Ciberejercicios

Para el Sistema Financiero

2019

BANCO CENTRAL
DE LA REPÚBLICA ARGENTINA

Agenda

1 | Ciberejercicios – Para que?

2 | Ejercicio del 2018 – Objetivo, Explicacion y Hallazgos

3 | Ejercicio del 2019- Objetivo, Explicacion y Hallazgos

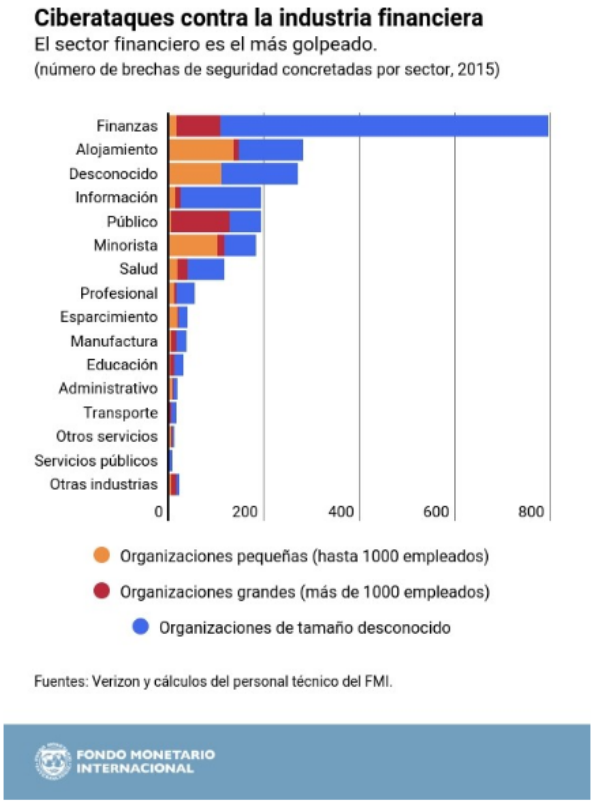
4 | Recomendaciones generales y técnicas – Lecciones aprendidas

Ciberejercicio del Sistema Financiero

Ante el fuerte proceso de innovación tecnológica que sufren los servicios financieros, aparecen mayores beneficios pero también nuevos riesgos. Con el fin de evitar un eventual disrupción que pudiera afectar la Estabilidad financiera, diversos foros internacionales impulsan acciones.

FMI 2017

Fuente :https://blog-dialogoafondo.imf.org/?p=8448



El ciber riesgo en el FMI y WEF

Global Risks Report

North America
The risks of greatest concern for doing business

	rank
Cyber attacks	1
Terrorist attacks	2
Asset bubble	3
Fiscal crises	4
Failure of climate change adaptation	5

Source: Executive Opinion Survey 2017, World Economic Forum

- **El riesgo cibernético es un desafío creciente. Entonces, ¿cómo podemos prepararnos?**

Fuente: https://www.weforum.org/agenda/2018/01/our-exposure-to-cyberattacks-is-growing-we-need-to-become-cyber-risk-ready/

- **Estimación del riesgo cibernético en el sector financiero**

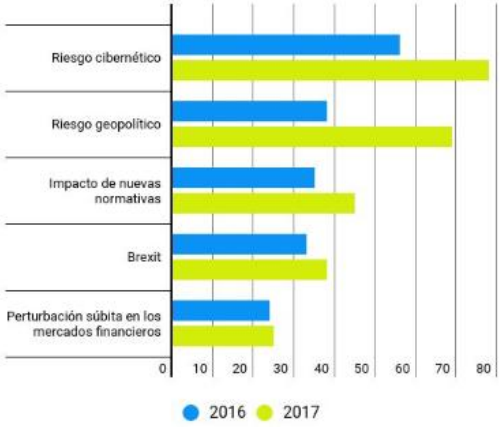
Por Christine Lagarde 2018

Fuente: https://blog-dialogoafondo.imf.org/?p=9460

El riesgo cibernético ocupa el primer lugar en las encuestas

Los gestores de riesgo y otros directivos del sector financiero observan que la amenaza de ataques cibernéticos va en aumento y representa un riesgo superior al planteado por los acontecimientos geopolíticos y las nuevas normativas.

