto identidades como dependencias y aplicar políticas a nivel de recurso (servicio, aplicación, usuario o cuenta de servicio), se reduce de manera drástica el movimiento lateral dentro de la red [54]. En consonancia con el principio de mínimo privilegio, la comunicación queda circunscrita al tráfico estrictamente imprescindible.

En AWS, tal modelo se materializa con el servicio Virtual Private Cloud (VPC), reforzado con grupos de seguridad (filtrado con estado) y listas de control de acceso de red (sin estado) para el control del tráfico a nivel de instancia. En Microsoft Azure, las *Virtual Networks* se complementan con *Network Security Groups* (NSG) y, cuando se requiera, Azure Firewall. En Google Cloud, las reglas de *firewall* de VPC —definidas por etiquetas o cuentas de servicio— habilitan la microsegmentación a gran escala [55].

Soluciones especializadas como Illumio Zero Trust Segmentation [56] y Akamai Guardicore Segmentation [57] aportan un plano de control coherente para arquitecturas híbridas y multinube. Mediante sensores o agentes ligeros, estas recogen telemetría, construyen mapas de dependencias casi en tiempo real y formulan políticas que se expresan con atributos de identidad de proceso, etiquetas, metadatos de entorno y contexto de aplicación. Esta aproximación orientada a identidad facilita la contención de brechas y la delimitación de relaciones legítimas sin anclar reglas a topologías cambiantes, permitiendo controles de segmentación consistentes en todo el perímetro lógico.

4.1.2 Web Application Firewalls (WAF) y balanceadores de carga

Los firewalls de aplicaciones web (WAF) resguardan servicios en línea mediante la inspección del tráfico HTTP/HTTPS y la neutralización de vectores habituales —como la inyección SQL y el XSS, entre otros—, antes de que alcancen la lógica de negocio. En AWS, AWS WAF se integra con CloudFront, API Gateway y Application Load Balancer (ALB); en Azure, la función WAF se concreta a través de Application Gateway y Front Door; y en Google Cloud (GCP), Cloud Armor actúa como WAF y añade mitigación frente a DDoS [55].

En paralelo, los balanceadores de carga distribuyen las solicitudes entre instancias para asegurar la alta disponibilidad y sirven como punto de anclaje de políticas de protección: en AWS, ALB y NLB operan a nivel regional —en capas 7 y 4, respectivamente— y se integran con WAF; en Azure, Load Balancer funciona en la capa 4 y se complementa con Application Gateway en la capa 7 (L7); y en Google Cloud, Cloud Load Balancing ofrece modalidades globales y regionales con escalado automático [58].

La conjunción de estas piezas conforma un borde defensivo robusto que desacopla los orígenes de Internet, absorbe picos hostiles y bloquea patrones maliciosos en el perímetro, antes de que afecten a los servidores de aplicación.

4.1.3 Protección nativa frente a DDoS y autoescalado

Los proveedores implementan defensas nativas frente a DDoS en las capas 3 y 4 (L3 y L4). AWS Shield Standard, incluido sin costo para todos los clientes, supervisa el tráfico en los bordes de la red —por ejemplo, en CloudFront, Route 53 y Global Accelerator—, detectando y bloqueando ataques volumétricos en escalas de milisegundos [59].

En cuanto a GCP, se apoya en una dirección IP *anycast* global que distribuye el tráfico de manera eficiente desde el punto de vista geográfico, dispersando las ofensivas masivas. Además, Cloud Armor proporciona defensa tanto a nivel de red como de aplicación (capa 7 o L7) [60].

Microsoft Azure, por su parte, ofrece protección básica integrada contra DDoS para sus recursos públicos. Para un blindaje más sólido, dispone de dos niveles de servicio avanzados: DDoS IP Protection y DDoS Network Protection. Este último destaca porque ajusta automáticamente las políticas de mitigación a los patrones de tráfico característicos de cada aplicación, y entrega métricas detalladas y alertas en tiempo real [61]. En una defensa por capas, resulta recomendable combinar Azure Front Door —servicio que actúa como puerta de enlace global de API y resguarda frente a ataques DDoS en L3 y L4— con un WAF para detener amenazas web en L7.

Conviene, asimismo, acoplar el autoescalado para absorber picos: ante un DDoS persistente, las aplicaciones pueden escalar horizontalmente para preservar la disponibilidad, aunque esto suponga un gasto adicional. En AWS, por ejemplo, este enfoque se concreta mediante Auto Scaling Groups, activados a través de alarmas personalizadas desde CloudWatch que ajustan dinámicamente la capacidad de EC2 en función de métricas como la CPU, la memoria o la E/S de red [62].

En suma, una arquitectura preparada para DDoS combina la reducción de superficie —cerrar puertos innecesarios u ocultar orígenes tras una CDN—, el escalado automático ante incrementos drásticos de solicitudes y un WAF con reglas dirigidas a frenar inundaciones HTTP o *botnets* antes de que saturen los recursos.

4.2 Identidades, accesos y secretos

4.2.1 Principio de mínimo privilegio y Zero Trust

El principio de mínimo privilegio exige que cada identidad (humana o de servicio) reciba solo las autorizaciones estrictamente necesarias sobre recursos y acciones, partiendo de permisos mínimos y ampliándolos solo cuando la función lo demande. Procediendo así, se reduce el impacto de credenciales expuestas o de errores operativos. En AWS, se dispone de políticas IAM granulares y herramientas como IAM Access Analyzer, que detecta exposiciones de acceso público o entre cuentas, identifica permisos internos no previstos, valida la sintaxis y la semántica de las políticas JSON frente a buenas prácticas y, a partir de trazas de CloudTrail, sintetiza plantillas de privilegio mínimo coherentes con el uso real de cada usuario o rol [63]. En el ecosistema de Azure, se recurre a Microsoft Entra ID (antes Azure Active Directory, AD) y al modelo RBAC, que delimita permisos a ámbitos correctamente definidos [64]. En Google Cloud, IAM asigna roles con precisión a lo largo de la jerarquía (organización, carpeta y proyecto).

Por su lado, la arquitectura de confianza cero (*zero trust*) se cimenta en la idea de que no existe confianza implícita por ubicación de red o propiedad del activo; por ello, toda solicitud debe autenticarse y autorizarse de manera explícita, compartiendo señales contextuales (postura del dispositivo, ubicación, tiempo o riesgo) en cada ingreso [65]. En la práctica, lo anterior se aplica combinando MFA obligatoria, evaluación continua por solicitud y publicación de aplicaciones internas sin VPN, con decisiones de acceso basadas en el contexto.

En Microsoft Entra, la característica Conditional Access aplica políticas en tiempo real basándose en indicadores como el comportamiento anómalo del usuario, la locación asociada a la dirección IP y la puntuación de riesgo individual [64]. El agente de opti-

mización integrado con Microsoft Security Copilot sugiere nuevas políticas y ajusta las existentes conforme a los principios de *zero trust* y a las prácticas recomendadas por Microsoft. Este asistente examina, entre otros aspectos, la exigencia de MFA, la imposición de controles en el equipo (conformidad del terminal, protección de aplicaciones y pertenencia al dominio) y el bloqueo de la autenticación heredada o de flujos basados en códigos del dispositivo [66].

En Google Cloud, BeyondCorp/Identity-Aware Proxy (IAP) [67], coloca un *proxy* de identidad delante de las aplicaciones privadas: consulta *tokens* OAuth/OIDC y, mediante Context-Aware Access, integra atributos de dispositivo, geografía, horario y etiquetas de recurso para evaluar políticas ABAC, trasladando el control al perímetro lógico de la aplicación sin recurrir a túneles tradicionales. En su edición Enterprise, Chrome actúa como *front end* reforzado con la extensión Endpoint Verification y un perfil corporativo que impone las normas de uso aceptable, la separación de cuentas personales, el DLP o Safe Browsing, el escaneo *antimalware*, las listas de extensiones/aplicaciones autorizadas y el diagnóstico de postura (respecto al cifrado, versión del SO, entre otros). Con ello, se habilitan salvaguardas granulares para bloquear las interacciones con aplicaciones de Google o de terceros, impedir descargas o extracción de contenido sensible y, cuando procede, restringir el ingreso a plataformas de nube [67].

Construida sobre principios de confianza cero, AWS Verified Access expone aplicaciones internas sin VPN, evaluando cada solicitud contra políticas que combinan identidad federada (IdP SAML/OIDC) y postura del dispositivo (contexto de proveedores como CrowdStrike, Jamf o JumpCloud) [68]. Otros servicios complementarios son Amazon Verified Permissions, Amazon WorkSpaces. En conjunto, estos componentes proveen un acceso seguro a los recursos corporativos y dificultan de forma sustantiva el movimiento lateral, aun cuando una credencial aislada queda expuesta.

4.2.2 Identidad federada y directorios centralizados

Las organizaciones suelen centralizar la administración de identidades en un directorio corporativo o IdP único y federar credenciales hacia los distintos servicios en la nube. La federación implica que un IdP externo autentica al usuario y el servicio consume esa aserción para otorgar permisos conforme a políticas predefinidas. De este modo, las personas inician sesión en AWS, Azure o Google Cloud con sus credenciales corporativas, evitando usar cuentas locales en cada plataforma.

En AWS, la federación se apoya en SAML 2.0, OIDC y OAuth 2.0 (desde Active Directory u Okta, por ejemplo) y se operacionaliza con IAM Identity Center, que conecta el directorio central y asigna roles en cada cuenta a partir de grupos corporativos [69]. En Microsoft Entra ID, el AD actúa como IdP principal, se sincroniza con directorios activos

locales y emite identidades federadas hacia aplicaciones SaaS y otras nubes a través de protocolos estándar [64].

Este esquema concentra la provisión, retiro y ajustes de credenciales en un punto único, viabiliza la incorporación de MFA coherente, instaura normas homogéneas de contraseñas y consolida la huella de auditoría, favoreciendo el cumplimiento. Tal enfoque aminora la carga administrativa y el riesgo de parametrizaciones defectuosas (por ejemplo, cuentas huérfanas con privilegios persistentes), al tiempo que reduce la dispersión operativa y conserva una única fuente de verdad sobre la identidad, aplicando de manera consistente el principio de mínimo privilegio en la totalidad de los recursos.

4.2.3 Plataformas de identidad y APIs entre proveedores

En el ecosistema de Microsoft, Microsoft Graph no actúa como un *API gateway* genérico al estilo de Azure API Management, sino que opera como una interfaz unificada que centraliza el ingreso programático a la información de Microsoft 365, de componentes de Enterprise Mobility and Security (Microsoft Entra, Identity Manager o Intune, por ejemplo) y otros servicios de productividad, colaboración, inteligencia y educación. Por lo tanto, través de un único punto de entrada. expone recursos de usuarios, grupos, archivos (OneDrive), correo (Outlook) y colaboración (Teams), integrando un modelo de permisos coherente y un esquema de autorización granular [70].

Pese a que no enruta aplicaciones propias de terceros como haría una puerta de enlace clásica, impone controles de seguridad y gobierno comparables a los de este elemento. En el plano de identidad y gestión de acceso a red [70], las API de Microsoft Entra constituyen un entramado fundamental para orquestar políticas de autenticación, perfiles de usuarios, grupos, credenciales, aplicaciones y roles, en conjunto con marcos de autorización condicional y autenticación multifactor. Tales interfaces no solo administran identidades humanas y de servicio, sino que también delimitan permisos sobre recursos internos o externos, habilitan políticas de privilegio escalonado (*just-in-time*) y otorgan visibilidad de riesgos asociados a credenciales y privilegios excesivos. En el ámbito de conectividad, las API permiten definir filtros de tráfico, regular interacciones con aplicaciones públicas o privadas y formular reglas que se integran con políticas condicionales de seguridad [70]. Todo lo anterior se alinea con una arquitectura de confianza cero.

En Google, el rol funcional se distribuye entre las Google Workspace APIs (Gmail, Drive, Calendar y People) y el Admin SDK (gestión de dominios, usuarios y grupos), respaldados por Google Identity y flujos OAuth 2.0 [71]. Tales recursos logran capacidades cercanas —manejo de identidades, directorios, correo y archivos—; sin embargo, no existe un único portal que agregue datos de colaboración, indicadores de seguridad y perfiles

de usuario con la misma uniformidad y bajo una semántica común como lo hace Graph. Para los CSC, esta aproximación satisface requerimientos de manejo de productividad y de directorio, pero exige armonizar múltiples APIs y aplicar políticas de autorización de forma consistente a lo largo del portafolio.

4.3 Almacenamiento acorde a exigencias de retención, inmutabilidad y cumplimiento

Categorías y atributos técnicos Las plataformas de almacenamiento en la nube no se reducen a simples contenedores de ficheros: conforman capas con propiedades bien diferenciadas que inciden en la disponibilidad, el costo total de propiedad, la resiliencia y el cumplimiento. Elegir la clase correcta determina la solidez del plan de continuidad y la viabilidad de los objetivos RTO/RPO, así como la inmutabilidad exigida por las normativas del sector financiero.

- **Almacenamiento de objetos (*Object Storage*)**. Diseñado para información no estructurada (copias de seguridad, bitácoras, contenido multimedia y archivos inmutables de larga conservación), destaca por una durabilidad extraordinaria de 11 nueves (es decir, una pérdida esperada de un objeto entre cien mil millones al año) y por escalas de precio muy competitivas en clases «frías» o de archivo, donde el costo por GB desciende a cambio de mayores latencias de recuperación. Amazon S3 Object Lock, en modos *governance* y *compliance*, emplea el modelo de escribir una vez y leer múltiples veces (*Write Once Read Many*, WORM) para satisfacer requerimientos regulatorios respecto a alteraciones o eliminaciones de objetos [72]. Por su lado, Azure Immutable Storage añade retención por tiempo y bloqueo por litigio que prohíbe eliminaciones hasta que se retire la orden [73]. Finalmente, en GCP, Cloud Storage Bucket Lock fija una política de conservación a nivel de *bucket* que impone el bloqueo para impedir cualquier modificación antes del vencimiento [74]. Combinadas con el versionado y la remoción reversible (*soft delete*), estas facultades fortalecen la trazabilidad, la cadena de custodia y el no repudio, atributos esenciales para las auditorías y para la preservación de evidencia en organizaciones supervisadas.
- **Almacenamiento de bloques (*Block Storage*)**. Útil para cargas con latencia reducida y rendimiento elevado —por ejemplo, bases de datos transaccionales, ERP o motores de pagos—, el cual expone «volúmenes» que se adjuntan a máquinas virtuales y se direccionan como discos crudos. Su desempeño se caracteriza por IOPS (operaciones de entrada/salida por segundo) y rendimiento (MB/s) sostenidos, métricas decisivas para lograr transacciones consistentes [75]. La recupe-

ración se apoya en *snapshots* incrementales y consistentes a nivel de volumen, definidos como instantáneas que aceleran las restauraciones y acortan las ventanas de indisponibilidad.

