CONGRESO DE
PREVENCIÓN DEL FRAUDE Y SEGURIDAD

Construyendo **experiencias** desde un **entorno seguro.**

FECHA 15 - 16 DE NOVIEMBRE /2018
HOTEL GRAND HYATT BOGOTÁ

Raúl Morales

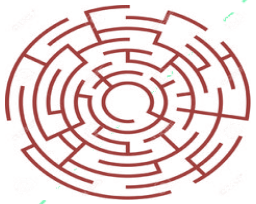
Ciberseguridad y la cooperación internacional

CEMLA, hub de banca central

- La única asociación de banca central de la región
  - Establecida en La Habana en 1952, 53 miembros a la fecha
  - "La misión de CEMLA es promover una mejor comprensión de cuestiones monetarias y financieras que son relevantes para la banca central de América Latina y el Caribe (ALC) “

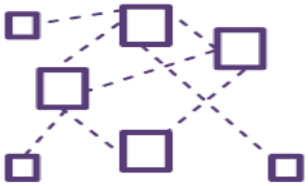
- CEMLA persigue esta misión mediante:
  - Promover el desarrollo de capacidades y el aprendizaje continuo;
  - Una agenda de investigación y discusión sobre cuestiones de política; y
  - Hospedar grupos de expertos técnicos y ofrecer un foro para el debate de temas de interés común.
    - Como resultado de estos grupos se han creado iniciativas regionales diversas como el FOCOSC.

Riesgo cibernético: un llamado de atención para la comunidad internacional



Sofisticación

Difícil de identificar o erradicar, difícil de determinar amplitud del daño.



Sin barreras

Proveniente de una amplia gama de puntos de entrada (instituciones, FMI vinculadas y terceros proveedores de servicios).

Disruptivo

Puede causar interrupciones significativas en el sistema financiero o en la economía, lo que puede llevar a un riesgo sistémico.

Silencioso

Imperceptible y capaz de infiltración y expansión sumamente rápidas

Source: CPMI, BIS (2017)

Ataques recientes a sistemas de pago

Bangladesh Bank

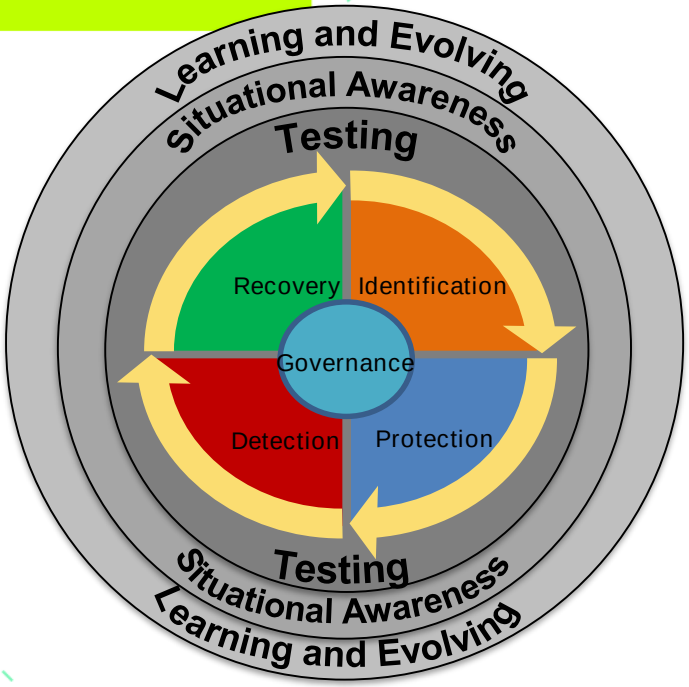
Banco de Chile

SPEI de Mexico

"El fraude en SIPS se está volviendo cada vez más sofisticado y se espera que evolucione más. Necesitamos movernos rápido, y juntos, para evitar cualquier pérdida de confianza en el sistema ".

Prácticas y coordinación internacionales

…68%



y 60%

76% de miembros del FSB

EUROPEAN CENTRAL BANK
EUROSYSTEM

> 15 países

Source: FSB (2017)

Desarrollando un marco de trabajo

- Compromiso institucional al más alto nivel. El riesgo cibernético debe integrarse en la agenda de los órganos de gobierno y en el marco de gestión de riesgos de toda entidad pública o privada.
- La gobernabilidad es decisiva. Dado que todos manejan, generan, reciben y almacenan datos, o tienen acceso a la información, las políticas y estrategias deberían abarcar todo en cada institución.
- Concientización y cultura sobre la seguridad cibernética entre el personal debe ser parte de cualquier esfuerzo para fortalecer la seguridad cibernética. Muchos ataques cibernéticos utilizan puntos de entrada impulsados por humanos.
- Las regulaciones cibernéticas deben exigir que las entidades, terceros y la industria en general desarrollen marcos de control y respuesta eficaces, comprobables y proactivos para hacer frente al riesgo cibernético
- Promover una mayor colaboración con la industria para mejorar las prácticas de ciberseguridad y lograr la cooperación transfronteriza y la armonización de las prácticas.

El FOCOSC del CEMLA

Foro regional sobre ciberseguridad

- 15 bancos centrales miembros, +50 usuarios
- Reuniones virtuales (inc. comunicación con la industria)

Lecciones aprendidas

- Establecer un marco de trabajo y gobernanza apropiados y medidas específicas flexibles pero efectivas para prevenir, detectar y responder a eventos que vulneren información, servicios y procesos críticos.
- Conciencia y la cultura entre el personal de las instituciones. Los ciberataques han demostrado que el factor humano es decisivo.
- Mayor colaboración transfronteriza para intercambiar información relevante y armonizar prácticas, con el fin de mejorar el entorno de ciberseguridad global.
- Responsabilidad compartida. Cada actor debe proteger su propio entorno, hacer cumplir los controles con terceros y compartir información con las autoridades para anticipar más riesgos.