



Riesgo cibernético en los sistemas de pagos e infraestructuras de mercados financieros

Retos y aprendizajes

Eduardo Tejeda

Fecha : Sep-2025

Uso Público

Información de acceso público.



Advertencia

Las opiniones y argumentos expresados en esta presentación
son responsabilidad exclusiva del autor y no necesariamente
reflejan la postura oficial del Banco de México.

Contenido



El contexto de las IMF



Riesgos ciberneticos



Tres lecciones

La importancia de las IMF

¿Qué son?

- **Las Infraestructuras de los Mercados Financieros (IMF) son un conjunto de instrumentos, procedimientos y reglas para la transferencia de fondos entre dos o más participantes.** La infraestructura incluye a los participantes y a la entidad que opera el mecanismo.
- Estas incluyen los **sistemas de pagos, las contrapartes centrales, depósitos y sistemas de liquidación de valores, repositorios y sistemas de información** y otros mecanismos de pago.

¿Por qué son importantes?

- Disminuyen el **riesgo de incumplimiento** entre los participantes del sistema.
- Fomentan la **estabilidad del sistema**, al promover que las operaciones se liquiden de forma segura y eficiente.
- Impulsan el **desarrollo económico**, al facilitar la inversión y los movimientos de capital.



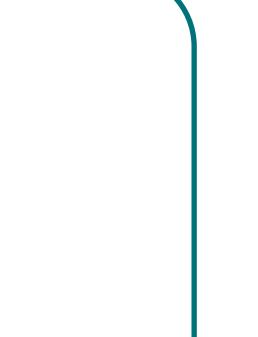
'Las tuberías del sistema financiero'

El rol de los bancos centrales en las IMF

La mayoría de los bancos centrales en el mundo, tiene entre sus finalidades promover el buen funcionamiento de las IMF. Esta finalidad tiene impacto en las demás funciones.



La conducción de la política monetaria, ya que su instrumentación depende crucialmente de la disponibilidad de **IMF confiables y eficaces**.

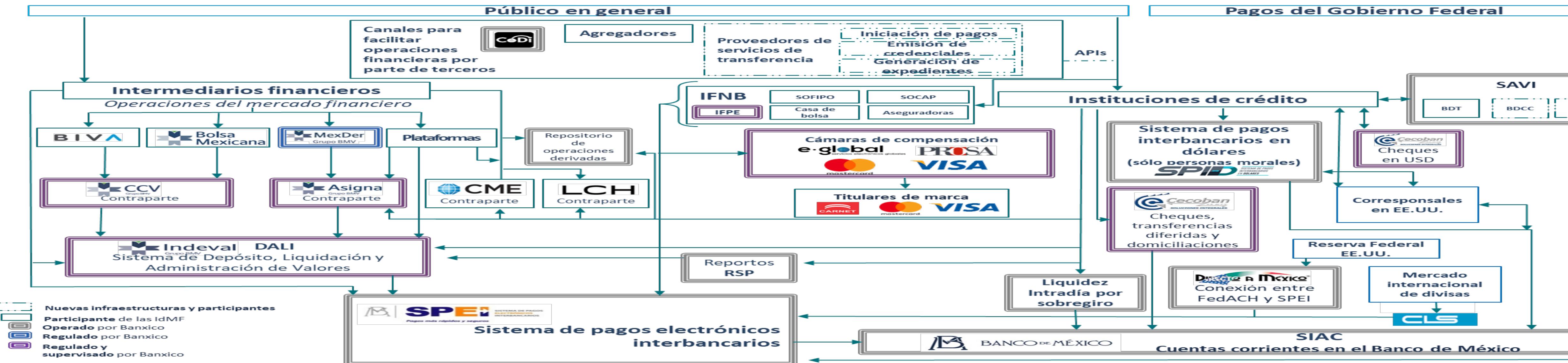


La gestión del **riesgo sistémico**, particularmente en tiempos de incertidumbre, que puede menoscabar la **estabilidad financiera y monetaria**.