En AWS, los volúmenes EBS gp3 escalan hasta 16000 IOPS y 1000 MB/s, mientras que las instantáneas EBS son incrementales para reducir tiempos y costes [76]. En Azure, los Managed Disks (Ultra, Premium SSD v2, Premium SSD y Standard SSD/HDD) cubren distintos perfiles de rendimiento [77]. Además, el proveedor soporta la modalidad de discos compartidos, en la que un mismo volumen puede montarse simultáneamente en varias máquinas virtuales dentro de un clúster, lo que posibilita arquitecturas de alta disponibilidad donde múltiples nodos requieren acceso concurrente a un mismo volumen sin pérdida de consistencia.

En Google Cloud, Persistent Disk y Hyperdisk detallan límites de IOPS/rendimiento y suministran copias incrementales estándar o de archivo. Este recurso resulta idóneo cuando se busca un RTO muy bajo y latencias predecibles bajo presión transaccional [78].

- **Almacenamiento de archivos (*File Storage*)**. Proporciona un sistema de ficheros compartido accesible mediante NFS (*Network File System*) o SMB (*Server Message Block*), con semántica POSIX (permisos, enlaces y bloqueo de archivos) esperada por numerosas aplicaciones tradicionales y flujos colaborativos [79]. Entre los servicios administrados destacan Amazon EFS (NFS elástico y de múltiple instancia), Azure Files (comparticiones SMB y NFS con integración de identidades y cuotas) y Google Filestore (sistema de alto rendimiento tipo NFS). Todos contemplan mecanismos de captura puntual o copias gestionadas para recuperar estados previos, sostener la continuidad operativa y ejecutar devoluciones controladas en caso de errores lógicos [79]. Esta modalidad resulta conveniente cuando las aplicaciones requieren rutas compartidas, jerarquía de directorios y consistencia de nombres, sin reescribir la lógica hacia modelos de objeto o bloque.

4.3.1 Consideraciones para bancos centrales

Las regulaciones financieras fijan períodos de retención de datos concretos —por ejemplo, en entidades estadounidenses trabajan en un rango de 5 a 7 años— dependiendo de la naturaleza del registro [80]. Las soluciones de almacenamiento en la nube aportan mecanismos que se alinean con tales exigencias: políticas de retención con bloqueo, versionado de objetos y eliminación reversible [74]. Su adopción posibilita una conformidad más automatizada y verificable, al tiempo que preserva la inmutabilidad requerida para auditorías —como la regla 17a-4 de la SEC, la cual exige un formato no reescribible y no borrable [80]— y reduce la exposición a borrados accidentales o ma-

liciosos. Con ello, la custodia documental deja de depender de procesos manuales y pasa a apoyarse en controles nativos con trazabilidad robusta, mitigando riesgos legales y operativos asociados a una administración deficiente del ciclo de vida de la información.

Operar en múltiples países exige sortear marcos de retención heterogéneos, en ocasiones incluso en tensión entre sí [80], lo que conecta de forma directa con la problemática de la soberanía del dato discutida previamente. Para los bancos centrales, ello implica que las soluciones de almacenamiento en la nube deben exhibir suficiente flexibilidad para acomodar horizontes de conservación y mandatos acerca de la localización que varían según la jurisdicción, sin sacrificar trazabilidad ni gobernanza. Lo anterior se traduce en seleccionar parámetros alineados con cada obligación legal; diseñar flujos sustentados en procedencia, taxonomía y plazo de conservación; y activar replicación con alcance geográfico acotado. En el plano contractual, conviene anotar cláusulas sobre residencia del dato, transferencias transfronterizas, derechos de auditoría, notificación de incidentes y cadena de subproveedores. Asimismo, cuando los requerimientos divergen entre países, puede resultar necesario un despliegue multirregional, inclusive multinube o híbrido, para satisfacer las directrices sin elevar la dependencia a un único proveedor.

En suma a lo anterior, la complejidad regulatoria derivada de trabajar en múltiples jurisdicciones demanda un andamiaje normativo y técnico capaz de conservar conformidad demostrable. Los proveedores aportan piezas clave para tal fin: AWS Artifact actúa como un repositorio autoservicio de elementos de auditoría (ISO 27001, PCI DSS, SOC, entre otros) sobre la infraestructura subyacente [81]. Por su parte, Azure Blueprints y Azure Policy despliegan ajustes y controles prescriptivos alineados con marcos de referencia, favoreciendo auditorías y correcciones automatizadas [82]. Por último, Google Cloud Security Command Center (SCC) centraliza el inventario, los hallazgos y los indicadores de riesgo, mientras que Assured Workloads impone limitaciones de ubicación, requisitos de personal y segmentación por región para escenarios con exigencias elevadas [83].

4.4 DevSecOps e infraestructura como código

4.4.1 Actualizaciones a gran escala y patching orquestado

VM Manager en GCP otorga un marco unificado para administrar a gran escala sistemas operativos Windows y Linux que ejecutan Compute Engine, con foco en actualización, inventario y configuración [84]. Su componente de Patch Management orquesta la aplicación de parches del proveedor —actualizaciones correctivas y de seguridad— en

modalidad bajo demanda, programada o recurrente. En paralelo, OS Inventory Management recoge telemetría del sistema (versiones, paquetes instalados y otros metadatos) para consolidar una visión fidedigna de las instancias disponibles [84]. Finalmente, las OS policies son descripciones declarativas del «estado deseado» (paquetes, repositorios, archivos o recursos personalizados); el agente OS Config aplica las configuraciones y corrige desviaciones en ciclos frecuentes, logrando líneas base homogéneas por entorno [84].

4.4.2 Controles integrados en pipelines CI/CD

La seguridad en CI/CD (integración continua/entrega continua) involucra controles sobre el ciclo de vida del desarrollo de software (SDLC) desde el inicio, con el fin de detectar y neutralizar vulnerabilidades antes de que alcancen producción [85]. Tal enfoque se apoya en la automatización y la escalabilidad alineadas con prácticas ágiles [86], de modo que cada cambio de código atraviesa compuertas de comprobación robustas. Entre las actividades recomendadas destacan el escaneo de vulnerabilidades, las pruebas orientadas a debilidades de aplicación, el monitoreo continuo de la cadena de construcción de paquetes, la separación de funciones, la actualización periódica de dependencias, el modelado de amenazas, el tratamiento confidencial de secretos y las auditorías regulares de permisos y autorizaciones [85].

En primera instancia, se dispone de técnicas tales como:

- **SAST (*Static Application Security Testing*)**: Examina el código fuente en etapas tempranas del SDL bajo el paradigma de caja blanca. Al operar sobre artefactos estáticos, se integra de forma fluida en los pipelines de CI para inspecciones rápidas en cada *commit* o *merge*, detectando patrones inseguros, llamadas peligrosas y configuraciones defectuosas [85]. Respecto a sus limitaciones, exige visibilidad del repositorio y no contempla fallos que emergen en tiempo de ejecución, así como tampoco problemas condicionados por la parametrización del entorno o la interacción entre servicios [86]. Algunos ejemplos son SonarQube, Checkmarx, Fortify, CodeQL, etc.,
- **DAST (*Dynamic Application Security Testing*)**: Evalúa la aplicación en ejecución desde la perspectiva de caja negra, emulando técnicas de ataque reales sobre interfaces web o API. Resulta especialmente útil para descubrir debilidades explotables en la lógica de negocio, validaciones insuficientes, dependencias ocultas y falencias visibles en producción [85]. Su principal desventaja radica en que los hallazgos suelen aparecer en etapas tardías del SDLC, lo que exacerba el costo de corrección y exige una [85]. Herramientas populares abarcan OWASP ZAP, Burp Suite (automatizable), IBM AppScan, etc.

- **SCA (*Software Composition Analysis*)**: Lleva a cabo el inventario de dependencias de terceros y librerías de código abierto, localiza vulnerabilidades conocidas y señala licencias incompatibles, además de advertir sobre dependencias obsoletas [86]. Esta práctica también aporta trazabilidad de la lista de materiales de software (*Software Bill of Materials*, SBOM) y contribuye a la higiene de la cadena de suministro al evitar la propagación de paquetes comprometidos. Plataformas como Sonatype Nexus Lifecycle, Snyk, OWASP Dependency-Check o GitHub Dependabot se encargan de esta tarea [87].

Cada metodología abordada exhibe ventajas y desventajas distintas [86]. En un banco central, apoyarse en un único método de prueba resulta claramente insuficiente. Una disciplina de DevSecOps madura debe articular los tres frentes para conseguir una defensa en profundidad, desde la concepción y el *build* (SAST y SCA) hasta la comprobación en tiempo de ejecución previa a la publicación y en preproducción (DAST). Con ello, se reducen los puntos ciegos, se mejora la priorización basada en el riesgo real y se somete a las aplicaciones que manejan información financiera sensible a una comprobación rigurosa antes y después del despliegue. Procediendo así, cualquier descubrimiento crítico detiene la compilación hasta que no sea solucionado, evitando que el código vulnerable avance hacia producción.

Otra práctica es emplear políticas como código (*Policy as Code*, PaC), las cuales constituyen reglas de resguardo expresadas como código declarativo, verificables automáticamente y que minimizan la posibilidad de que un error humano ocasione exposición. Motores como Open Policy Agent (OPA) contrastan cada modificación con normas corporativas y rechazan despliegues que incumplan [88].

Más allá de SAST, DAST y SCA, DevSecOps automatiza controles adicionales. El análisis de configuración de infraestructura como código (*Infrastructure as Code*, IaC) —es decir, la definición de infraestructura mediante plantillas versionadas como código— revisa Terraform, AWS CloudFormation y manifiestos de Kubernetes para detectar parámetros riesgosos con instrumentos como Checkov o kube-score. En paralelo, Amazon ECR incorpora inspección nativa (vía Amazon Inspector), Azure Container Registry se integra con Microsoft Defender for Cloud y Google Cloud dispone de Artifact/Container Analysis. Finalmente, los detectores de secretos (por ejemplo, Gitleaks) rastrean repositorios y commits en busca de credenciales, tokens y claves expuestas de forma accidental, reduciendo el riesgo de filtraciones previas al lanzamiento.

4.4.3 Análisis de contenedores e imágenes

En Google Cloud, Artifact Analysis [89] aporta visibilidad y control sobre la cadena de suministro de software al inspeccionar imágenes de contenedor alojadas en Artifact

Registry o Container Registry, extrayendo metadatos (paquetes, dependencias y licencias) e inspeccionando vulnerabilidades tanto en el ingreso (escaneo automático al subir la imagen) como de forma continua (revisión periódica de imágenes ya analizadas) y bajo demanda. El servicio reporta CVE, CVSS, paquetes afectados, posibles correcciones y una gravedad efectiva derivada de la fuente pertinente. En suma a ello, puede interrumpir compilaciones cuando una política de listas permitidas queda vulnerada, impidiendo la promoción de artefactos con riesgo conocido. Como complemento, Binary Authorization impone políticas de despliegue a través de pruebas y procedimientos de validación continua: solo las imágenes que cumplen los criterios preestablecidos avanzan a ejecución [89]. Por último, la revisión en segundo plano corrobora que los *pods* activos siguen alineados con las reglas, reduciendo la probabilidad de introducir software no autorizado o con defectos en entornos productivos.

4.4.4 Caos como prueba continua de confiabilidad en CI/CD

La ingeniería del caos (*chaos engineering*) induce fallas controladas con el fin de examinar —de manera sistemática— la robustez de sistemas distribuidos antes de que un incidente real afecte a los usuarios [90]. Su metodología arranca con la definición de un estado estable (*steady state*) como salida cuantificable del servicio; posteriormente, se formula una hipótesis sobre la conservación de dicho estado frente a perturbaciones realistas y se intenta refutarla mediante condiciones adversas tales como caídas de instancias, pérdidas de red, picos de CPU o degradación regional [90]. Ante variaciones apreciables del estado estable, se identifican fragilidades y se prioriza su remediación. Por lo tanto, integrar el caos en CI/CD transforma la confiabilidad en un filtro de calidad equiparable a las pruebas unitarias o de integración.

En la nube pública, los principales proveedores ofrecen plataformas gestionadas para ensayar perturbaciones de manera segura. Azure Chaos Studio [91] permite orquestar experimentos sobre recursos de Azure —máquinas virtuales, redes y servicios PaaS— a través de bibliotecas de fallas, recolección de métricas integrada y control fino del radio de explosión para limitar el alcance del experimento y ampliar gradualmente la cobertura.

En AWS, el Fault Injection Service (FIS) habilita la inyección de fallas sustentadas en los principios del caos [92]: interrupciones de instancias, degradación de EBS, alteraciones de red, afectación de nodos de Amazon EKS o averías en aplicaciones sin servidor, con mecanismos de seguridad y condiciones de detención para abortar si se supera un umbral fijado. Adicionalmente, el CSP suministra instrucciones para automatizar experimentos en pipelines CI/CD.

Con fundamento en lo anterior, una implantación rigurosa exige [93] [94]: (a) hipóte-

sis explícitas vinculadas a los objetivos de nivel de servicio (*Service Level Objectives*, SLO) y a los presupuestos de error (*error budgets*) —por ejemplo, una disponibilidad del 99,9 % delimita la tolerancia a fallas dentro de una ventana temporal—; (b) un radio de explosión (*blast radius*) acotado, junto con mecanismos de reversión confiables —paradas inmediatas y *rollbacks*— para evitar impactos indeseados en los ecosistemas; (c) observabilidad integral —métricas, registros y trazas— que permita contrastar la hipótesis con evidencia empírica; y (d) criterios de aprobación del pipeline condicionados a la conservación del estado estable.

