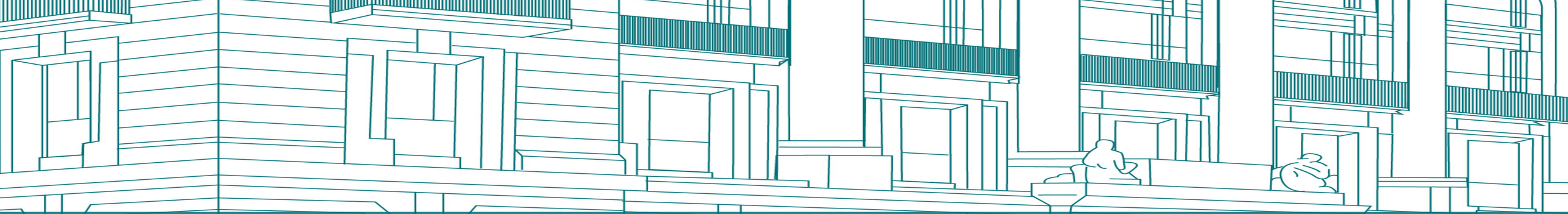


Preparación Ante Ciberataques con Simulacros de Crisis

Pavel Solís

Estado: Final
Unidad Administrativa: DEF
Fecha de última actualización: 12-Sep-2025

BANCO DE MÉXICO®

Uso Público

Información de acceso público.

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

Ciberataques: Una Amenaza Latente

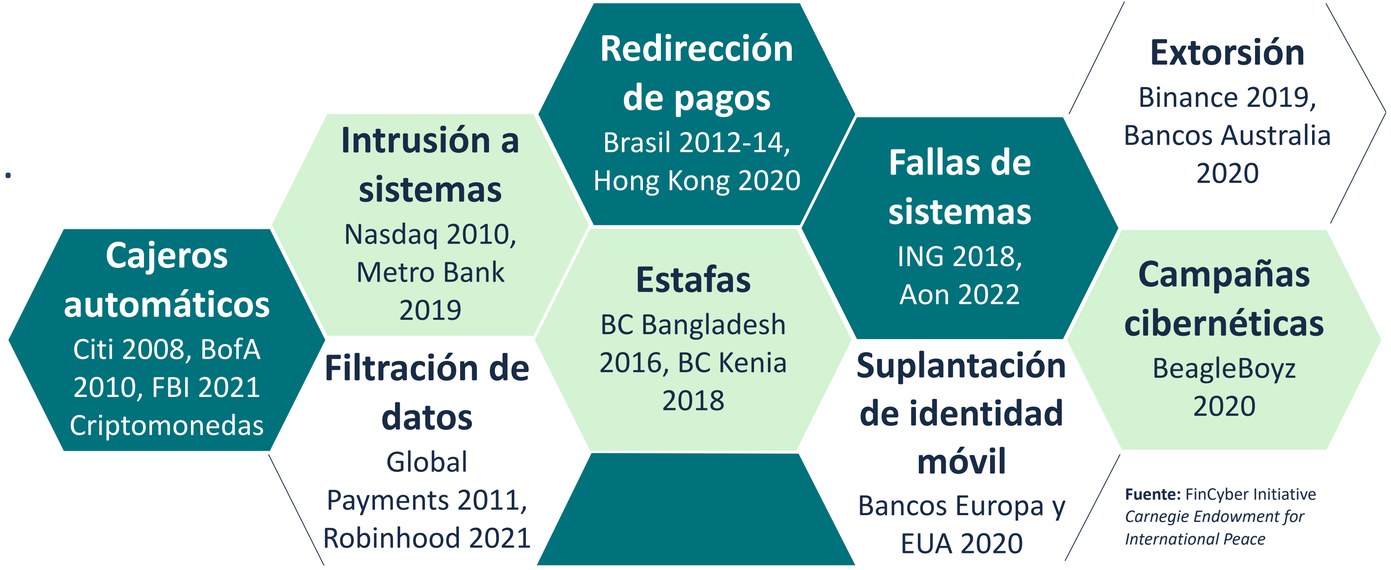
- Rápida **digitalización** del sistema financiero.
  - Usuarios de servicios financieros en línea y vía dispositivos móviles en **aumento**.
- Sistemas financieros están altamente **interconectados**.
  - Interdependencias aumentan **vulnerabilidad** ante ciberamenazas.
- El riesgo cibernético puede afectar la estabilidad financiera (G20 2017).
  - Ciberataques pueden propagarse **rápidamente** con implicaciones **sistémicas**.

Información de acceso público.

Ciberataques al Sector Financiero

- Industria financiera, uno de los sectores más atacados.

- Ciberataques aumentan en:
  - Frecuencia.
  - Sofisticación.
  - Modalidad.