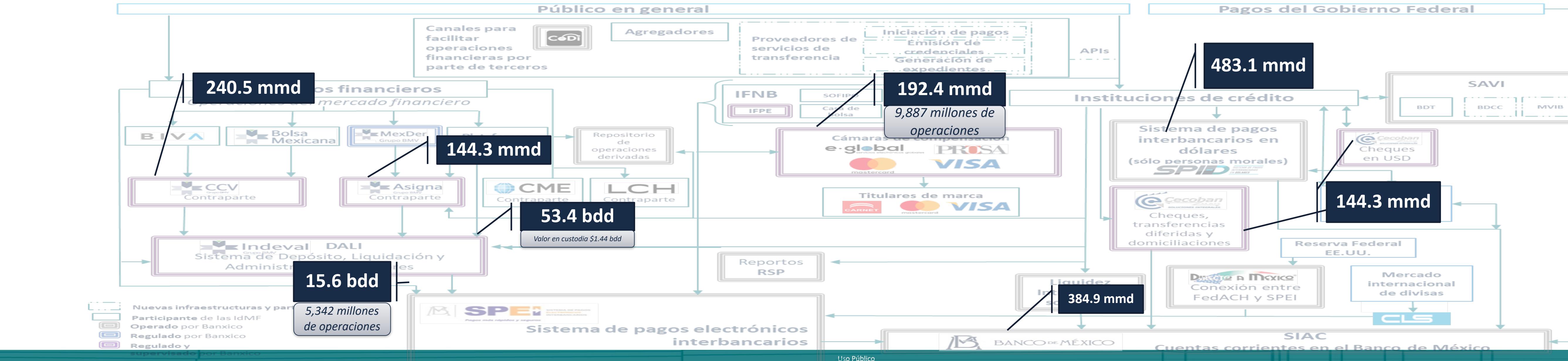


La **estabilidad y aceptación de la moneda**, debido a que el buen funcionamiento de las IMF es un requisito previo para la **confianza de los usuarios y el público inversionista**.

Ejemplo. Panorama de las IMF en México



Ejemplo. Panorama de las IMF en México



Ejemplo. Panorama de las IMF en México

Servicios que ofrecen el sistema de pagos nacional

Transferencias electrónicas instituciones financieras en tiempo real

Dispersión de pagos de nómina, programas sociales y proveedores de la tesorería de la federación

Liquidación de operaciones cambiarias en mercados internacionales

Liquidación en pesos de transferencias realizadas desde los EEUU

Soporte del esquema de entrega contra pago en operaciones con valores



Contenido



El contexto de las IMF



Riesgos ciberneticos



Tres lecciones

Riesgo cibernéticos. La paradoja de la modernización

La evolución hacia el sistema financiero digital, más rápido y más interconectado, lo expone a mayores riesgos cibernéticos.

Tema	Antes	Ahora	Impactos en la ciberseguridad
Procesos de liquidación	Liquidación de transferencias T + 1	Servicios de liquidación inmediata (“fast payments”)	Menor tiempo para reaccionar
Infraestructura	Operaciones “on – premise”	Servicios en la nube	Dependencia en varios proveedores
Medios	Dependencia del papel	Todo ocurre en ambientes virtuales	Fraudes pueden venir de todas partes del mundo
Interconectividad	Servicios financieros relativamente aislados	Servicios globales	Mayores efectos potenciales de propagación

Riesgo cibernéticos. Una preocupación constante

A nivel mundial

5º riesgo considerado de mayor severidad a corto plazo es la **guerra y espionaje cibernéticos**, según las empresas a nivel mundial

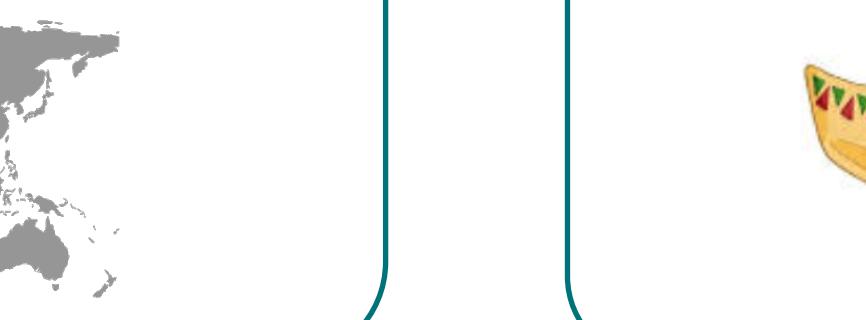
Fuente: The Global Risks Report 2025 del WEF