Algunas buenas prácticas para aplicar la ingeniería del caos, enfocadas en bancos centrales y cargas críticas, se explican a continuación [90]:

1. **Diseño como código**: versionar los experimentos junto al despliegue y asociar cada ensayo a un riesgo concreto (por ejemplo, caída del plano de control de Kubernetes, pérdida de conectividad a KMS/HSM, *timeouts* en APIs interbancarias).
2. **Entornos y progresión**: iniciar en *staging* con tráfico sintético, luego avanzar a *canary release* en producción cuando el estado estable logre los rangos pactados y el presupuesto de error no se consuma en su totalidad. Asimismo, escalar el alcance de forma gradual, priorizando las dependencias críticas.
3. **Métricas de salida del pipeline**: instrumentar el tiempo medio de detección (MTTD) bajo experimento, variación de SLO durante la perturbación, tasa de reversión, tiempo de conmutación hacia la región alternativa y latencia p95/p99 en rutas transaccionales. Estas señales alimentan tableros SRE y decisiones de liberación.
4. **Gobernanza**: conservar un listado de fallas autorizado por cada riesgo; aplicar el mínimo privilegio en los permisos de inyección; registrar evidencias por *release* en bitácoras inmutables; y detener el despliegue mediante compuertas cuando se superen límites de SLO o del presupuesto de error.

4.4.5 Centro de mando de seguridad (Security Command Center)

SCC es la plataforma unificada de Google Cloud para visibilidad de riesgo y gobierno técnico, la cual consolida hallazgos procedentes de servicios nativos e integraciones de terceros, correlaciona señales y prioriza remediaciones [83]. Además, otorga detección de debilidades de parametrización, exposición involuntaria de recursos, credenciales filtradas y vulnerabilidades conocidas, además de seguimiento de conformidad frente a marcos como NIST, HIPAA, PCI-DSS y CIS. Asimismo, ofrece capacidades para reconocer y contener actividad maliciosa y herramientas de postura para definir políticas, eliminar permisos excesivos y vigilar cambios en ajustes críticos. En materia de datos, habilita residencia por región y exportación de eventos a BigQuery o Pub/Sub

para analítica avanzada y automatización. En el propio SCC, Web Security Scanner rastrea aplicaciones desplegadas en App Engine, GKE o Compute Engine, identificando fallas frecuentes (XSS, inyección SQL y otras del OWASP Top 10) para cerrar brechas con antelación al despliegue a producción [83].

5 Respuesta a incidentes y resiliencia operativa organizacional

5.1 Visibilidad, monitoreo y telemetría centralizada

5.1.1 Integridad y completitud de los logs

A fin de detectar y responder a amenazas en la nube, las entidades financieras requieren una visión completa de sus plataformas mediante registros centralizados y observabilidad consistente. Un desafío recurrente es la completitud de los eventos disponibles frente a entornos locales: en IaaS públicos el cliente instrumenta el sistema operativo, pero la capa de virtualización (hipervisor) queda bajo dominio del proveedor26. Por ende, ciertos sucesos que serían visibles a escala local (como señales de hardware o del propio hipervisor) no se exponen de forma directa. Para mitigar esa brecha, resulta esencial habilitar la totalidad de los servicios nativos de auditoría —AWS CloudTrail, Azure Monitor y Google Cloud Audit Logs— y pactar contractualmente el acceso a evidencias críticas durante investigaciones.

Como primer hito, conviene inventariar sistemas y aplicaciones que emiten trazas relevantes (capa de red, *kernel*, servicios, planos de administración o API) y definir los eventos mínimos por cada fuente de acuerdo con casos de uso de seguridad y requisitos de auditoría. En suma a ello, la retención debe alinearse con políticas internas y mandatos del sector financiero, puesto que los valores por defecto del proveedor suelen ser limitados. Puntualmente, las bitácoras deben reflejar puntos finales de API, autenticación y autorización de usuarios, detalles de solicitud/respuesta e IPs de origen [95]. Asimismo, se requiere trazabilidad detallada de actividades de administración, consulta de información sensible y documentación de operaciones de procesamiento. Dichos registros han de protegerse con cifrado, controles de privilegio y enmascaramiento, evitando exposiciones innecesarias durante su ciclo de vida [95].

En escenarios híbridos, lograr una vista unificada de eventos locales y en la nube es prioritario. No basta con recolectar, sino que es imprescindible correlacionar y normalizar

formatos heterogéneos para cimentar un panorama holístico de la postura de seguridad, reducir puntos ciegos y sostener procesos de auditoría y respuesta a incidentes con indicativos consistentes y oportunos [95].

La Figura 5.1 organiza las fuentes comunes de recopilación de telemetría en plataformas en la nube:

Registros del plano de gestión	Registros de servicio	Registros de recurso	Herramientas en la nube
• Fuente crítica dada la importancia de proteger el plano de gestión.	• Pasarela API: registros de acceso. • Almacenamiento: registros de acceso. • Red: registros de flujo de la VPC. • Función/sin servidor: registros de actividad. • Equilibrador de carga en la nube: registros de actividad. • Servidor de nombres de dominio (DNS, por sus siglas en inglés) en la nube: registros de consulta. • WAF/cortafuegos en la nube: registros de actividad.	• Carga de trabajo: registros de instancias y máquinas virtuales. • Registros de cambios de configuración. • Registros de invocación de funciones en la nube. • Registros de transacciones de bases de datos. • Registros de acceso a archivos de almacenamiento de objetos. • Registros de instantáneas e imágenes (almacenamiento en bloque).	• CSPM. • CASB. • Plataforma de protección de aplicaciones nativas de la nube (CNAPP, por sus siglas en inglés). • SSPM. • DSPM. • Análisis IAM. • Detección y respuesta en la nube.

Figura 5.1: Fuentes comunes de recopilación de telemetría en plataformas en la nube. Fuente: *Protección de los servicios de nube pública ante amenazas de ransomware* [96].

5.1.2 Recolección y análisis centralizado de registros

La centralización de registros en el ecosistema de nube constituye un pilar para la vigilancia continua y la gobernanza del riesgo. En entidades financieras, lo habitual es volcar los eventos procedentes de los principales servicios de nube en una plataforma corporativa SIEM y correlacionarlos con telemetría on-premise. Los proveedores actuales aportan capacidades avanzadas de monitoreo y asociación que antes queda-

ban reservadas a organizaciones con infraestructuras muy maduras: a partir de feeds de inteligencia de amenazas, técnicas UEBA (*User and Entity Behavior Analytics*) y avisos de configuración insegura, es posible revelar patrones anómalos —como actividad irregular de cuentas con privilegios elevados o provisión inusual de recursos— con un esfuerzo operacional acotado [97].

En paralelo, diversas instituciones diseñan arquitecturas de logging federado, donde consolidan eventos de múltiples nubes y del centro de datos local en un único repositorio. Tal enfoque amplía la perspectiva y expone conductas maliciosas que, en silos independientes, pasarían inadvertidas. En adición a los logs tradicionales, en la nube adquieren relevancia fuentes de observación poco convencionales: alertas por discrepancias en la facturación, notificaciones nativas del proveedor e inteligencia enriquecida de terceros.

En cuanto a funcionalidades, las plataformas SIEM concentran, enriquecen y normalizan eventos de seguridad de un amplio espectro de fuentes, desde equipamiento de red y servidores hasta servicios administrados y aplicaciones críticas [98]. Su utilidad principal es consolidar cronologías históricas con alertas en tiempo casi real, estableciendo vínculos que permiten reconocer anomalías relevantes o comportamientos fuera de lo habitual en la infraestructura tecnológica [97].

Los SIEM tradicionales, concebidos para despliegues locales, tienden a revelar limitaciones frente al volumen masivo y la velocidad de los registros en la nube, lo que ocasiona elevados costos y zonas de opacidad en la visibilidad [98]. En contraste, las soluciones nativas con capacidades SIEM/SOAR (por ejemplo, Microsoft Sentinel o Google Security Operations) se distinguen por su escalabilidad elástica, la automatización avanzada [99] y la integración orgánica con servicios como AWS CloudTrail, Azure Monitor o Google Cloud Audit Logs. Tales herramientas no solo exploran de manera automática las fuentes configuradas, sino que también ejecutan *playbooks* de remediación orquestada, habilitan retenciones prolongadas con costes optimizados y amplían la capacidad investigativa del SOC [98].

En Sentinel, la ingestión mediante conectores preconstruidos se compagina con reglas basadas en lenguaje de consultas (*Kusto Query Language*, KQL) y mapeos contra MITRE ATT&CK para priorizar hallazgos, condensar alertas en incidentes y mejorar el panorama defensivo. Adicionalmente, otorga retenciones prolongadas con niveles de costo diferenciados, inteligencia de amenazas y ejecución de playbooks mediante Logic Apps para remediaciones coordinadas [100]. Sobre este sustrato, la IA perfila patrones, fija líneas base dinámicas y resalta comportamientos atípicos [97], permitiendo inspeccionar cada solicitud según la identidad, el contexto y el estado del dispositivo, en línea con el enfoque de confianza cero. Para los bancos centrales, tal habilidad es valiosa frente a riesgos internos, puesto que las cuentas con privilegios legítimos pueden convertirse en vectores de exfiltración de contenido sensible o abuso accidental.

5.1.3 Controles complementarios y su optimización

La consolidación de barreras de contención avanzadas se ha convertido en una condición esencial para que las instituciones financieras fortalezcan su postura de defensa y conserven una visibilidad completa sobre sus operaciones digitales. En complemento a la extensión de las plataformas SIEM tradicionales hacia arquitecturas híbridas y soluciones nativas, las instituciones despliegan herramientas de detección y respuesta en puntos finales (*Endpoint Detection and Response*, EDR) sobre máquinas virtuales y cargas de trabajo en la nube, instalando agentes capaces de inspeccionar procesos, memoria y operaciones del sistema [97]. Tal enfoque reproduce e incluso extiende la visibilidad que antes se limitaba a entornos locales, pero introduce desafíos adicionales, como cubrir instancias efímeras o infraestructuras con autoescalado dinámico. A pesar de dichas dificultades, la instalación de EDR en la nube resulta indispensable para interrumpir actividades maliciosas, desde infecciones de *malware* hasta movimientos laterales en servidores virtualizados.

Al mismo tiempo, los controles de red y perímetro se rediseñan para acoplarse a un esquema virtualizado. En particular, se parametrizan firewalls virtuales, grupos de seguridad, WAF y sistemas IDS/IPS en la nube, que actúan como barreras para inspeccionar y filtrar tráfico en tiempo real. En suma a ello, la microsegmentación y las arquitecturas de confianza cero refuerzan la resiliencia al confinar cargas sensibles en dominios aislados y acotar cualquier propagación de amenazas hacia activos esenciales.

Finalmente, Microsoft Sentinel, al integrarse de forma nativa con la plataforma XDR de Microsoft Defender, consolida telemetría y casos en un plano único que articula SIEM y XDR. Tal acoplamiento, reforzado por modelos de IA —desde priorización sustentada en riesgo hasta triaje asistido y *threat hunting* guiado— acelera el descubrimiento de comportamientos anómalos, depura el ruido, estandariza flujos de corrección y eleva la eficiencia operativa a gran escala [100].

5.2 Gestión y respuesta a incidentes en la nube

5.2.1 Playbooks y automatización de flujos

La respuesta a incidentes en la nube constituye un proceso estructurado que abarca la detección temprana, la evaluación del alcance, la contención de la amenaza y la posterior resolución con el objetivo de reducir al mínimo el impacto operativo y reputacional. Los incidentes más frecuentes en la nube abarcan la filtración de información sensible, el compromiso de cuentas privilegiadas, configuraciones erróneas en servicios de al-

macenamiento, ataques de denegación de servicio distribuida (DDoS), infecciones de malware o *ransomware* en máquinas virtuales, así como campañas de cryptojacking que explotan recursos de cómputo para minería ilícita [101].

Los planes de respuesta exigen una adaptación específica al contexto de nube, puesto que exhiben particularidades distintas a las de entornos locales [101]. En consecuencia, para los bancos centrales, confiar exclusivamente en manuales diseñados para infraestructuras tradicionales podría derivar en respuestas tardías o descoordinadas. En su lugar, los playbooks deben contemplar controles nativos como grupos de seguridad, segmentación granular mediante VPCs, mecanismos de contención orquestados a través de APIs y registros ajustados al plano de nube. Ejemplos concretos incluyen la exposición de datos en un bucket abierto, la explotación de vulnerabilidades en servicios gestionados o la propagación de ransomware en instancias híbridas.

Una práctica recomendable es elaborar tales planes con antelación y emprender simulacros periódicos, de modo que los equipos de seguridad se familiaricen con la secuencia de acciones y puedan perfeccionar tiempos de reacción [101]. En el ámbito financiero, los supervisores suelen vigilar la preparación de las entidades mediante ejercicios sectoriales de ciberresiliencia, donde se examina la rapidez con que los bancos pueden contener y recuperar la operatividad ante incidentes graves. Tales simulaciones, como las impulsadas por el BCE a través del TIBER-EU [102], afianzan la competencia técnica del personal y refuerzan la coordinación entre los diferentes actores del ecosistema financiero.

5.2.2 Coordinación con proveedores durante incidentes

En un escenario real sobre plataformas públicas, la conducción de incidentes exige un engranaje formal con el proveedor: canales de emergencia, procedimientos de escalamiento y apoyos técnicos preacordados. La CSA, a través del CIRF, subraya que los clientes deben negociar de antemano con el CSP las tareas de notificación, comunicación y apoyo durante la contingencia, así como la división precisa de funciones en concordancia con el modelo de responsabilidad compartida [2] [9]. Este marco también orienta sobre la selección de capacidades de los operadores de servicios en la nube, la preparación documental y los intercambios de información entre organizaciones para reducir riesgos sistémicos.