Fuente: FinCyber Initiative *Carnegie Endowment for International Peace*

Amenazas Actuales

Ataques de día cero
Google Chrome (2022, 2023)
Windows (2023)
SharePoint (2025)

Ataques de *ransomware* avanzados
Proveedores de *ransomware* como servicio (RaaS)

Ataques a dispositivos con internet (IoT)
Asistentes inteligentes y enrutadores Wi-Fi constantemente conectados

Computación cuántica
Pone en peligro tecnologías de cifrado actuales

Inteligencia Artificial (IA)
Falsificaciones finas (imágenes, voz, IDs), persuasión dañina

Exposición a terceros
SocialArks (2021)
Facebook
Instagram
LinkedIn
CrowdStrike (2024)

Información de acceso público.

¿Qué Hacer ante una Amenaza Latente?

- No es cuestión de si sucederá o no …

  sino de cuándo y qué tan grave será.

- Ante una amenaza latente … prepararse.
  - Detección.
  - Protocolos.
  - Comunicaciones.

Cómo Prepararse ante Ciberataques (1/2): Antígenos

- Ataques reales controlados en colaboración con *hackers* ‘buenos’ (*white-hats*).
  - “A veces, es necesario demostrar una amenaza para desencadenar la solución”

    Barnaby Jack (1977-2013)

  - Elazari (2014), "Hackers: The Internet's Immune System".

  - Banco de Inglaterra: Ataques encubiertos a instituciones seleccionadas.

Información de acceso público.

Cómo Prepararse ante Ciberataques (2/2): Simulacros de Crisis

- Misma idea, diferentes enfoques.
  - Cadenas de correos para simular crisis financieras.
    - Resoluciones bancarias, acceso a liquidez de emergencia del banco central (marzo 2023).
  - Ejercicios de escritorio *(tabletop)* para analizar respuestas a incidentes y recuperación a crisis.
    - Ejercicios militares (*war games*), calabozos y dragones (*RPGs*), ciberataques a una institución.

- Simulacros de crisis de ciberseguridad con un enfoque de **estabilidad financiera**.

Información de acceso público.

Ventajas

- Permiten identificar y rectificar **debilidades** en **planes**.
  - Antes de que un incidente suceda.
  - En entorno controlado de bajo riesgo.
  - Sin consecuencias reales.
- Participantes aumentan su **preparación**.
- Fomentan el trabajo en equipo y mejoran la **coordinación**.

Desventajas

- Periodos de planeación prolongados.
- Con cadena de correos:
  - Queda registro (puede inhibir discusión abierta).
  - Correos pueden pasar desapercibidos.
  - Decisiones pueden salirse del guion.
- Ejercicios de escritorio requieren a facilitador experimentado.

Información de acceso público.

Funcionamiento

- Ejercicios de simulación basados en la argumentación y toma de decisiones para navegar escenarios hipotéticos.
  - Un **facilitador** experimentado presenta a los participantes un escenario extremo pero plausible (lo más realista posible).
  - Participantes toman decisiones críticas sin presión, y se les pide que analicen sus respuestas.
  - El facilitador guía la discusión y fomenta la participación, asegurándose de que siga el rumbo del escenario.
- Los participantes actúan como si la situación sucediera en la vida real.
- Los participantes a menudo son responsables de roles clave en la respuesta a incidentes y gestión de crisis.

Información de acceso público.

Buenas Prácticas

- Involucrar a participantes (sectores) y equipos **diversos** (TI, finanzas, cumplimiento regulatorio, comunicación).
  - Tratar información compartida con el facilitador como **confidencial**.
  - No exponer **vulnerabilidades** entre participantes del sector privado.
  - No identificar individualmente a participantes o instituciones en el reporte final.
- Realizarlos **periódicamente**, al menos una vez al año.
  - Incorporar **lecciones** aprendidas de los ejercicios previos.
  - Dar **seguimiento** a la implementación de las recomendaciones.

Información de acceso público.

Características

- No son ejercicios técnicos.
- No son ejercicios que se aprueban o reprueban.
- No son ejercicios de supervisión.
  - Autoridades no recolectan información de los participantes de la industria durante el ejercicio.
- Todos los participantes (autoridades e industria) ponen a prueba sus protocolos de respuesta a incidentes.
- Discusiones bajo la regla de *Chatham House* (opiniones libres porque no hay atribución).

Información de acceso público.

Objetivos

- Poner a prueba los protocolos de **respuesta** de los participantes ante un ciberataque.
- Poner a prueba los canales de **comunicación** al interior y entre los participantes.
- Identificar los canales de **propagación** de incidentes.
- Identificar áreas de **mejora** tanto a nivel individual como colectivo.
- Poner a prueba la preparación de las autoridades para una **resolución** detonada por un incidente de ciberseguridad.

