Panorama actual de la ciberseguridad

Un desafío constante para la industria financiera.

Octubre 2025

ARMMA

Resumen **Ejecutivo**

La industria financiera en Chile está entrando en una fase de **mayor exigencia regulatoria y supervisión coordinada,** mientras la **acelerada digitalización** (banca digital, servicios cloud, Fintech, Inteligencia Artificial) **expone nuevas superficies de ataque.**

Esto genera presión para **madurar la gestión de riesgo en ciberseguridad,** mejorar los controles de detección y respuesta, brindar mayores capacidades de seguridad y privacidad a usuarios finales, y transformar el gobierno y la gestión de proveedores.

La adopción tecnológica está avanzando más rápido que la capacidad que se tiene para asegurarlas. Esto a su vez abre **oportunidades** a las empresas para **diferenciarse y entregar confianza,** tanto a clientes como reguladores.

Contexto **Industria**

1

Mayor exigencia regulatoria y formalización de prácticas.

La **CMF** ha elevado los requisitos en materia de continuidad operacional, reportabilidad y gestión de incidentes, mientras la **Ley Marco de Ciberseguridad (2024)** impone nuevas obligaciones a las entidades críticas.

2

Coordinación interinstitucional.

La entrada en vigor de la **Agencia Nacional de Ciberseguridad (ANCI)** impulsa una supervisión transversal que obliga a las entidades financieras a alinear sus controles con marcos nacionales y sectoriales de ciberseguridad.

3

Transformación digital acelerada.

Las arquitecturas cloud híbridas, el modelo de Finanzas Abiertas y el ecosistema Fintech amplían la **dependencia de terceros y la superficie de riesgo,** convirtiendo la gestión de proveedores en un pilar crítico.

4

Fiscalización más activa y sanciones crecientes.

Entre el 2024 y 2025 se observó un incremento de las multas aplicadas por la CMF y la presión por cumplimiento demostrable, donde los incidentes mal gestionados o la falta de información oportuna han tenido **consecuencias financieras y reputacionales mas severas.**

ARMMA

- Aumento del 61% en incidentes de seguridad relacionados con servicios de nube en la región (LATAM).
- Las brechas de datos más relevantes vienen de ataques dirigidos a proveedores.

- Los atacantes están utilizando IA generativa para crear campañas de phishing avanzado, producir deepfakes y evadir controles de seguridad.
- Modelo RaaS facilita la entrada de actores menos técnicos al ecosistema.

- Se detectaron 14 millones de intentos de phishing en Chile durante el año 2024.
- Ataques son cada vez mas dirigidos (spear phishing) combinando redes sociales, ingeniería social y mensajería.

Amenazas y **Cibercrimen**

- Troyanos bancarios, phishing avanzado, y accesos remotos ilícitos son las amenazas mas comunes en banca y Fintech.
- Criminales utilizan datos públicos en Internet para dirigir y personalizar ataques.

- Aumento del scam financiero por medio de entidades falsas ofreciendo créditos o inversiones en sitios web fraudulentos, suplantando entidades reales y captando fondos a través de adelantos.

- Ransomware creciente, con múltiples capas de extorsión (cifrado, amenaza y ataques).
- Más del 50% de las empresas víctimas de ransomware han pagado rescates (Chile).

- Los ciberataques de grupos criminales crecieron un 30% en Chile durante el año 2024.
- Atacantes siguen buscando objetivos en instituciones financieras por capacidad de pago y sensibilidad de datos.

Impacto de **Nuevas Regulaciones**

1

Fortalecimiento del marco de gestión de ciberseguridad.

Las nuevas normativas requieren de políticas formales y roles claros definidos, a la vez que elevan los estándares de seguridad y resiliencia acorde con marcos internacionales como **NIST CSF 2.0, ISO/IEC 27001:2022, CIS Controls v8** y las directrices de **SWIFT CSP,** entre otros.

2

Reportabilidad estructurada.