(porcentaje de encuestados)



Fuente: Encuesta preparada por Depository Trust & Clearing Corp., publicada como DTCC Systemic Risk Barometer, primer trimestre de 2017.

FONDO MONETARIO INTERNACIONAL

Ciberejercicio del Sistema Financiero

Además…

FSB FINANCIAL STABILITY BOARD

ABOUT THE FSB | WHAT WE DO | PUBLICATIONS | PRESS

Home > Publications > Consultation Documents > Cyber Lexicon Consultative Document

Cyber Lexicon Consultative Document

Available as: PDF

Comisión Europea

G20 ARGENTINA 2018

CEMLA
CENTRO DE ESTUDIOS MONETARIOS LATINOAMERICANOS

FSB FINANCIAL STABILITY BOARD

Table 1: Recent cyber-attacks on central banks

Institution	Year	Type of attack	Details
Federal Reserve Bank of Cleveland	2010	Data breach	Theft of 122,000 credit cards
Federal Reserve Bank of New York	2012	Data breach	Theft of proprietary software code worth USD 9.5 Million
Sveriges Riksbank	2012	Business Disruption	Distributed Denial of Service (DDoS) attack left the website offline for 5 hours
Banco Central del Ecuador	2013	Fraud	USD 13.3 Million stolen from the account of the city of Riobamba at the central bank
Federal Reserve Bank of Saint Louis	2013	Data breach	Publication of credentials of 4,000 US bank executives by Anonymous
Central Bank of Swaziland	2014	Fraud	Theft of USD 688,000
ECB	2014	Data breach	20,000 email addresses and contact information compromised
Norges Bank	2014	Business Disruption	DDoS attack on seven large financial institutions, resulting in suspended services during a day.
Central Bank of Azerbaijan	2015	Data breach	Theft of thousands of bank customers' information
Bangladesh Bank	2016	Fraud	The SWIFT credentials of the Bangladesh central bank were used to transfer USD 81 Million from its account at the FRBNY. Hackers tried to steal USD 951 Million.
Bank of Russia	2016	Fraud	21 Cyber-attacks aimed at stealing USD 50 Million from correspondent bank accounts at the central bank, resulted in a loss of USD 22 Million.
Bank of Italy	2017	Data Breach	Hack of email accounts of two former executives.