En Latinoamérica

42% de las organizaciones en Latinoamérica no tiene confianza en que su país esté preparado para responder a incidentes cibernéticos contra infraestructura crítica, la mayor desconfianza entre regiones

Fuente: Global Cybersecurity Outlook 2025 del WEF



En México

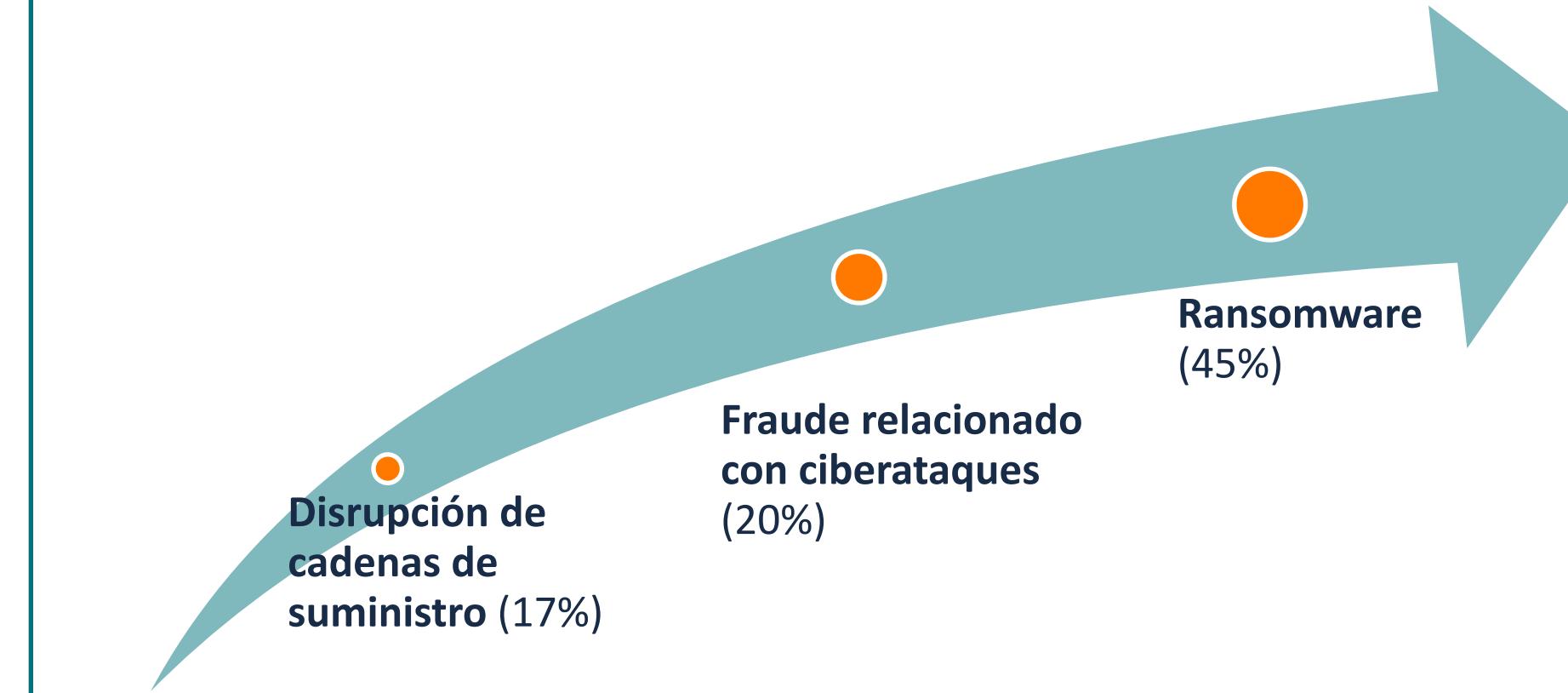
88%

de las instituciones financieras consideran los **riesgos cibernéticos y tecnológicos** entre las principales fuentes de riesgo no financiero