En el ecosistema de AWS, la coordinación se sustenta en equipos especializados y directrices operativas detalladas. La compañía publica guías que cubren el ciclo completo de un incidente —desde la preparación inicial hasta la contención, erradicación y recuperación— con recomendaciones sobre automatización, preservación de evidencias y prácticas forenses avanzadas [103]. A ello se añade el Customer Incident Respon-

se Team (CIRT), disponible de manera ininterrumpida, que brinda soporte en situaciones que afectan la capa de responsabilidad del cliente dentro del modelo compartido [104]. Para organizaciones con Enterprise Support, el servicio AWS Incident Detection and Response (IDR) elabora runbooks y planes específicos por carga, además de un acompañamiento preventivo y durante la interrupción. Paralelamente, el AWS Trust & Safety Center ofrece recursos dedicados para canalizar reportes relacionados con el uso indebido de componentes del inquilino en actividades maliciosas [105].

En Microsoft, el equipo Microsoft Incident Response otorga intervención especializada antes, durante y después del evento. En particular, combina investigación remota y presencial, coordinación con áreas de producto y socios estratégicos, así como la publicación de playbooks que organizan fases, hitos y acciones [106]. La recomendación operativa es escalar tempranamente a este grupo cuando se sospechen compromisos de alto impacto en Microsoft 365 o Azure, con el fin de acelerar la contención y la recuperación.

En Google Cloud se dispone de un formulario oficial para denunciar abusos en servicios como App Engine, Compute Engine, Cloud Storage, BigQuery, Cloud SQL o Cloud Datastore [107]. Asimismo, la plataforma mantiene la guía *Respond to abuse/misuse*, que expone prácticas recomendadas para actuar frente a incidentes frecuentes, como la exposición de claves de API, indicios de minería de criptomonedas o la presencia de malware en proyectos [107]. A esto se suma el servicio Mandiant Incident Response Services, parte del portafolio de Google Cloud Security Consulting, que ofrece asistencia experta en investigación, gestión de crisis y restauración de operaciones tras una intrusión [108].

Desde una perspectiva contractual, es indispensable consignar en los acuerdos con el proveedor aspectos primordiales como los tiempos y niveles de escalamiento [9], canales de comunicación fuera de banda, compromisos de acceso a logs en el plano de control del proveedor, apoyo durante la recopilación de evidencias y aclaraciones explícitas sobre el alcance del incidente (es decir, si afecta únicamente a un *tenant* o si deriva en consecuencias transversales a múltiples clientes). El CIRF subraya la necesidad de formalizar tales cláusulas y alinearlas con los marcos internos, evitando que los planes institucionales dependan de improvisaciones en medio de la crisis [2].

En términos operativos, resulta aconsejable preparar con anticipación un directorio de contactos verificados en el proveedor y en la entidad (disponibles 24/7), plantillas de casos de alta prioridad en el portal de soporte, matrices de decisión y mecanismos para canalizar hallazgos hacia las áreas legales y regulatorias. De manera adicional, en el ámbito del sector público financiero, suele ser obligatorio notificar al supervisor y coordinar con el operador para confirmar el perímetro del incidente [2].

La práctica recomendada consiste en activar de inmediato el canal de comunicación

con el CSP, compartir los hallazgos relevantes y solicitar colaboración en tareas puntuales. Esta aproximación reduce el tiempo de escalamiento y preserva la trazabilidad requerida para auditorías posteriores. En consecuencia, un trabajo contractual proactivo se convierte en un elemento esencial para mantener la colaboración fluida y prevenir disputas en escenarios de alta presión, impactando directamente en el tiempo medio de respuesta (MTTR) [101].

5.2.3 Análisis forense en entornos cloud

El examen forense constituye un pilar de la ciberresiliencia institucional: no solo habilita reconstrucciones fieles de lo sucedido tras un incidente, sino que sustenta informes regulatorios y eventuales actuaciones legales. A diferencia del escenario tradicional—donde el equipo de respuesta cuenta con proximidad física a servidores y soportes—, en la nube los datos residen en espacios administrados por el proveedor [109], lo que impone límites técnicos y procedimentales. En despliegues IaaS, se alude a la obtención de artefactos como instantáneas de volúmenes, volcados de memoria de instancias, trazas de actividad del plano de control (invocaciones de API) y registros de red. Por su lado, en PaaS/SaaS el foco recae en bitácoras de servicio y eventos de autenticación expuestos por el operador, dado que el cliente no controla el sistema operativo subyacente. El NIST codifica estas diferencias en la publicación SP 800-201, proponiendo arquitecturas y metodologías forenses acordes a los requerimientos de nube con lineamientos sobre preservación, cadena de custodia, temporalidad y validez probatoria. Asimismo, el informe NISTIR 8006 describe desafíos característicos del modelo de nube (multitenencia, volatilidad, jurisdicción e indicios distribuidos) [110].

Atendiendo tales consideraciones, las instituciones del sector financiero suelen adoptar prácticas como:

1. **Adquisición temprana y preservación**: en cuanto se confirma un evento, se crean instantáneas inmutables de los volúmenes afectados, se exportan registros de auditoría del plano de control y se resguardan artefactos en cuentas o proyectos aislados bajo políticas de retención y acceso restringido, minimizando el riesgo de rotaciones, sobrescrituras o manipulaciones. La guía *AWS Security Incident Response* recomienda centralizar soportes (por ejemplo, mover copias y logs a una cuenta de seguridad), definir listas de control de acceso estrictas y documentar cada paso para sustentar la cadena de custodia [103].
2. **Herramientas y habilidades especializadas**: Los equipos de respuesta en banca central requieren dominio de forense en la nube orientada a reconstruir hechos a partir de artefactos distribuidos. Ello implica operar utilidades capaces de: (i) extraer historiales de actividad administrativa y de API —por ejemplo, AWS Cloud-

Trail (historial de llamadas al plano de control), Azure Activity Log y Google Cloud Audit Logs—, (ii) consultar cronologías de configuración —AWS Config y Cloud Asset Inventory en Google Cloud y (iii) vincular trazas de red mediante VPC/NSG Flow Logs o Packet Mirroring para capturar tráfico de interés con fines de investigación. Por otro lado, dado que la evidencia puede repartirse entre regiones, cuentas o suscripciones, conviene normalizar la recopilación y retención: *organization trails* de CloudTrail, *aggregated sinks* en Google Cloud y arquitecturas de Log Analytics centralizadas en Azure simplifican la agregación transversal. Respecto a la preservación y cadena de custodia, resulta recomendable activar inmutabilidad en el almacenamiento (S3 Object Lock, Azure Blob Immutable Storage o GCP Bucket Lock) junto con políticas de retención acordes con requerimientos regulatorios. En cuanto a imágenes para análisis, la práctica forense en nube recurre a instantáneas de volúmenes (EBS, Managed Disks y Persistent Disk) y a *sandboxes* aislados para montar copias sin perturbar la producción.

3. **Procedimientos y playbooks en nube e híbridos**: Las fases clásicas de identificación, contención, erradicación, recuperación y lecciones aprendidas se enriquecen con actividades propias de entornos de nube. Inicialmente, es necesario catalogar con rapidez los recursos afectados (instancias, contenedores, funciones, cuentas y tenants). El etiquetado consistente y la historia de despliegues (por ejemplo, *drift* en CloudFormation, *deployment history* en Azure y *asset history* en Google) brindan visibilidad sobre cambios recientes y componentes sensibles. Posteriormente, en lugar de «desconectar un cable» para efectuar el aislamiento del elemento comprometido, se opta por la cuarentena lógica: mover instancias fuera de balanceadores de carga, restringir entradas/salidas con grupos de seguridad o NSG y cortar rutas mediante ACL/Firewall. Existen patrones automatizables sustentados en etiquetas y funciones sin servidor (Lambda, Logic Apps o Cloud Functions) u orquestación (Step Functions o Runbooks) para ejecutar acciones de instantáneas o cuarentena ante señales de riesgo [111].

5.3 Resiliencia y continuidad del negocio

Históricamente, el sector financiero ha desplegado planes de continuidad del negocio (*Business Continuity Plan*, BCP) y de recuperación ante desastres (*Disaster Recovery Plan*, DRP) de alta madurez. Con la migración hacia modelos de nube e infraestructuras híbridas, tales esquemas se reconfiguran para aprovechar redundancias multizona y topologías activo-activo, al tiempo que atenúan riesgos emergentes, como la concentración en un proveedor único o la dependencia de una región concreta. Dicha adaptación exige gobernanza técnica rigurosa, pruebas periódicas de conmutación por error

(*failover*) y métricas formales de recuperación. En suma a ello, ciertas instituciones incorporan enfoques multinube para diversificar la exposición y reforzar la residencia de datos conforme a la jurisdicción aplicable. Así, el cambio de enfoque es claro: ya no basta con restablecer servicios luego de un evento adverso, sino que la expectativa es sostener, de forma continua, un nivel mínimo aceptable de operación.

5.3.1 Copias de seguridad y restauración en la nube

El resguardo periódico de datos prioritarios constituye un pilar de resiliencia frente a ransomware y fallas catastróficas. En entornos de nube, las instituciones financieras formulan estrategias contemporáneas de respaldo que comprenden: automatización de instantáneas de bases de datos y volúmenes de bloque, replicación entre dominios geográficos y resguardo en entornos aislados [2]. Un principio ampliamente aceptado es la regla 3-2-1: tres copias, almacenadas en dos tipos de medios, con una de ellas fuera del sitio principal [112]. Lo anterior suele traducirse en mantener duplicados en una región alternativa o incluso en un operador o plataforma distintos.

El aislamiento de las copias de seguridad reduce de manera sustancial el alcance de posibles intrusiones. Las directrices de seguridad —como las emitidas por CISA en su iniciativa *StopRansomware*— recomiendan conservar determinados respaldos desconectados de la red principal y cifrados, tal que un atacante no logre perturbar ni eliminar la totalidad del acervo destinado a la recuperación [113]. De hecho, diversas campañas de ransomware buscan comprometer los instrumentos de respaldo mediante sustracción de credenciales o explotación de vulnerabilidades, con la intención de obstaculizar la restauración. Ante ello, resultan prudentes medidas como depósitos de solo lectura, almacenamiento inmutable bajo el modelo WORM o bóvedas ofertadas por los operadores que impiden alteraciones durante un periodo temporal preestablecido. En estas últimas, la implementación debe administrarse con cautela, verificando que las políticas de retención se acoplen a los requerimientos normativos y examinando con rigor los costos asociados [113].

Además del resguardo de datos, conviene preservar configuraciones y código fuente. Las organizaciones mantienen imágenes doradas (*golden images*, es decir, plantillas base estandarizadas de sistemas y aplicaciones) actualizadas para sus plataformas de misión, así como infraestructura como código (plantillas declarativas y guiones de despliegue), custodiadas en repositorios independientes y desconectados de la red [113]. Mediante tales recursos, resulta factible restaurar servicios en una cuenta nueva o en otro proveedor dentro de plazos acotados, con reducción del RTO. A razón de esto último, se debe reservar capacidad de cómputo —en instalaciones propias o en otra nube— para absorber cargas si la plataforma principal falla [113].

Se sugiere que dichas imágenes y guiones se sometan a pruebas periódicas en entornos limpios, a fin de corroborar que los respaldos mantienen coherencia y que los procedimientos de retorno al servicio se desarrollan según lo esperado [114].

5.3.2 Plan de recuperación ante desastres (DRP)

Un DRP consiste en una estrategia documentada para restaurar sistemas de TI críticos, datos y operaciones después de un evento disruptivo [115]. Concretamente, se enfoca en reducir el tiempo de inactividad y salvaguardar los activos sensibles, documentando para ello las metodologías de recuperación, los requerimientos de copia de seguridad y los roles y responsabilidades implicados [115].

Las prácticas de DRP contemporáneas se han refinado gracias a la elasticidad del modelo de nube: numerosas instituciones emplean esquemas *multi-AZ*, las cuales consisten en desplegar cargas de trabajo de misión en varias zonas de disponibilidad independientes dentro de la misma región del proveedor [116], de modo que la interrupción de un centro de datos no afecte la continuidad del servicio. Dicho enfoque atiende contingencias localizadas, por lo que para riesgos de mayor alcance se recurre a diseños multirregionales [116], que en algunos casos alcanzan un RTO igual a cero para determinados componentes [114].

Algunas entidades contemplan arquitecturas multinube con el fin de reducir la dependencia de un único proveedor (*vendor lock-in*) y la concentración de riesgo. Procediendo así, es viable planificar respaldos entre nubes ante impactos generalizados sobre un operador concreto [113]. No obstante, dicha aproximación introduce complejidad y costos adicionales, por lo que suele priorizarse, en primera instancia, el robustecimiento de la resiliencia dentro del proveedor principal antes de ampliar a una segunda plataforma.

Un componente cardinal del DRP consiste en establecer para cada servicio esencial los Objetivos de Tiempo de Recuperación (RTO) y los Objetivos de Punto de Recuperación (RPO), en consonancia con el apetito de riesgo y los compromisos con clientes y contrapartes. En la nube, se ofertan distintas estrategias para alcanzar RTO/RPO exigentes: reserva activa parcial (*warm standby*), donde un ecosistema secundario se mantiene mínimamente sincronizado y listo para escalar durante la conmutación por falla [117]; piloto luminoso (*pilot light*), en el que los recursos esenciales permanecen preconfigurados y se activan ante la contingencia [117]; o despliegues activo/activo en múltiples sitios [117].

Por último, el pilar de fiabilidad de AWS subraya la importancia de distribuir cargas de trabajo en múltiples ubicaciones independientes y de automatizar los procesos de restauración de elementos restringidos a una única locación [118].

El enfoque descrito supera con holgura las prestaciones tradicionales de recuperación ante desastres en entornos locales, donde las limitaciones de hardware y la dependencia de infraestructuras físicas restringen la continuidad operativa a escenarios limitados y poco escalables. Para los bancos centrales, la posibilidad de apoyarse en la red global de centros de datos en la nube representa un salto cualitativo hacia niveles de resiliencia inéditos, en los que la redundancia geográfica, la elasticidad de recursos y la automatización redefinen los estándares en el sector.