Source: ORX News

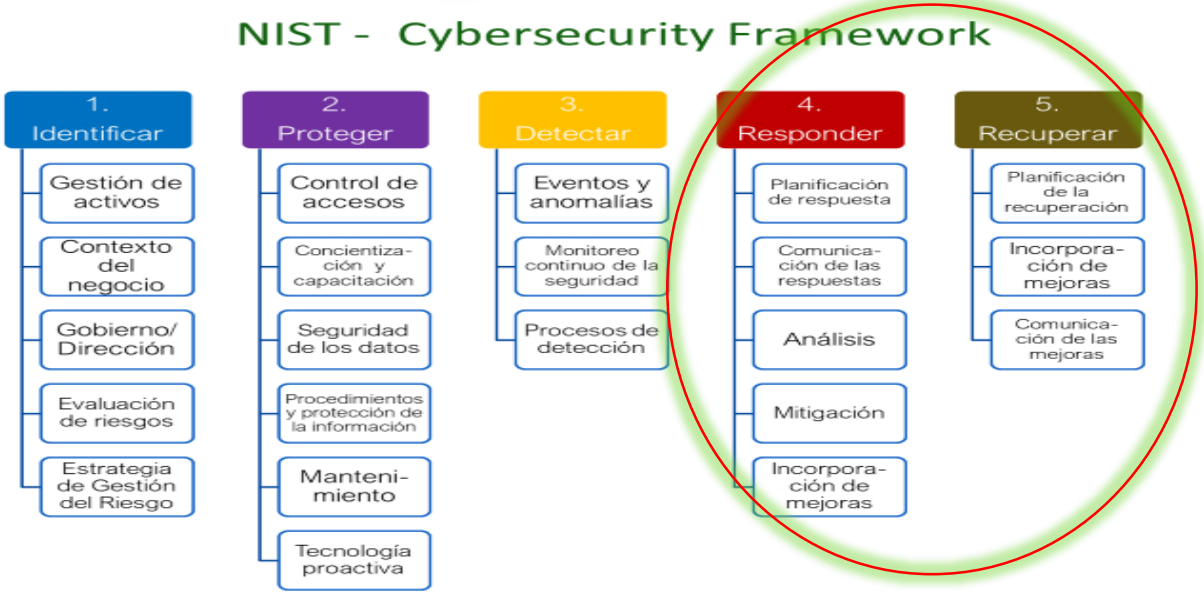
FMI 2018

https://www.imf.org/en/Publications/WP/Issues/2018/06/22/Cyber-Risk-for-the-Financial-Sector-A-Framework-for-Quantitative-Assessment-45924

CIRR - (Cyber Incident Response and Recovery)
Grupo de Trabajo en Respuesta y Recuperación ante incidentes del FSB

Ciberseguridad – Estándares

NIST - Cybersecurity Framework



Ciberejercicio, ¿para qué?

- *Ejercicio de simulación que plantea un caso mediante situaciones que deberían ser lo mas reales posibles con distintas finalidades.*
- *Concientizar que se requiere la acción de equipos multidisciplinarios que puedan abordar la crisis cubriendo la mayor cantidad de aspectos involucrados.*
- *Es ideal que se planifiquen de manera proactiva acciones de respuesta ante incidentes provocados por ciberataques, con el propósito de mitigar el impacto en la mayor medida posible.*
- *Importante: Los ciberejercicios no tienen resultados correctos o incorrectos, es el momento para encontrar puntos de mejora para los planes y procedimientos implementados.*

Objetivos del ciber ejercicio

Que las EEFF revisen sus planes de respuesta a incidentes

Probar la comunicación

- *Entre las áreas internas de los bancos.*
- *Entre cada idénticas áreas de los distintos bancos.*
- *Del BCRA con el resto de los Bancos.*

Medir las acciones necesarias para mitigar impactos evitando que el problema se propague a todo Sistema financiero.

Aspectos destacados - Actividades y Roles -

EEFF Participantes: 6 voluntarias

Roles: 5 por EEFF

- *Operaciones de Pago*
- *Prensa*
- *Seguridad de la Información*
- *TI*
- *Legales*

+5 meses de planificación |+50 reuniones (internas y externas)
+125 personas en total –

Rol del BCRA en el ciberejercicio 2018 -

- *Como Autoridad de aplicación: para ensayar como seria el rol de recibir información de un incidente grave, eventualmente compartirla con el sistema financiero y coordinar actividades.*
- *Como una entidad más para autoevaluar sus procesos.*
- *Como administrador del Sistema de pagos Local.*

Aspectos destacados – Recursos y actividades.

Recursos y actividades provistos por el Banco quien coordino el ejercicio, recursos del Área corporativa *dedicada específicamente a ciber ejercicios*.

- 2 Expertos internacionales en ciberjercicios asistiendo en todas las reuniones + especialistas locales.
- Gestion de las reuniones y lugar físico para las mismas.
- Preparacion y prueba de un playbook borrador.
- Los casos para el ejercicio fueron preparados por los expertos y los asistentes locales.
- Generación de informes finales y convenio de confidencialidad.

Planteo del ciberejercicio.

- *Cada Institución se reunió en sus instalaciones en una oficina con 5 puesto de trabajo para los integrantes del equipo.*
- *En una plataforma específica para realizar ejercicios a distancia, se simulaban las redes informaticas de las Entidades participantes, recibiendo correos electrónicos, Twits de activistas o clientes, solicitudes de transferencias, etc.*
- *Cada organización planteaba su "respuesta" a las actividades que lo requerían a través de la plataforma, de forma de hacer una autoevaluación de su reacción y procedimientos.*
- *Durante el juego se pautaron reuniones intermedias con distintas áreas (prensa, operaciones de pago, Seguridad, etc.)*

Puntos generales a incluir en los planes de crisis.