Fuente: Encuesta de riesgo sistémico de Banco de México, mayo de 2025



Principales preocupaciones sobre ciberseguridad de las empresas a nivel mundial

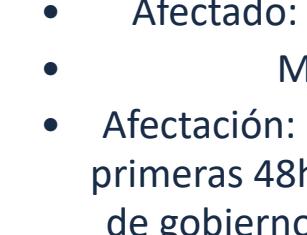


Fuente: WEF: "Global Cybersecurity Outlook 2025 INSIGHT REPORT"

Riesgo cibernéticos. Un riesgo persistente en el sistema financiero

Hackeo al Banco de Bangladesh (2016)

- Afectado: banco central de Bangladesh
- Método: ingeniería social para ganar acceso a la red *Swift*
- Afectación: USD \$81M



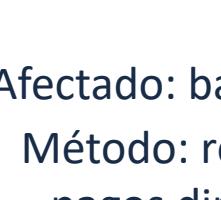
Participantes del SPEI (2018)

- Participantes del SPEI
- Método: vulnerabilidades en los aplicativos de conexión



Hackeo al gobierno de Costa Rica (2022)

- Afectado: 30 instituciones de gobierno
- Método: *ransomware*
- Afectación: pérdidas por USD 125M en las primeras 48hrs y disrupción de los servicios de gobierno por dos meses (no se pagó el rescate)



Hackeo al Banco de Uganda (2024)

- Afectado: banco central de Uganda

• Método: redireccionamiento de pagos dirigidos a organismos internacionales

- Afectación: USD 16.8M



Hackeo a participante del sistema nacional de pagos de Brasil (2025)

- Afectado: bancos comerciales participantes en el sistema nacional de pagos del Banco de Brasil
- Método: A través del proveedor de tecnología *C&I Software*
- Afectación: US \$140M



Uso Público

Información de acceso público.

Riesgo cibernéticos. Cuatro características clave

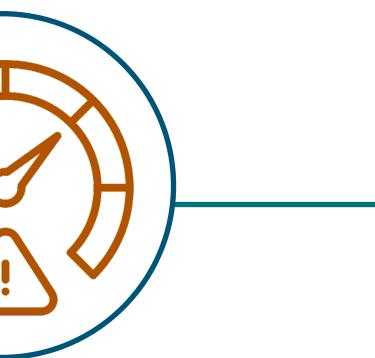
La evolución hacia el sistema financiero digital, más rápido y más interconectado, lo hace más expuesto a cuatro características de los riesgos cibernéticos:



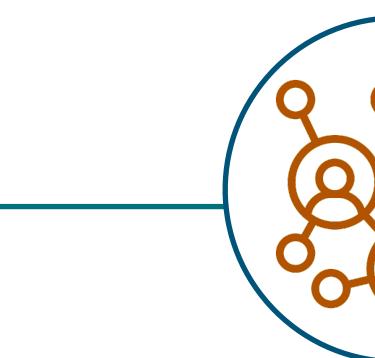
La naturaleza sofisticada y persistencia de los ataques



Variedad de puntos de acceso a través de los cuales una IMF podría verse comprometida



Algunas estrategias de continuidad del negocio son ineficaces en contextos de ciberseguridad



Los ciberataques pueden ser sigilosos y propagarse rápidamente dentro de una red de sistemas.