6 Fortalecimiento de capacidades y hoja de ruta

6.1 Plan de implementación por fases en seguridad en la nube

La elaboración de una hoja de ruta orientada al fortalecimiento de la protección en infraestructuras de nube demanda un ejercicio previo de autodiagnóstico, un proceso riguroso de jerarquización de iniciativas y una ejecución progresiva segmentada por fases. A continuación, se esbozan los elementos fundamentales para estructurar este trayecto transformacional:

1. **Diagnóstico inicial y definición del estado objetivo**: El primer paso consiste en realizar una evaluación exhaustiva del estado actual de exposición frente a amenazas en la nube, identificando las deficiencias estructurales, vectores de riesgo prevalentes y puntos de control ausentes o debilitados [119]. A partir de dicha caracterización, se debe proyectar un escenario deseable (estado objetivo) en términos de gobierno institucional, mecanismos de protección y configuración arquitectónica de los entornos de nube. Tal análisis debe fundamentarse en marcos de adopción de servicios en la nube, tales como los propuestos por AWS, Microsoft Azure o GCP, así como en lineamientos internacionales reconocidos, con el propósito de establecer un punto de referencia sobre el grado actual de madurez organizacional y determinar el trayecto de transformación requerido [96]. La participación simultánea de unidades tecnológicas y áreas funcionales no especializadas es indispensable, a fin de alinear los objetivos de protección con los fines misionales de la institución.
2. **Jerarquización de líneas de acción conforme al perfil de riesgo institucional**: Con fundamento en los hallazgos del diagnóstico, corresponde ordenar las medidas a desplegar conforme a criterios de impacto, urgencia y factibilidad. Debe priorizarse la incorporación de controles que mitiguen amenazas de alto nivel —por ejemplo, mecanismos avanzados de protección de información clasificada, con-

trol de accesos privilegiados o plataformas integradas de vigilancia— así como aquellas acciones cuyo efecto contribuya significativamente al fortalecimiento de la postura defensiva. Asimismo, resulta indispensable atender las obligaciones impuestas por las autoridades competentes del sector financiero, especialmente aquellas relacionadas con la supervisión de terceros proveedores de servicios en la nube y con la gestión de funciones críticas externalizadas.

Adicionalmente, la secuenciación debe considerar la asignación realista de recursos institucionales, tanto en términos de personal capacitado como de disponibilidad presupuestaria. Se aconseja iniciar con iniciativas de bajo esfuerzo y alto impacto (*quick wins*) que generen confianza y demuestren resultados tangibles en etapas tempranas (por ejemplo, la utilización de técnicas de cifrado robustas para datos en tránsito y reposo, así como la activación obligatoria de MFA en perfiles administrativos), para posteriormente avanzar hacia componentes de mayor complejidad. Una directriz eficaz consiste en alinear el despliegue con el apetito de riesgo previamente declarado por la organización, priorizando la atención de brechas consideradas intolerables de acuerdo con su matriz de riesgos.

3. *Arquitectura de decisiones y órganos de supervisión*: Es imprescindible concebir un entramado funcional que habilite el seguimiento metódico del progreso alcanzado en cada etapa del itinerario y la adopción de determinaciones estratégicas en función de los hallazgos. Para tal fin, conviene asignar competencias claramente delimitadas en materia de dirección de iniciativas de nube, las cuales se concentren en un comité cuya misión consista en examinar los avances logrados, descubrir nuevos factores de exposición, detectar desviaciones relevantes y reordenar prioridades cuando las circunstancias así lo exijan. Dicho órgano deberá, además, propiciar la coherencia entre las directrices orientadas a ambientes virtualizados y el acervo normativo institucional vigente en protección digital y gestión integral del riesgo [96].

Con base en lo anterior, se propone articular un plan de implementación estructurado en bloques temporales claramente delimitados, cada uno con productos verificables, actores institucionales responsables y cronogramas predefinidos, tal que cada segmento temporal corresponda con objetivos funcionales precisos. Resulta recomendable que este itinerario se articule con los programas institucionales vinculados a la transformación digital y a la planificación de recursos tecnológicos.

Una ejecución escalonada, sustentada en ciclos iterativos y retroalimentación pragmática, facilita la adecuación progresiva de los entornos y disminuye los efectos disruptivos sobre los procesos centrales [10]. Asimismo, el pilar de seguridad del CAF de AWS propone una trayectoria evolutiva estructurada por fases [8], cuya intención es acompañar a las organizaciones en su tránsito desde prácticas básicas hacia arquitecturas de protección altamente adaptativas y sostenidas por inteligencia contextual. Durante

la fase de inicio, se prioriza la alineación entre el perfil de riesgo y los objetivos institucionales, la delimitación clara de funciones mediante modelos de responsabilidad y la concordancia con principios de seguridad desde etapas tempranas del diseño [8]. En la fase intermedia, se introduce la iteración metódica de controles, la adopción de mecanismos modernos de autenticación adaptativa, la codificación de políticas y la automatización progresiva de salvaguardas [8]. Finalmente, en la fase avanzada o de excelencia, la entidad aprovecha el catálogo de soluciones nativas para desplegar mecanismos inteligentes de priorización, como el uso de analítica predictiva e IA, integrar prácticas de PaC o similares y afianzar la comunicación estructurada del riesgo entre unidades funcionales [8].

De acuerdo con los lineamientos descritos, se propone una tabla adaptada que articula fases funcionales con componentes prioritarios y consideraciones clave:

Tabla 6.1. Fases para una adopción segura de computación en la nube.

Etapa	Elementos clave
Fase 1: Fundamentos	Diagnóstico inicial de exposición, diseño de gobierno institucional, administración de identidades (IAM), MFA y clasificación de activos sensibles.
Fase 2: Protección reforzada	Prácticas *DevSecOps*, seguridad en procesos CI/CD, cifrado sólido de datos, protección de cargas de trabajo y detección de secretos en flujos automatizados.
Fase 3: Automatización adaptativa	Madurez en arquitectura de confianza cero, detección avanzada de amenazas, respuesta orquestada, administración de accesos con privilegios temporales (*just-in-time*), endurecimiento de entornos (*hardening*) y elasticidad defensiva.
Fase 4: Innovación con gobernanza inteligente	Protección de entornos SaaS, APIs y arquitecturas *serverless*, controles en soluciones con IA, gestión de aplicaciones mediante *SSPM* e integración de marcos SASE.

6.1.1 Referentes funcionales para la reducción de riesgos en la nube

En el marco del fortalecimiento institucional de la seguridad en la nube, resulta pertinente integrar un compendio de controles, marcos metodológicos y buenas prácticas reconocidas que contribuyan a reducir la exposición ante vectores de ataque relevantes, como el ransomware o el abuso de interfaces expuestas. La Tabla 6.2 sintetiza las principales recomendaciones organizadas conforme al Marco de Ciberseguridad 2.0 del NIST, con base en el documento técnico *Protección de los servicios de nube pública*

ante amenazas de ransomware - Mejores Prácticas en Ciberseguridad [96]. Tal desglose funcional ofrece una referencia estructurada para orientar la formulación de hojas de ruta, la planificación por fases y la alineación de medidas con marcos regulatorios vigentes en el sector financiero.

Tabla 6.2: Mecanismos y herramientas para reducir el riesgo cibernético para cada categoría del NIST CSF.

Función (NIST CSF 2.0)	Temas abordados	Controles / recomendaciones clave
Gobernar	Enfoque organizacional de la nube	**Estrategia de gestión de riesgos:** Apetito de riesgo, supuestos, tratamiento (aceptar/rechazar/transferir/mitigar), mapeo de requisitos de partes interesadas, plan de salida y rol del DPO. Además, evaluar seguro cibernético y construir una función GRC en nube.
		Política: La política corporativa incluye un capítulo para la nube y criterios de medición (KCI/KGI/KPI/KRI/OKR) con periodicidad y responsables.
		Seguridad de la cadena de suministro: Criterios de selección del CSP como certificaciones, soberanía/portabilidad de datos, recursos que soporten la investigación y revisión de cumplimiento y acceso al equipo de seguridad del CSP.
Identificar	Inventario y evaluación de activos cloud	**Mapeo de activos:** Elaborar inventario (información, HW/SW, servicios, regiones o APIs) y diagramas de flujo de datos/procesos; asignar sensibilidad/criticidad según BIA; activar logs de VPC, CSPM/DSPM para visibilidad y *shadow IT; d*efinir asociaciones con IAM (*BYOD, linked, hybrid*) y controles para detectar inactivos o maliciosos.
		Evaluación de riesgos: TTP, detección de vulnerabilidades en CSP y CSC, CTI y PIA.
		Aspiración de mejora continua: Ejercicios periódicos para medir competencia y preparación**.**
Proteger	Acceso, cifrado, arquitectura y Zero Trust	**Identidad y acceso:** MFA resistente a *phishing*, acceso condicional (contexto/ubicación, postura del dispositivo, riesgo en tiempo real), PoLP/SoD, CIEM, políticas de recursos que eviten bypass de IAM, *just-in time admin* y *dual control*, cuentas *break-glass* restringidas y monitorizadas. Para secretos, almacenamiento en KMS/HSM, gestión del ciclo de vida y *secret detection* en CI/CD.
		Sensibilización y formación debe cubrir superficie de ataque y configuraciones seguras exigidas.

		Resiliencia infraestructura: Zero Trust por pilares (identidad, dispositivos, redes, apps, cargas y datos), jerarquía de recursos (*landing zones,* IaC, *policy-as-code*, evitar eliminación o modificación de recursos, restringir creación y transferencia, eludiendo el paso por Internet (AWS PrivateLink). - **SaaS sobre CSP**: aislar inquilinos, WAF/RASP/WAAP, SSPM como control compensatorio. - **Malware:** CWPP en *gateways* y recursos; respuesta a entornos efímeros y *roaming*; CDR en entrada/salida. - **DDoS**: respuesta a ataques volumétricos, de protocolo y aplicación, monitoreo permanente, CDN y *autoscaling*. - **Segmentación:** *deny-by-default*, NACL/SG, VXLAN/Geneve, NGFW central y *port mirroring*. - **Gestión de cambios:** *baselines* (CIS Benchmark), AWS Config/equivalentes para *drift*, IaC para reconstrucción rápida, política de contraseñas robusta, bloqueo de RDP/SSH (preferir *Bastion Host*). - ***Serverless***: documentar ciclo de vida, aplicar *least privilege*, controlar dependencias y serialización y garantizar cobertura en gestión de vulnerabilidades. - ***DevSec***: *secure by design/default*, OWASP ASVS/MASVS, SBOM/SaaSBOM integrado a gestión de vulnerabilidades. - **IA**: Cubrir todo el ciclo de vida, AIBOM e integración en programa de vulnerabilidades.
		Seguridad de la plataforma: - **API**: mTLS para M2M, MFA para H2M; hardening de tokens, *throttling*, *rate limiting*, *geo-fencing, fine-grained access, logging,* SAST/SCA/DAST/IAST y revisiones de código. - **Servicio de acceso seguro Edge** (SASE) como evolución de VPN. - **Mensajería SaaS:** DMARC/BIMI, control de Pub/Sub y listas de aplicaciones/servicios. - **On-premise:** lista de ataques frecuentes; CASB en línea con inspección TLS, descubrimiento P2P/-Web3, UEBA, DLP y RBI.

		Aseguramiento de la información: cifrado, DLP apoyado en gobernanza de datos, *privacy-enhancing technologies* y minimización de datos; - **Backups**: pruebas de restauración completa en sandbox, retro-hunting de malware, detección anomalías, almacenamiento protegido (WORM) con aprobadores independientes, retention-lock y versionado de copias. - **Replicación**: Asincrónica, otra región/CSP, versiones.
Detectar	Visibilidad y monitoreo en la nube	**Monitoreo continuo**: Activación de telemetría, integrar CSPM/DSPM, envío temprano a SIEM/*data lake*, retención acorde, asimilar lag operativo (tasa de llegada de registros es menor que la de alertas), normalización y mapeo de esquema para multinube, superficie de ataque y configuraciones e integridad de archivos.
		Análisis de incidentes anormales: IA para priorización y triaje, SOAR, CTI para respuesta rápida y *situational awareness* y reglas mínimas de anomalías: volumen/tipo de tráfico, consumo financiero, CRUD, cambios en *backups*/destinos e IAM (creación, localización o bloqueos).
Responder	Mitigación de incidentes y malware	**Gestión de incidentes:** forense en nube (logs de activos efímeros antes de apagados y etiquetas para investigación), evitar que políticas bloqueen forense, apoyo externo con SLA, ejercicios, cobertura híbrida/multinube y capacidades de cadena de custodia.
		Informes y comunicación: Obligaciones regulatorias (país de operación y de datos); notificación al CSP (posibles bloqueos por riesgo a terceros) y canales alternos.
		Mitigación del impacto: SOAR o funciones *serverless* para procesos de respuesta básicos.
Recuperar	Restauración y servicios críticos	**Ejecución del plan de recuperación**: BCP/DRP con conciencia de nubec ensayo “from-scratch” y operando desde el nuevo entorno, *backups* probados y asegurados, IaC y *drift* para reconstrucción.
		Comunicación en recuperación: Actualizaciones periódicas a *stakeholders,* tableros en CSP para seguimiento del progreso y referencias a guías (NIST/CSA/ENISA).

Marcos de referencia	Lineamientos que guían todas las categorías	MITRE D3FEND, *CSA Cloud Controls Matrix*, OWASP ASVS/MASVS y normativas de organismos como NIST, CISA, ISO/IEC y DISA.

6.1.2 Marco normativo y alineación con mandatos regionales

El plan progresivo debe sustentarse sobre una arquitectura institucional coherente y actualizada. El entramado regulador en Latinoamérica en torno a la nube y los riesgos derivados de terceros ha evolucionado gradualmente hacia marcos que exigen responsabilidad contractual, auditoría de servicios externalizados y mecanismos de verificación de seguridad.

En Brasil, la Resolución CMN 4893/2021 impone requisitos a entidades financieras para que los contratos con proveedores de servicios de datos, almacenamiento y computación en la nube contengan cláusulas relativas a confidencialidad, auditoría, monitoreo, ubicación de servicios y derechos de extracción de datos[120]. En Chile, la Norma de Externalización de Servicios propuesta por la CMF prescribe criterios de materialidad y criticidad de funciones delegadas [121], mientras que el Capítulo 20-7 de la regulación bancaria modera la contratación de prestadores externos para servicios de computación en la nube en entidades del ámbito económico [122].