Las entidades deben **informar y reportar** tanto a la **CMF** como a la nueva institucionalidad **(ANCI),** los cuales esperan reportes más rápidos y estandarizados ante incidentes, lo que obliga a mejorar capacidades de detección, playbooks, forenses y coordinación interáreas.

3

Protección de datos personales.

La Ley 21.719 entra en vigor en Diciembre del 2026, pero las entidades ya se encuentran trabajando para cumplir los requisitos. La falta de acción temprana puede traducirse en sanciones y pérdida operativa, **asumir el cambio puede constituir una ventaja competitiva.**

4

Interoperabilidad financiera.

La Ley Fintech y el nuevo modelo plantea un desafío doble: garantizar la disponibilidad de APIs seguras y proteger la confidencialidad de la información compartida entre actores diversos. Esto impulsa la adopción de estándares maduros **(FIDO2, OAuth 2.0, mTLS).**

Principales **Desafíos**

Madurez desigual.

Bancos grandes avanzan rápido; cooperativas y entidades menores pueden quedar rezagadas en controles, presupuesto y cultura de ciberseguridad.

Fragmentación de políticas internas.

Las áreas de TI, seguridad, riesgo, auditoría y cumplimiento aún operan con silos de información. El modelo de tres líneas de defensa se debe ajustar a un panorama regulatorio y de amenazas que requiere cada vez más estrecha colaboración y gestión coordinada entre equipos.

Relaciones con terceros.

La dependencia con proveedores aumenta el riesgo y exposición a brechas de seguridad, a la vez que la definición de requerimientos de seguridad en contratos, monitoreo y revisión continua de SLAs y SLOs se consideran frecuentemente como áreas débiles del gobierno.

Detección temprana y respuesta.

La falta de visibilidad y correlación de eventos de seguridad en infraestructura cloud y entornos distribuidos, retrasa la respuesta de equipos operativos, lo que puede aumentar el impacto ante un potencial incidente.

Escasez de talento especializado.

Se cuenta con una dificultad para desarrollar y retener talento, en una industria donde se requieren perfiles con experiencia en seguridad financiera y cumplimiento regulatorio, y donde se necesitan skills de ciberseguridad avanzada (análisis forense, malware reversing).

Oportunidades **Estratégicas**

Diferenciación por resiliencia y confianza digital.

Las instituciones que integren ciberseguridad en la propuesta de valor tendrán una ventaja competitiva en su estrategia comercial (confianza del cliente, mejores términos).

Colaboración interbancaria y público-privada.

La nueva institucionalidad y el intercambio de inteligencia permiten anticipar amenazas, armonizar respuestas y fomentar la participación de ejercicios entre entidades críticas.

Integración de seguridad por diseño.

Aplicar mejores prácticas de desarrollo seguro (SSDLC) y secure-by-design en recursos de APIs e infraestructura cloud, para todos los productos financieros digitales, con la finalidad de mitigar riesgos tempranamente (shift-left) y reducir costos futuros de cumplimiento.

Uso de automatización e inteligencia artificial.

Automatizar evidencias, reportes y pruebas continuas reduce el riesgo de sanción por incumplimiento regulatorio. Herramientas GRC y compliance-as-code permiten evidenciar controles en tiempo real, las aplicaciones de IA pueden amplificar estas capacidades.

Orquestación de seguridad.

La centralización de controles a través de herramientas como SOAR y/o Identity Fabric permiten agilizar las operaciones de seguridad, al unificar plataformas y tareas que permiten automatizar flujos de trabajo, reduciendo costos y elevando consistencia.

Recomendaciones para **CISOS y Líderes**

1

Mapear obligaciones regulatorias y evaluar brechas de control.

Contar con una matriz de cumplimiento para CMF/Ley Marco/Ley Datos Personales, entre otras circulares. Identificar brechas y definir roadmap priorizado de cierre para gaps críticos.

2

Robustecer el programa de gestión de terceros.

Incluir cláusulas de seguridad en contratos con proveedores, realizar pruebas periódicas, reforzar derechos de auditoría y aplicar modelos de riesgo por proveedor. El monitoreo de terceros debe ser continuo y accionable según calificación de riesgo (TPRM).