Contenido



El contexto de las IMF



Riesgos ciberneticos

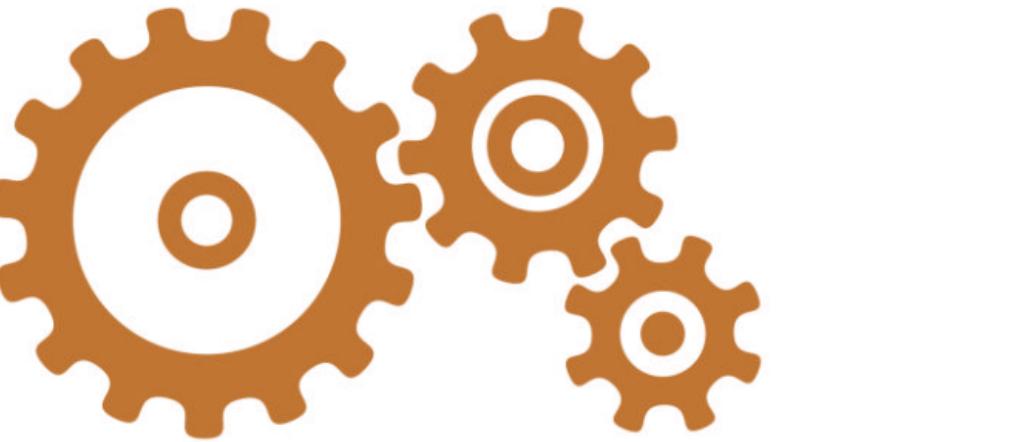


Tres lecciones

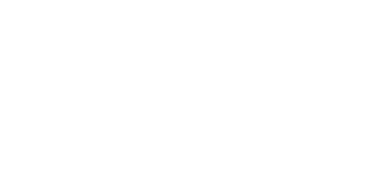
Visiones aisladas no funcionan

¿Por qué?

El éxito es multifactorial



¿Qué estamos haciendo?



Marco de gobernanza

- Involucramiento desde arriba
- Estrategia de ciberseguridad
- Tres líneas de defensa
- Áreas independientes de ciberseguridad



Tecnología

- Actualización constante
- Considerar esquemas alternativos para evitar puntos únicos de falla.



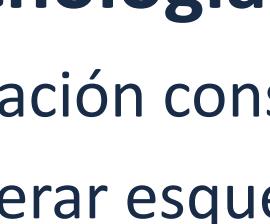
Procesos

- Controles
- Esquemas de coordinación a distintos niveles (entre áreas, autoridades, con participantes).



Personas

- Concentración
- Capacitación
- Pruebas de confianza



El papel no es suficiente

¿Por qué?

El factor humano, ningún evento es igual al anterior



¿Qué estamos haciendo?

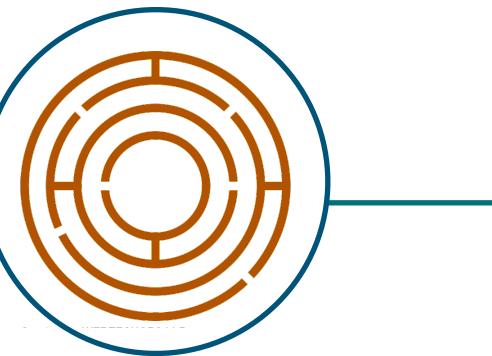


Pruebas, pruebas y más pruebas

- Sobre protocolos de actuación y comunicación
- Pruebas sobre los desarrollos (caja negra, caja blanca)
- Penetración
- Red team
- Operaciones de operación en sitio alternativo
- Internas, con participantes y con otras autoridades

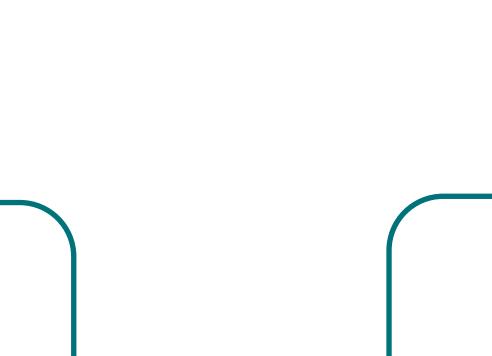
Reflexiones finales: ¿Esperamos un futuro más sencillo?