En Colombia, los *Lineamientos de seguridad de la información para el uso de nube*, emitidos por el Ministerio de Tecnologías de la Información y las Comunicaciones, delinean conceptos clave como la delegación de responsabilidades, la clasificación de datos, evaluación de riesgos y las medidas aplicables a los servicios externalizados [123]. En otros países de la región, como México, se han publicado cláusulas generales para la contratación de servicios TIC que mencionan restricciones para procesos sensibles sobre nubes públicas e imponen requerimientos adicionales para terceros en el sector financiero [124].

6.2 Métricas e indicadores clave en la nube (KPI/KRI)

El diseño de un sistema de monitoreo eficaz para ambientes de nube debe contemplar dos categorías de métricas complementarias: los indicadores clave de riesgo (KRI) y los indicadores clave de desempeño (KPI). Los primeros constituyen métricas anticipatorias, concebidas para revelar señales tempranas sobre condiciones que podrían derivar en escenarios de exposición no tolerables. Por ejemplo, un alto porcentaje de vulnerabilidades sin corregir o una concentración excesiva de accesos con privilegios elevados puede indicar una tendencia ascendente de riesgo latente [125].

En contraste, los KPI presentan una orientación retrospectiva, midiendo la eficacia de un programa de protección con base en resultados observables [125]. Algunas métricas relevantes en este dominio son el tiempo promedio de respuesta ante incidentes, la tasa de ejecución de actualizaciones críticas, la cobertura de capacitaciones en seguri-

dad entre los empleados y el porcentaje de intentos de intrusión frustrados [125].

El enfoque más avanzado para capturar tales parámetros se sustenta en esquemas de monitoreo continuo de controles (*Continuous Controls Monitoring*, CCM), los cuales aportan visibilidad casi en tiempo real respecto al comportamiento de los controles implementados, detectando tanto desviaciones (KRI) como niveles de cumplimiento (KPI) [125]. Para los bancos centrales, tal trazabilidad resulta fundamental no solo para preservar sus activos estratégicos, sino también para anticiparse a perturbaciones sistémicas que comprometan la estabilidad regional.

La Tabla 6.3 describe los KPI y KRI sugeridos.

Tabla 6.3: Indicadores de desempeño (KPI) y riesgo (KRI) en seguridad cloud.

Categoría	Tipo	Métrica	Propósito
Vulnerabilidades y configuración	KRI	Porcentaje de vulnerabilidades críticas sin parchear.	Alerta temprana; señal de exposición creciente.
		Número de configuraciones erróneas detectadas en la nube.	Detección de riesgo de brecha por configuración errónea.
	KPI	Cumplimiento de parcheo dentro de SLA (% corregido ≤ X días)	Eficacia de remediación; reducción de ventana de riesgo.
		% de recursos con etiquetado conforme a política (dueño, criticidad o dato personal).	Ordenamiento de activos y trazabilidad para auditoría.
Identidad y acceso (IAM/CIEM)	KRI	Hallazgos de privilegios excesivos detectados por CIEM.	Indicio de escalamiento indebido; abuso potencial de permisos.
		Alertas de escalamiento de privilegios en el plano de control del CSP.	Señal de toma de control; riesgo crítico.
	KPI	Tiempo medio para revocar credenciales comprometidas.	Rapidez de contención ante cuentas expuestas.
		% de cuentas con MFA activa.	Adopción de control de autenticación robusta.
Datos y criptografía	KRI	Claves/secretos caducados o sin rotación dentro del umbral definido.	Debilidad criptográfica; comprender la exposición y el compromiso.
		Intentos de exfiltración de datos en la nube.	Indicador de actividad maliciosa o potencial fuga en curso.
	KPI	Cifrado en reposo y en tránsito habilitado por defecto (% de activos).	Protección de información; alineación con las normas vigentes.

	KPI	Edad media de secretos/llaves antes de rotación (días).	Disciplina criptográfica; disminución de riesgo residual.
Telemetría y observabilidad (SIEM/CSPM)	KRI	Anomalías de egreso (picos de tráfico saliente no habituales).	Indicio de exfiltración; compromiso probable.
	KPI	Recursos con *logging* hacia el SIEM central (% con telemetría completa).	Visibilidad para la detección; funciona como base para la respuesta.
Detección y respuesta	KPI	MTTD (tiempo medio en la detección).	Eficacia en el monitoreo; prontitud ante los nuevos hallazgos.
		MTTR (tiempo medio en la respuesta).	Desempeño de contención y recuperación.
		Tasa de contención de incidentes en la nube	Capacidad de limitar impacto durante eventos.
Red y superficie de ataque	KRI	Almacenes de objetos expuestos a Internet (por ejemplo, *buckets* públicos).	Superficie ampliada; riesgo de fuga.
	KPI	Servicios con *private endpoints* o tránsito por enlaces privados (% de flujos sensibles).	Aislamiento del tráfico; minimización en la exposición.
APIs y servicios	KRI	Intentos de abuso de API (tasa de códigos 401 o 403; *rate limiting* activado)	Señal de fuerza bruta o *token* inválido.
	KPI	APIs detrás de *API Gateway* con validación de esquema y autenticación fuerte (% total).	Robustez de interfaz; control de acceso.
DevSecOps e IaC	KPI	Número de pruebas de seguridad automatizadas en CI/CD.	Madurez de *DevSecOps* durante el ciclo de entrega.

	KPI	Cumplimiento de políticas como código en IaC (despliegues que satisfacen validaciones).	Higiene de configuración; reducción de *drift*.
SaaS y postura	KRI	Eventos de *shadow IT* detectados por CASB.	Riesgo fuera de gobierno; fuga potencial.
	KPI	Aplicaciones SaaS con revisión SSPM (% del catálogo).	Gobierno de terceros; disminución de *shadow IT*.
Terceros y cumplimiento	KRI	Incumplimientos de SLA del proveedor que afectan cargas sensibles.	Riesgo de disponibilidad; exposición contractual.
	KPI	Tasa de aprobación de auditorías de cumplimiento en la nube.	Adhesión a marcos regulatorios y estándares.
Disponibilidad y recuperación	KPI	Copias de seguridad inmutables con pruebas de restauración superadas.	Confiabilidad ante *ransomware*; salvaguarda de servicios.
		RTO/RPO cumplidos por servicio crítico.	Desempeño frente a contingencias; alineación con apetito de riesgo.
Zero Trust y arquitectura	KPI	Cobertura de confianza cero por pilar (identidad, dispositivos, redes, aplicaciones, datos).	Avance arquitectónico; madurez de control.
Concienciación y talento	KPI	Tasa de finalización de formación en seguridad en la nube para empleados.	Cultura de seguridad; preparación del personal.
Protección de cargas (CWPP)	KPI	Cobertura de agentes CWPP activos.	Visibilidad sobre cargas; endurecimiento efectivo.

6.3 Colaboración regional e intercambio de prácticas de excelencia

La protección en entornos de nube exige una coordinación transfronteriza sostenida. Para los bancos centrales de América Latina resulta provechoso articular alianzas entre pares y con organismos especializados, a fin de robustecer las competencias de manera conjunta. Un referente reciente es la iniciativa liderada por la Agencia de Ciberseguridad de Chile, con apoyo de la Unión Europea, orientada al fortalecimiento y desarrollo de capacidades en América Latina y el Caribe en materia de ciberseguridad, que contempla talleres, programas de formación, documentos de referencia e incluso una propuesta de ley modelo para la región [126].

Tales esquemas cooperativos facilitan la homologación de estándares, la transferencia de lecciones aprendidas y la convergencia de criterios frente a retos comunes de transición a despliegues en nube o arquitecturas híbridas. La participación en foros sectoriales o mesas de trabajo regionales brinda acceso a experiencias comparables y acelera la maduración institucional. A su vez, posibilita ejercicios coordinados —por ejemplo, simulacros sectoriales de incidentes cibernéticos— que evalúan la preparación colectiva y revelan dependencias críticas entre actores.

Conclusión

El documento elabora una ruta integral para que un banco central transite hacia arquitecturas de nube e infraestructuras híbridas con criterios de gobernanza sólidos y controles verificables. El primer bloque (GRC) consolida la alineación institucional: define marcos normativos de referencia, órganos decisorios y políticas internas, profundizando en la evaluación formal de proveedores de servicios en la nube (CSP), con énfasis en transferencia de riesgo, pólizas de ciberseguro y cláusulas contractuales críticas. El resultado es un andamiaje de gobierno capaz de orquestar responsabilidades, supervisar a terceros y someter las acciones externalizadas a debida diligencia, evitando puntos ciegos regulatorios y contractuales.

El segundo capítulo aterriza el modelo de responsabilidad compartida y sus consecuencias en IaaS/PaaS/SaaS, delineando fronteras precisas entre «seguridad de la nube» (operada por el CSP) y «seguridad en la nube» (propia del cliente). Se abordan rutas de migración, patrones de implementación y requisitos de integración para entornos híbridos, con una postura coherente frente a arquitecturas de confianza cero y flujos interplataforma. La lectura práctica es inequívoca: sin inventarios confiables, segmentación granular, identidad federada y runbooks de transición, cualquier programa queda expuesto a riesgos de parametrización, concentración y dependencia excesiva.

El tercer eje construye una defensa de datos por capas: clasificación fina por sensibilidad; soberanía y residencia; cifrado en reposo, en tránsito y en uso; administración de llaves (KMS/HSM) con BYOK/HYOK (*Bring/Hold Your Own Key*); y un panorama de criptografía avanzada marcado por técnicas cuánticas y homomórficas.

El cuarto módulo ensambla controles por dominios críticos: perímetro y red (microsegmentación, WAF, balanceo y defensa nativa frente a DDoS), identidades y secretos, almacenamiento con retención e inmutabilidad, así como CI/CD con revisiones integradas, análisis de contenedores y validaciones declarativas (políticas como código). Asimismo, se contempla la ingeniería del caos como una prueba automatizada de confiabilidad.

El quinto capítulo consolida la dimensión de respuesta a incidentes y robustez operacional: telemetría exhaustiva, recolección central de registros, playbooks vigentes,

coordinación con CSP durante eventos que exigen una panorámica técnica más amplia y aptitudes forenses acopladas a entornos de nube. Además, se describen los planes de resiliencia y continuidad del negocio, abordando recomendaciones en torno a objetivos de recuperación consistentes, redundancia geográfica, elasticidad de recursos y conmutación entre regiones o nubes para minimizar el impacto sistémico.

Finalmente, se elabora una hoja de ruta por fases y un sistema de métricas dual con KPI/KRI (indicadores de desempeño y riesgo) para supervisar el progreso, priorizar cierres y orientar la inversión. Se destaca que la colaboración regional, el intercambio de inteligencia de amenazas y la adopción de estándares de la industria financiera refuerzan la convergencia entre supervisores, operadores críticos y proveedores.

Referencias

[1] Alexander Nelson, Sanjay Rekhi, Murugiah Souppaya y Karen Scarfone. *NIST SP 800-61 Rev. 3 Incident Response Recommendations and Considerations for Cybersecurity Risk Management: A CSF 2.0 Community Profile*. National Institute of Standards y Technology (NIST), 2025. URL: https://csrc.nist.gov/pubs/sp/800/61/r3/final (vid. pág. 3).

[2] Soon Tein Lim, Alex Siow, Ricci Ieong Michael Roza y Saan Vandendriessche. *Cloud Incident Response (CIR) Framework*. Cloud Security Alliance (CSA), 2021. URL: https://cloudsecurityalliance.org/artifacts/cloud-incident-response-framework (vid. págs. 4-6, 18, 54, 55, 58).

[3] *Cloud Computing - Benefits, risks and recommendations for information security*. European Network e Information Security Agency (ENISA), 2009. URL: https://www.enisa.europa.eu/sites/default/files/publications/Cloud%20Computing%20Security%20Risk%20Assessment.pdf (vid. pág. 4).

[4] Martin Johnson. *What is the MITRE ATT&CK® Cloud Matrix?* Balbix. 2024. URL: https://www.balbix.com/insights/mitre-attck-for-cloud/ (vid. págs. 4-6).

[5] Rey LeClerc Sveinsson. *Aligning Your Incident Response Plan with NIST SP 800-61 Rev. 3: What's Changed and What to Do Now*. ERMProtect. n.d. URL: https://ermprotect.com/blog/aligning-your-incident-response-plan-with-nist-sp-800-61-rev-3/ (vid. pág. 5).

[6] Rich Mogull y Mike Rothman. *Security Guidance for Critical Areas of Focus in Cloud Computing v5*. Cloud Security Alliance (CSA), 2025. URL: https://cloudsecurityalliance.org/artifacts/security-guidance-v5 (vid. págs. 6, 19, 21).

[7] *Build a cloud governance team*. Microsoft. n.d. URL: https://learn.microsoft.com/en-us/azure/cloud-adoption-framework/govern/build-cloud-governance-team (vid. págs. 6, 10).

[8] *Security governance*. Amazon Web Services (AWS). n.d. URL: https://docs.aws.amazon.com/whitepapers/latest/aws-caf-security-perspective/security-governance.html (vid. págs. 6, 10, 62, 63).