Información de acceso público.

Simulacros de Crisis de Ciberseguridad en México

- Recomendación CESF (2019) y FSAP (2022).

- Enfoque progresivo.
  - **Jun 2023:** Solo autoridades (1 día).
  - **Jul 2024:** Autoridades y bancos (2 días).
  - **Oct 2025:** Autoridades e infraestructuras financieras (3 días).
  - **Adelante:** Autoridades y diferentes intermediarios financieros.

Información de acceso público.

Diseño

1. **Lineamientos.** Encargado del proyecto y facilitador definen lineamientos.
2. **Escenario.** Equipo interdisciplinario desarrolla escenario y preguntas, redacta invitaciones.
3. **Sesión informativa.** Dinámica del ejercicio y respuesta a preguntas de la industria.
4. **Ejecución.** Facilitador presenta escenario y facilita discusiones.
5. **Reporte final.** Hallazgos y recomendaciones.

Logística. Agenda, convocatorias, sede, accesos, preparativos.

Información de acceso público
Información cuyo acceso está restringido a un grupo limitado de personas empleadas por el Banco de México y, en su caso, personas ajenas al mismo.

Escenarios

2023

Secuestro de datos (***ransomware***) a un banco ficticio basado en un banco mediano existente.

- **Día 1.** Solo autoridades.

2024

Programa malicioso (***malware***) infecta a un proveedor de servicios ficticio que genera reportes regulatorios a los bancos.

- **Día 1.** Solo autoridades.
- **Día 2.** Autoridades y 5 bancos.

2025

Secuestro de datos (***ransomware***) a una infraestructura sistémica.

- **Día 1.** Solo autoridades.
- **Día 2.** Autoridades e infraestructura afectada.
- **Día 3.** Autoridades y otras infraestructuras sistémicas.

Información de acceso público.

Ejemplos

Hora	Eventos
7:00	• Noticieros de radio comentan incidentes del banco. • Clientes no pueden acceder a sus cuentas (actividad masiva en redes sociales).
10:30	• El banco informa <u>únicamente</u> a una autoridad que no puede acceder a sus bases de datos.

Hora	Eventos
08:30	• Proveedor informa a sus clientes que le tomará un par de días restaurar sus sistemas y generar los reportes.
09:00	• Autoridades siguen sin recibir los reportes regulatorios del día anterior.
09:15	• Algunos bancos (clientes del proveedor) detectan un programa malicioso en sus sistemas.

Lecciones: Mejores Prácticas

- Implementar **protocolos robustos** de ciberseguridad.
  - Contraseñas robustas, autenticación multifactorial, accesos controlados, respaldar y encriptar información, actualizar programas, instalar cortafuegos, capacitar empleados, planes de respuesta a incidentes, auditorías de ciberseguridad, pensar como atacante.
- Poner a prueba **frecuentemente** la capacidad de respuesta y coordinación ante una crisis bajo diferentes escenarios.
  - Revela deficiencias y áreas donde se requiere mayor preparación.
- **Plataforma** para intercambiar información sobre incidentes en tiempo real entre autoridades y sector privado (MISP).
  - Mejora la preparación, facilita toma de decisiones, crucial para respuesta eficaz, lenguaje común, reportes estandarizados.

Información de acceso público.

Lecciones: Colaboración

- Autoridades financieras deben fomentar la coordinación y cooperación entre los actores públicos y privados.
- **Foro de coordinación** en ciberseguridad con perspectiva de estabilidad financiera (escalamiento).
  - Formalizar protocolos de las autoridades para determinar si un evento pudiera tener implicaciones sistémicas.
- **Marco de respuesta de las autoridades** para incidentes ‘sistémicos’ y ponerlo a prueba frecuentemente.
  - Objetivo: Coordinar la actuación de autoridades, industria y proveedores de servicios.
  - Industria debe tener claridad sobre cuándo o cómo involucrarse.

Información de acceso público.

Lecciones: Anticipación

- Abordar preguntas relevantes y difíciles con **anticipación**.
  - El tiempo es escaso en crisis.
  - Definir con anticipación una **estrategia de comunicación** que mitigue el impacto negativo bajo diferentes escenarios.
  - Mitigar efectos de **contagio** dada la interconectividad.
- Reconocer la importancia de los **proveedores externos críticos**.
  - Lista de contactos, proveedores alternos para continuidad de servicios, mecanismos para fomentar relación de trabajo.

Información de acceso público.

Conclusiones

- **Ciberataques**: Es cuestión de cuándo y qué tan grave serán.

- Ante una amenaza latente, **prepararse**.

Información de acceso público.

Información de acceso público