3

Fortalecer capacidades de detección y respuesta.

Integrar SIEM, XDR y SOAR con telemetría en cloud y endpoints, diseñar playbooks alineados a requisitos regulatorios, y realizar ejercicios de tabletop a través de herramientas de simulación interactiva (wargaming) con áreas legales y comunicación.

4

Medir y reportar datos relevantes.

Definir KPIs accionables (MTTD/MTTR, cobertura de activos, % de recursos cloud en cumplimiento de postura, SLA de proveedores) y reportarlos al directorio. Utilizar dashboards para métricas regulatorias y adoptar capacidades para automatizar evidencias.

5

Capacitación y retención.

Invertir en talento y formación a través de programas internos de carrera para roles críticos, rotación planificada y alianzas con proveedores e instituciones académicas.

Conclusiones

El sistema financiero chileno se encuentra en un etapa de **madurez regulatoria, aumento de amenazas de ciberseguridad y redefinición tecnológica.**

Las regulaciones locales e internacionales están **elevando el estándar y forzando a las instituciones a robustecer sus estructuras** de gobierno, privacidad y seguridad.

Las instituciones que logren **equilibrar innovación, cumplimiento y resiliencia digital** establecerán el nuevo estándar de confianza en la industria financiera.

El punto clave para los líderes (CISO, CRO, Directorio) será **combinar inversiones tecnológicas con gobernanza, métricas y ejercicios de respuesta,** para cumplir los plazos y expectativas de reporte que impone la nueva institucionalidad.

Cómo te puede ayudar ARMMA?

Estándares y **Normativas**

Regulaciones y requisitos obligatorios

- RAN CMF
- CUR/ NCG
- LMC/ LPDP

Marcos y estándares de ciberseguridad

- ISO
- NIST/ CIS
- COBIT/ SOC2

Normativas de industria

- PCI DSS
- SWIFT CSP
- BCBS 239

Cómo podemos **ayudarlos?**

- Servicios de vCISO corporativo para empresas.
- Auditoría de Cumplimiento Normativo (RAN/NCG).
- Evaluación de Ley Marco de Ciberseguridad (21.663).
- Evaluación de Ley Protección de Datos Personales (21.719).

- Auditoría de Cumplimiento Normativo (ISO).
- Diagnóstico y Roadmap de Ciberseguridad (NIST/CIS).
- Diagnóstico y Roadmap de Seguridad Cloud (CSA CCM).
- Auditoría de Seguridad en Nubes Públicas (CIS Benchmarks).

- Auditoría de Cumplimiento Normativo (PCI DSS).
- Evaluación de Seguridad Transaccional (SWIFT CSP).

Dikson Pradenas
Partner & Co-Founder

Alex Müller
Tech Risk Senior Manager

Iván Gray
Information Security
& Cybersecurity Advisor

ARMMA | Advisory Services | Technology and Analytics Solutions

Acerca de ARMMA
ARMMA es una consultora en gestión de riesgos y soluciones tecnológicas. Nuestros servicios ayudan a impulsar el éxito sostenible de nuestros clientes en diversas industrias. Nos comprometemos a trabajar en equipo para cumplir con nuestras promesas hacia todos los interesados. A través de nuestro trabajo, desempeñamos un papel en la mejora de la estabilidad financiera y la promoción de la innovación para nuestros clientes y nuestro equipo. ARMMA CONSULTING LIMITADA opera como una firma de consultoría independiente, proporcionando servicios de asesoría y tecnología adaptados a las necesidades únicas de nuestros clientes. Para más información sobre nuestra organización, visita armma.cl.

Los Militares 5953, Piso 5, Las Condes, Santiago, Chile.

armma.cl

ARMMA

CONTÁCTANOS

Dikson Pradenas
Partner & Co-Founder
dpradenas@armma.cl
+569 9748 7311

Alex Müller
Tech Risk Senior Manager
amuller@armma.cl
+569 4474 0096

Iván Gray
Information Security
& Cybersecurity Advisor
igray@armma.cl
+56 9 6531 9587