[9] *Security in a Cloud Computing Environment*. National Credit Union Administration (NCUA). 2020. URL: https://ncua.gov/newsroom/press-release/2020/

ffiec-issues-statement-risk-management-cloud-computing-services/security-cloud-computing-environment (vid. págs. 7, 11, 18, 54, 55).
[10] Kacper Rafalski. *How To Develop a Banking Cloud Strategy in 2025?* Netguru. 2025. URL: https://www.netguru.com/blog/banking-cloud-strategy (vid. págs. 10, 15, 18, 19, 62).
[11] Vinay Male y Research Scholar II. «Financial services and cloud governance: ensuring regulatory compliance». En: *International Journal of Computer Engineering and Technology* 16 (feb. de 2025), págs. 2847-2863. DOI: 10.34218/IJCET_16_01_200 (vid. págs. 10, 11).
[12] *ECB consults on outsourcing cloud services*. European Central Bank (ECB). 2025. URL: https://www.bankingsupervision.europa.eu/press/pr/date/2024/html/ssm.pr240603~e625aaca33.en.html (vid. págs. 11, 12).
[13] *Cloud Executive Steering Group*. U.S Department of the Treasury. n.d. URL: https://home.treasury.gov/about/offices/domestic-finance/financial-institutions/cloud-executive-steering-group (vid. págs. 11, 12).
[14] *What Is Cyber Insurance? Why Is It Important?* Fortinet. n.d. URL: https://www.fortinet.com/resources/cyberglossary/cyber-insurance (vid. pág. 13).
[15] *Understanding Contingent Business Interruption in Cyber Insurance*. At-Bay Editorial. 2023. URL: https://www.at-bay.com/articles/contingent-business-interruption-cyber-insurance/ (vid. pág. 13).
[16] *Cloud Outage Insurance*. Parametrix Solutions. n.d. URL: https://www.parametrixinsurance.com/solutions-cloud (vid. pág. 14).
[17] *AWS Cyber Insurance Competency Partners*. Amazon Web Services (AWS). n.d. URL: https://aws.amazon.com/es/partners/cyber-insurance-partner-solutions/?nc1=h_ls (vid. pág. 14).
[18] *Risk Protection Program*. Google Cloud. n.d. URL: https://cloud.google.com/security/products/risk-protection-program?hl=en (vid. pág. 14).
[19] *Embrace the Cloud: Three Best Practices for Financial Institutions*. Saratoga Software. 2021. URL: https://saratogasoftware.com/embrace-the-cloud-three-best-practices-for-financial-institutions/ (vid. págs. 15, 16).
[20] *Cost Optimization tradeoffs*. Microsoft. 2024. URL: https://learn.microsoft.com/en-us/azure/well-architected/cost-optimization/tradeoffs (vid. pág. 15).
[21] *How Financial Services Can Maximize the Benefits of Operating in Hybrid Cloud*. Rackspace Technology. 2025. URL: https://www.rackspace.com/blog/how-financial-services-maximize-benefits-hybrid-cloud (vid. págs. 16, 17).
[22] *The 6 Rs of application modernization*. Microsoft. 2025. URL: https://learn.microsoft.com/en-us/azure/app-modernization-guidance/plan/the-6-rs-of-application-modernization (vid. pág. 16).
[23] Gal Nakash. *What is Hybrid Cloud Security? Best Practices and Solutions*. Micro-

soft. 2025. URL: https://www.reco.ai/learn/hybrid-cloud-security (vid. pág. 17).
[24] *Responsabilidades compartidas y destino compartido en Google Cloud*. Google Cloud. 2021. URL: https://cloud.google.com/architecture/framework/security/shared-responsibility-shared-fate?hl=es-419 (vid. pág. 20).
[25] *What Is Data Classification?* Palo Alto Networks. n.d. URL: https://www.paloaltonetworks.com/cyberpedia/data-classification (vid. págs. 21, 22).
[26] *Why Data Classification is the Unsung Hero of Financial Data Security*. Spirion. 2025. URL: https://www.spirion.com/blog/data-classification-hero-of-financial-data-security (vid. págs. 21, 22).
[27] *Data Retention Policies in Finance: How To Ensure and Scale Compliance in 2025*. Atlan. 2025. URL: https://atlan.com/know/data-governance/data-retention-policies-in-finance/ (vid. págs. 21, 22).
[28] *Soberanía digital y del dato en Google Cloud (José Carlos Cerezo, Google Cloud)*. Capacidad de Respuesta a Incidentes de Seguridad de la Información del Centro Criptológico Nacional (CCN-CERT). 2021. URL: https://www.youtube.com/watch?v=3k8NCFLnM94&t=1032s (vid. págs. 22, 24).
[29] *Soberanía de datos*. IT NOW. 2023. URL: https://www.youtube.com/watch?v=9fiSTYshJGI (vid. págs. 22, 32).
[30] *Global Data Sovereignty: A Comparative Overview*. Cloud Security Alliance (CSA). 2025. URL: https://cloudsecurityalliance.org/blog/2025/01/06/global-data-sovereignty-a-comparative-overview (vid. pág. 23).
[31] Austin Chia. *Data Sovereignty vs. Data Residency: What's The Difference?* Splunk. 2025. URL: https://www.splunk.com/en_us/blog/learn/data-sovereignty-vs-data-residency.html (vid. pág. 23).
[32] *Default encryption at rest*. Google Cloud. 2025. URL: https://cloud.google.com/docs/security/encryption/default-encryption?hl=en (vid. págs. 24, 25).
[33] *Encryption in transit for Google Cloud*. Google Cloud. 2025. URL: https://cloud.google.com/docs/security/encryption-in-transit?hl=en (vid. págs. 24, 25).
[34] *Confidential Computing*. Google Cloud. n.d. URL: https://cloud.google.com/security/products/confidential-computing?hl=en (vid. pág. 25).
[35] *Google Distributed Cloud*. Google Cloud. n.d. URL: https://cloud.google.com/distributed-cloud?hl=en (vid. pág. 25).
[36] *Protecting data with server-side encryption*. Amazon Web Services (AWS). n.d. URL: https://docs.aws.amazon.com/AmazonS3/latest/userguide/serv-side-encryption.html (vid. pág. 25).
[37] *Key stores*. Amazon Web Services (AWS). n.d. URL: https://docs.aws.amazon.com/kms/latest/developerguide/key-store-overview.html (vid. pág. 25).

[38] *AWS Nitro Enclaves*. Amazon Web Services (AWS). n.d. URL: https://aws.amazon.com/es/ec2/nitro/nitro-enclaves/?nc1=h_ls (vid. pág. 25).

[39] *Data protection in Amazon EC2*. Amazon Web Services (AWS). n.d. URL: https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/data-protection.html (vid. pág. 25).

[40] Vijaykumar Bidve, Aruna Pavate, Rahul Raut, Shailesh Kediya, Pakiriswamy Sarasu, Koteswara Anne, Aryani Gangadhara y Ashfaq Shaikh. «Secure financial application using homomorphic encryption». En: *Indonesian Journal of Electrical Engineering and Computer Science* 38 (abr. de 2025), pág. 595. DOI: 10.11591/ijeecs.v38.i1.pp595-602 (vid. págs. 25, 30).

[41] *Homomorphic Encryption Use Cases*. IEEE. n.d. URL: https://digitalprivacy.ieee.org/publications/topics/homomorphic-encryption-use-cases/ (vid. pág. 25).

[42] Pedro Gonzalo Méndez Hernández. «Introducción a la Criptografía Homomórfica». Tesis de mtría. Universidad de La Laguna, 2022. URL: https://riull.ull.es/xmlui/bitstream/handle/915/30351/Introduccion%20a%20la%20Criptografia%20Homomorfica.pdf?sequence=1 (vid. págs. 26, 29).

[43] Xun Yi, Russell Paulet y Elisa Bertino. *Homomorphic Encryption and Applications*. Springer Cham, 2014. URL: https://doi.org/10.1007/978-3-319-12229-8 (vid. pág. 27).

[44] *Combining Machine Learning and Homomorphic Encryption in the Apple Ecosystem*. Apple. 2024. URL: https://machinelearning.apple.com/research/homomorphic-encryption (vid. pág. 29).

[45] Sander Tamme. *A Guide to Cloud Key Management Best Practices*. Fortanix. 2025. URL: https://www.fortanix.com/blog/a-guide-to-cloud-key-management-best-practices (vid. págs. 31, 34).

[46] *Cloud Key Management*. Google Cloud. n.d. URL: https://cloud.google.com/security/products/security-key-management?hl=en (vid. págs. 31, 32).

[47] Annie Badman y Matthew Kosinski. *What is key management?* IBM. n.d. URL: https://www.ibm.com/think/topics/key-management (vid. págs. 31, 32).

[48] *Cloud External Key Manager*. Google Cloud. n.d. URL: https://docs.cloud.google.com/kms/docs/ekm (vid. pág. 32).

[49] Lanre Ogunmola. *Architecting for database encryption on Google Cloud*. Google Cloud. 2022. URL: https://cloud.google.com/blog/topics/inside-google-cloud/architecting-for-database-encryption-on-google-cloud (vid. pág. 33).

[50] *Post-quantum cryptography*. Google Cloud. n.d. URL: https://cloud.google.com/security/resources/post-quantum-cryptography?hl=en (vid. pág. 35).

[51] *SEALSQ Enhances Financial Sector Security with Post-Quantum Cryptography Solutions*. SEALSQ. 2025. URL: https://www.sealsq.com/investors/news-relea

ses/sealsq-enhances-financial-sector-security-with-post-quantum-cryptography-solutions (vid. págs. 35, 36).
[52] *AWS post-quantum cryptography migration plan*. Amazon Web Services (AWS). 2024. URL: https://aws.amazon.com/blogs/security/aws-post-quantum-cryptography-migration-plan/?utm_source=chatgpt.com (vid. pág. 35).
[53] Nelly Porter y Christiane Peters. *PQC in plaintext: How we're helping customers prepare for a quantum-safe future*. Google Cloud. 2025. URL: https://cloud.google.com/blog/products/identity-security/how-were-helping-customers-prepare-for-a-quantum-safe-future (vid. pág. 35).
[54] *¿Qué es la microsegmentación?* Zscaler. n.d. URL: https://www.zscaler.com/es/resources/security-terms-glossary/what-is-microsegmentation (vid. pág. 37).
[55] Charlie Treadwell. *Mastering Microsegmentation in the Cloud*. 2023. URL: https://www.elisity.com/blog/public-cloud-microsegmentation (vid. págs. 37, 38).
[56] *Zero Trust: The imperative for modern security realities*. Illumio. n.d. URL: https://www.illumio.com/solutions/zero-trust (vid. pág. 37).
[57] *Plataforma Akamai Guardicore para Zero Trust*. Akamai Technologies. n.d. URL: https://www.akamai.com/es/products/akamai-guardicore-platform (vid. pág. 37).
[58] *Compara los servicios de AWS y Azure con Google Cloud*. Google Cloud. 2024. URL: https://cloud.google.com/docs/get-started/aws-azure-gcp-service-comparison?hl=es-419 (vid. pág. 38).
[59] *AWS Shield Features*. Amazon Web Services (AWS). n.d. URL: https://aws.amazon.com/es/shield/features/ (vid. pág. 38).
[60] *Google Cloud Armor*. Google Cloud. n.d. URL: https://cloud.google.com/security/products/armor?hl=es-419 (vid. pág. 38).
[61] *What is Azure DDoS Protection?* Microsoft. n.d. URL: https://learn.microsoft.com/en-us/azure/ddos-protection/ddos-protection-overview (vid. pág. 38).
[62] *Auto Scaling groups*. Amazon Web Services (AWS). n.d. URL: https://docs.aws.amazon.com/autoscaling/ec2/userguide/auto-scaling-groups.html (vid. pág. 39).
[63] *AWS IAM Access Analyzer*. Amazon Web Services (AWS). n.d. URL: https://docs.aws.amazon.com/access-analyzer/latest/APIReference/Welcome.html (vid. pág. 39).
[64] *Microsoft Entra ID documentation*. Microsoft. n.d. URL: https://learn.microsoft.com/en-us/entra/identity/ (vid. págs. 39, 41).
[65] Gregg Lindemulder y Matthew Kosinski. *¿Qué es la confianza cero (zero trust)?* IBM. 2024. URL: https://www.ibm.com/mx-es/think/topics/zero-trust (vid.

pág. 39).
[66] *Microsoft Entra Conditional Access optimization agent*. Microsoft. 2025. URL: https://learn.microsoft.com/en-us/entra/security-copilot/conditional-access-agent-optimization (vid. pág. 40).
[67] *BeyondCorp Enterprise Zero Trust Framework Explained*. StrataPrime y Google. 2023. URL: https://www.youtube.com/watch?v=orEinYpZpzg (vid. pág. 40).
[68] *Third-party trust provider context for Verified Access trust data*. Amazon Web Services (AWS). n.d. URL: https://docs.aws.amazon.com/verified-access/latest/ug/trust-data-third-party-trust.html (vid. pág. 40).
[69] *Identity federation in AWS*. Amazon Web Services (AWS). n.d. URL: https://aws.amazon.com/es/identity/federation/ (vid. pág. 40).
[70] *Microsoft Graph documentation*. Microsoft. n.d. URL: https://learn.microsoft.com/en-us/graph/ (vid. pág. 41).
[71] *Develop on Google Workspace*. Google. n.d. URL: https://developers.google.com/workspace/guides/get-started (vid. pág. 41).
[72] *Locking objects with Object Lock*. Amazon Web Services (AWS). n.d. URL: https://docs.aws.amazon.com/AmazonS3/latest/userguide/object-lock.html (vid. pág. 42).
[73] *Store business-critical blob data with immutable storage in a write once, read many (WORM) state*. Microsoft. 2024. URL: https://learn.microsoft.com/en-us/azure/storage/blobs/immutable-storage-overview (vid. pág. 42).
[74] *Bucket Lock*. Google Cloud. n.d. URL: https://cloud.google.com/storage/docs/bucket-lock (vid. págs. 42, 43).
[75] *Amazon Elastic Block Store*. Amazon Web Services (AWS). n.d. URL: https://aws.amazon.com/es/ebs/ (vid. pág. 42).
[76] *Amazon EBS General Purpose Volumes*. Amazon Web Services (AWS). n.d. URL: https://aws.amazon.com/es/ebs/general-purpose/?nc1=h_ls (vid. pág. 43).
[77] *Managed Disks pricing*. Microsoft. n.d. URL: https://azure.microsoft.com/en-us/pricing/details/managed-disks/ (vid. pág. 43).
[78] *Google Cloud Hyperdisk overview*. Google Cloud. n.d. URL: https://cloud.google.com/compute/docs/disks/hyperdisks (vid. pág. 43).
[79] *File storage on Compute Engine*. Google Cloud. 2025. URL: https://cloud.google.com/architecture/filers-on-compute-engine (vid. pág. 43).
[80] *Data Retention Policies in Finance: How To Ensure and Scale Compliance in 2025*. Atlan. 2025. URL: https://atlan.com/know/data-governance/data-retention-policies-in-finance/ (vid. págs. 43, 44).
[81] *AWS Artifact*. Amazon Web Services (AWS). n.d. URL: https://aws.amazon.com/es/artifact/?nc1=h_ls (vid. pág. 44).
[82] *Documentación de Azure Blueprint*. Microsoft. n.d. URL: https://learn.microsoft.com/es-es/azure/governance/blueprints/ (vid. pág. 44).