La complejidad tiende a aumentar (mayor conectividad, nuevos jugadores en el mercado)



mayor
n
ctivos,
ntes)

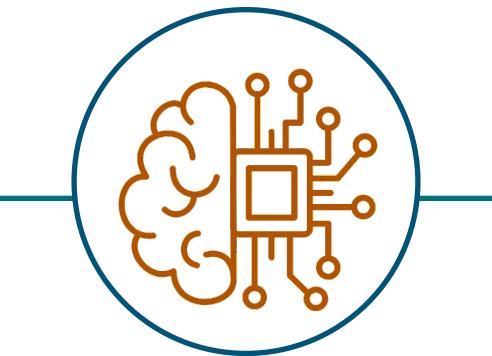
Alta depen
proveedo
(servic
sistem



100

ia en ciencia tecnológico la nube erativos

Incertidumbre nuevas tecnol (cómputo cuá ntico, IA)



Referencias

- Amerise, A. (2022). «Estamos en guerra»: 5 claves para entender el ciberataque que tiene a Costa Rica en estado de emergencia. BBC News Mundo. <https://www.bbc.com/mundo/noticias-america-latina-61516874>
- Ayres, M. (2025). Cyberattack on Brazil tech provider affects reserve accounts of some financial institutions. Reuters. <https://www.reuters.com/world/americas/brazils-cm-software-hit-by-cyberattack-central-bank-says-2025-07-02/>
- Banco de México. (2025). Reporte de Estabilidad Financiera: Junio 2025. <https://www.banxico.org.mx/publicaciones-y-prensa/reportes-sobre-el-sistema-financiero/%7B018CA111-CB56-EC25-9554-69F482C51492%7D.pdf>
- EY & IIF. (2025). Agility in volatility: Rebalancing CRO priorities in a shifting risk matrix: 14th annual EY/IIF global bank risk management survey. <https://www.ey.com/content/dam/ey-unified-site/ey-com/en-gli/insights/banking-capital-markets/documents/ey-and-institute-of-international-finance-bank-risk-management-survey-02-2025.pdf>
- Gartner. (2024). Gartner Forecasts Global Information Security Spending to Grow 15% in 2025. <https://www.gartner.com/en/newsroom/press-releases/2024-08-28-gartner-forecasts-global-information-security-spending-to-grow-15-percent-in-2025>
- Hammer, J. (2018). The Billion-Dollar Bank Job. The New York Times. <https://www.nytimes.com/interactive/2018/05/03/magazine/money-issue-bangladesh-billion-dollar-bank-heist.html>
- IBM. (2025). Cost of a Data Breach Report 2025: The AI Oversight Gap. <https://www.ibm.com/downloads/documents/us-en/131cf87b20b31c91>
- IMF. (2024). Global Financial Stability Report: The Last Mile: Financial Vulnerabilities and Risks. <https://www.imf.org/en/Publications/GFSR/Issues/2024/04/16/global-financial-stability-report-april-2024>
- Kharpal, A. (2023). China's ICBC, the world's biggest bank, hit by cyberattack that reportedly disrupted Treasury markets. CNBC. <https://www.cnbc.com/2023/11/10/icbc-the-worlds-biggest-bank-hit-by-ransomware-cyberattack.html>
- Lloyd's. (s. f.). Counting the economic cost: How vulnerable could you be? <https://www.lloyds.com/insights/futureset/futureset-insights/systemic-risk-scenarios/illuminating-cyber-crime/economic-impact>
- Reuters. (2025). Uganda detains 9 finance ministry officials over central bank hack. <https://www.reuters.com/world/africa/uganda-detrains-9-finance-ministry-officials-over-central-bank-hack-2025-02-05/>
- The Noun Project. (s. f.). Free Icons and Stock Photos For Everything. <https://thenounproject.com/> [Imágenes]
- WEF. (2025a). Global Cybersecurity Outlook 2025 Insight Report. https://reports.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2025.pdf
- WEF. (2025b). Global Risks Report 2025. https://reports.weforum.org/docs/WEF_Global_Risks_Report_2025.pdf