[83] *Security Command Center documentation*. Google Cloud. n.d. URL: https://cloud.google.com/security-command-center/docs (vid. págs. 44, 48, 49).
[84] *VM Manager documentation*. Google Cloud. n.d. URL: https://cloud.google.com/compute/vm-manager/docs (vid. págs. 44, 45).
[85] *What Is CI/CD Security?* Palo Alto Networks. n.d. URL: https://www.paloaltonetworks.com/cyberpedia/what-is-ci-cd-security (vid. pág. 45).
[86] Beth Grayson. *SAST, DAST, or SCA: Which is best for application security testing?* Outpost24. 2025. URL: https://outpost24.com/blog/application-security-testing-sast-dast-sca/ (vid. págs. 45, 46).
[87] Efraín Escamilla. *Automatización en DevSecOps: SAST, DAST y Más Herramientas Clave*. Ventus Technology. 2025. URL: https://blog.ventus-tech.com/seguridad-y-cumplimiento-ti/automatizacion-devsecops-sast-dast-herramientas (vid. pág. 46).
[88] *Open Policy Agent Core Documentation*. Open Policy Agent. 2025. URL: https://www.openpolicyagent.org/docs (vid. pág. 46).
[89] *Artifact Analysis overview*. Google Cloud. n.d. URL: https://docs.cloud.google.com/artifact-analysis/docs/artifact-analysis (vid. págs. 46, 47).
[90] *What is chaos engineering?* IBM. n.d. URL: https://www.ibm.com/think/topics/chaos-engineering (vid. págs. 47, 48).
[91] *Azure Chaos Studio documentation*. Microsoft. n.d. URL: https://learn.microsoft.com/en-us/azure/chaos-studio/ (vid. pág. 47).
[92] *What is AWS Fault Injection Service?* Amazon Web Services (AWS). n.d. URL: https://docs.aws.amazon.com/fis/latest/userguide/what-is.html (vid. pág. 47).
[93] *Chaos Engineering: the history, principles, and practice*. Gremlin. 2023. URL: https://www.gremlin.com/community/tutorials/chaos-engineering-the-history-principles-and-practice (vid. pág. 47).
[94] Jim Hirschauer. *How to Use Error Budgets for Reliability Management*. Harness. 2023. URL: https://www.harness.io/blog/how-use-error-budgets-reliability-management (vid. pág. 47).
[95] *Best practices for streamlining log centralization with Cloud Logging*. Google Cloud. 2024. URL: https://cloud.google.com/blog/products/devops-sre/how-to-centralize-log-management-with-cloud-logging (vid. págs. 50, 51).
[96] *Protección de los servicios de nube pública ante amenazas de ransomware*. Dirección Nacional de Ciberseguridad de Israel y Banco Interoamericano de Desarrollo, 2025. URL: https://publications.iadb.org/es/publications/spanish/viewer/Proteccion-de-los-servicios-de-nube-publica-ante-amenazas-de-ransomware-mejores-practicas-en-ciberseguridad.pdf (vid. págs. 51, 61, 62, 64).
[97] *SIEM Log Management: The Complete Guide*. Exabeam. 2024. URL: https://ww

w.exabeam.com/explainers/event-logging/events-and-logs/ (vid. págs. 52, 53).

[98] *Cloud SIEM and Flex Logs: Enhanced security insights for the cloud*. Datadog. 2025. URL: https://www.datadoghq.com/blog/cloud-siem-flex-logs/ (vid. pág. 52).

[99] *Google Security Operations (SecOps)*. Google Cloud. n.d. URL: https://cloud.google.com/security/products/security-operations?hl=en (vid. pág. 52).

[100] *Microsoft Sentinel documentation*. Microsoft. n.d. URL: https://learn.microsoft.com/en-us/azure/sentinel/ (vid. págs. 52, 53).

[101] *What is Cloud Incident Response?* Palo Alto Networks. n.d. URL: https://www.paloaltonetworks.com/cyberpedia/unit-42-cloud-incident-response (vid. págs. 54, 56).

[102] *What is TIBER-EU?* European Central Bank (ECB). n.d. URL: https://www.ecb.europa.eu/paym/cyber-resilience/tiber-eu/html/index.en.html (vid. pág. 54).

[103] *What is AWS Security Incident Response?* Amazon Web Services (AWS). n.d. URL: https://docs.aws.amazon.com/security-ir/latest/userguide/what-is.html (vid. págs. 54, 56).

[104] Kyle Dickinson. *Welcoming the AWS Customer Incident Response Team*. Amazon Web Services (AWS). 2022. URL: https://aws.amazon.com/es/blogs/security/welcoming-the-aws-customer-incident-response-team/ (vid. pág. 55).

[105] *AWS Trust and Safety Center*. Amazon Web Services (AWS). 2025. URL: https://repost.aws/aws-trust-and-safety (vid. pág. 55).

[106] *Microsoft Incident Response*. Microsoft. n.d. URL: https://www.microsoft.com/en-us/security/business/microsoft-incident-response (vid. pág. 55).

[107] *Respond to abuse notifications and warnings in Google Cloud*. Google Cloud. n.d. URL: https://cloud.google.com/docs/security/respond-to-abuse-misuse (vid. pág. 55).

[108] *Asesoramiento de Mandiant sobre seguridad cibernética*. Google Cloud. n.d. URL: https://cloud.google.com/security/consulting/mandiant-services?hl=es-419 (vid. pág. 55).

[109] Benjamin McInnis. *Cloud Forensics Explained*. Google Cloud. 2025. URL: https://www.crowdstrike.com/en-us/cybersecurity-101/cloud-security/cloud-forensics/ (vid. pág. 56).

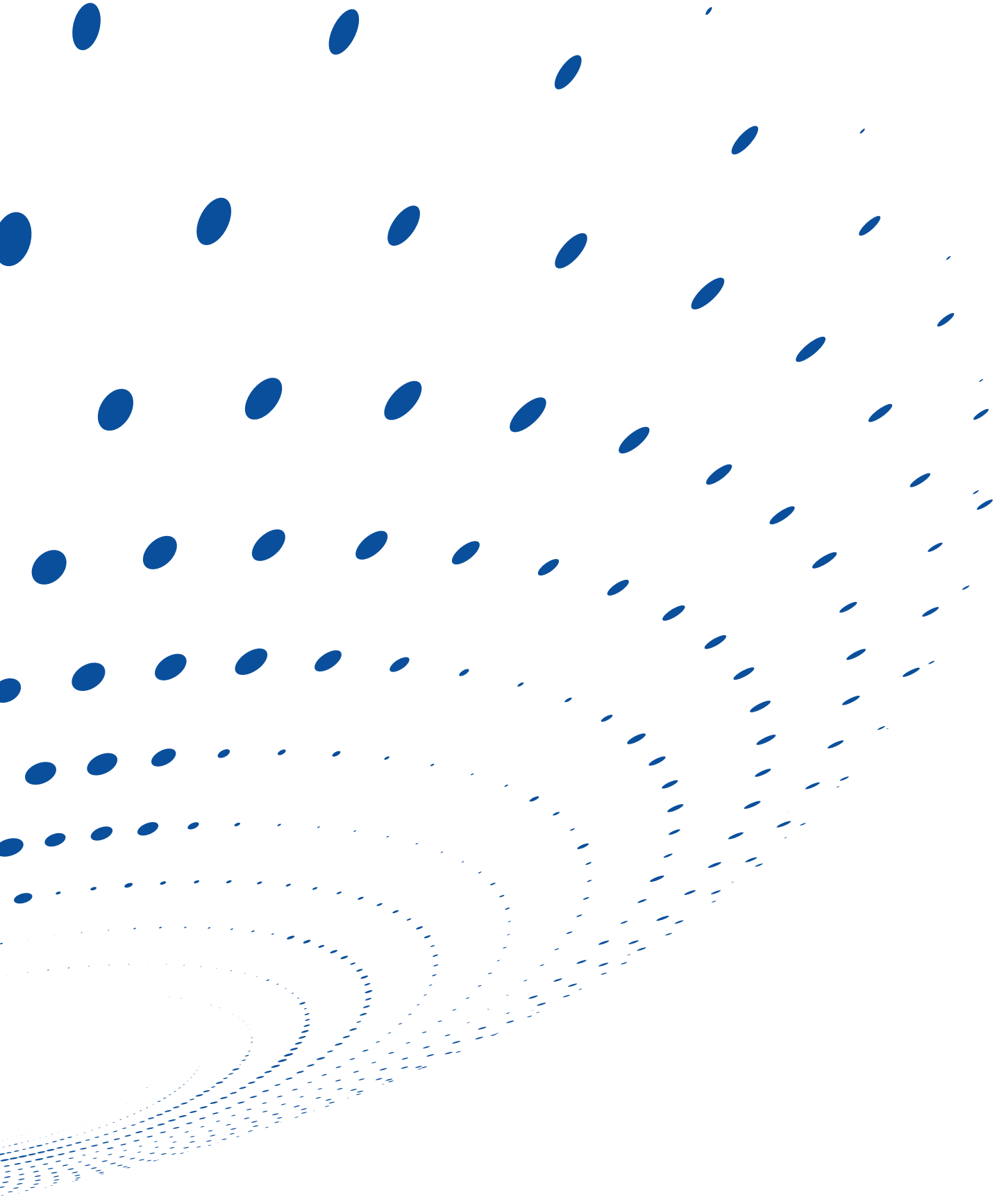
[110] National Institute of Standards y Technology (NIST). *NIST Cloud Computing Forensic Science Challenges*. 2020. URL: https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8006.pdf (vid. pág. 56).

[111] Jose Obando. *Automate Amazon EC2 instance isolation by using tags*. 2021. URL: https://aws.amazon.com/es/blogs/security/automate-amazon-ec2-instance-isolation-by-using-tags/ (vid. pág. 57).

[112] Julia Furst Morgado. *What is the 3-2-1 Backup Rule?* Veeam. 2025. URL: https://www.veeam.com/blog/321-backup-rule.html (vid. pág. 58).
[113] *#StopRansomware Guide*. Multi-State Information Sharing y Analysis Center (MS-ISAC), 2023. URL: https://media.defense.gov/2023/May/23/2003227891/-1/-1/0/CSI-StopRansomware-Guide.PDF (vid. págs. 58, 59).
[114] Michael Wilson. *Establishing RPO and RTO Targets for Cloud Applications*. Amazon Web Services (AWS). 2022. URL: https://aws.amazon.com/es/blogs/mt/establishing-rpo-and-rto-targets-for-cloud-applications/ (vid. pág. 59).
[115] *Cloud backup and disaster recovery*. Darktrace. 2025. URL: https://www.darktrace.com/cyber-ai-glossary/cloud-backup-and-disaster-recovery (vid. pág. 59).
[116] *Multi-AZ vs. Multi-Region in the Cloud*. FlashGrid. 2024. URL: https://www.flashgrid.io/news/multi-az-vs-multi-region-in-the-cloud/ (vid. pág. 59).
[117] Seth Eliot. *Disaster Recovery (DR) Architecture on AWS, Part III: Pilot Light and Warm Standby*. Amazon Web Services (AWS). 2021. URL: https://aws.amazon.com/es/blogs/architecture/disaster-recovery-dr-architecture-on-aws-part-iii-pilot-light-and-warm-standby/ (vid. pág. 59).
[118] Seth Eliot. *Pilar de fiabilidad: Marco de AWS Well-Architected*. Amazon Web Services (AWS). 2024. URL: https://docs.aws.amazon.com/es_es/wellarchitected/latest/reliability-pillar/welcome.html (vid. pág. 59).
[119] Surajit Mitra. *Roadmap your bank's journey to successful cloud adoption*. Virtusa. 2023. URL: https://www.virtusa.com/insights/perspectives/roadmap-your-banks-journey-to-successful-cloud-adoption (vid. pág. 61).
[120] *Central Bank of Brazil (Brazil)*. Google Cloud. n.d. URL: https://cloud.google.com/security/compliance/bcb-brazil?hl=en (vid. pág. 69).
[121] *Informe Normativo Norma de Externalización de Servicios en Compañías de Seguros*. Regulador y Supervisor Financiero de Chile, 2025. URL: https://www.cmfchile.cl/institucional/legislacion_normativa/normativa_tramite_ver_archivo.php?id=2025081438&seq=1 (vid. pág. 69).
[122] *Externalización de servicios*. Regulador y Supervisor Financiero de Chile, 2014. URL: https://www.cmfchile.cl/portal/principal/613/articles-28982_doc_pdf.pdf (vid. pág. 69).
[123] *Lineamientos de seguridad de la información para el uso de servicios en la nube*. Dirección de Gobierno Digital, 2025. URL: https://gobiernodigital.mintic.gov.co/692/articles-401777_recurso_1.pdf (vid. pág. 69).
[124] *Cómputo en la nube para el sector financiero: oportunidades para México*. Instituto Mexicano para la Competitividad, 2022. URL: https://imco.org.mx/wp-content/uploads/2022/09/Computo-en-la-nube-para-el-sector-financiero_Documento.pdf (vid. pág. 69).
[125] Gowsika Vadivel. *KRIs vs KPIs - What's the Difference?* Cyber Sierra. 2025. URL:

https://cybersierra.co/blog/kris-vs-kpis-whats-the-difference/ (vid. págs. 69, 70).

[126] *Chile inicia un proyecto para fortalecer la ciberseguridad en América Latina y el Caribe*. SeguriLatam. 2025. URL: https://www.segurilatam.com/ciberilatam/chile-inicia-proyecto-fortalecimiento-ciberseguridad-america-latina-caribe_20250602.html/ (vid. pág. 74).



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