- *Se requiere identificar parámetros o indicadores que señalen situaciones anómalas para que las áreas de Pago notifiquen a las áreas de Ciberseguridad.*

- *Es necesario establecer definiciones de criticidad de estas situaciones anómalas para la eventual convocatoria de un comité de crisis (evento, incidente, crisis).*

- ***Surge la necesidad de establecer un mecanismo para reportar problemas originados en incidentes de ciberseguridad*** *(metodología, protocolo, canal, interlocutores válidos, etc.)* ***para evitar su propagación al resto del sistema. Acciones preventivas.***

A impulsar desde el BCRA

- *Promover la cultura de ciberseguridad y ciberresiliencia.*
- *Impulsar este tipo de ejercicio para ensayar las acciones en casos de ciberincidentes graves.*
- *Proponer circuito para informar incidentes, compartir información, establecer protocolos conjuntos con otros organismo, definir alertas, asistencias, comunicación, etc.*

Objetivos del ciberejercicio 2019

- *Promover mayor concientización, comunicación y coordinación entre los distintos actores del sistema financiero para mejorar las capacidades de respuesta y recuperación ante incidentes de ciberseguridad.*
- *Probar el circuito para informar los incidentes.*
- *Chequear la comunicación ante incidentes y proponer mejoras*

Aspectos destacados - Participantes

BCRA Coordinador y líder.

5 EEFF seleccionadas por su importancia sistémica

7 integrantes por equipo EEFF

- *Seguridad de la Información y TI*
- *Legales*
- *Servicios financieros (plazo fijo web)*
- *Prensa*
- *Riesgo (optativo)*

Aspectos destacados - Participantes

Mesa de Coordinación y liderazgo :BCRA

Veedores:
Integrantes del Comité de Ciberseguridad Nacional.

Participantes Banco Central:

- *GP Estabilidad Financiera*
- *GP de Sistemas de Pago*
- *GP Protección Usuario de Servicios Financieros.*
- *GP Comunicación Estratégica*
- *G. A. Externa de Sistemas*
- *G. Administrativa Judicial*

Soporte metodológico/ facilitador Accenture

Características del ejercicio:

- *Anonimato: Los equipos no fueron identificados con su nombre real y los integrantes de una entidad pertenecían al mismo equipo.*

- *La situación simulada se usa (una excusa) para ejercitar la reacción ante incidentes de ciberseguridad, no es objetivo explorar los detalles operativos ni técnicos del caso planteado.*

- *Concientización de todas las áreas sobre "cómo pueden escalar los problemas de seguridad informática".*

- *El ejercicio llevo un dia completo en instalaciones del BCRA*

- *Se firmaron acuerdos de confidencialidad.*

Aspectos a analizar y Resultados:

El objetivo era que las entidades participantes prueben sus planes ante incidentes y analizar los flujos de comunicación

- *Interna (entre distintas áreas de las entidades)*
- *Entre entidades (distintas áreas)*
- *Con el regulador*

durante un incidente de ciberseguridad que pueda desencadenar un problema sistémico, se observaron los siguientes elementos:

- *Detalle de comunicaciones de las entidades con externos*
- *Flujo de comunicaciones externas*
- *Canales utilizados*

Hallazgos en las comunicaciones de la Actividad 1:

- *La gran mayoría se comunicó directamente con el BCRA, mientras que uno de los equipos recurrió a una Asociación con el objetivo de coordinar alguna respuesta.*
- *En la primera parte de la actividad 1 , el 80% de las entidades se comunicó con la Compensadora desde sus respectivas áreas de IT.*
- *El 60 % se comunicó con el Banco Atacado (Banco Z en el ejercicio) para consultar por el estado de las transacciones de los plazos fijo web.*
- *El 40 % de los equipos no se contactaron con el Banco Atacado (Banco Z en el ejercicio) en la primera etapa de la actividad, sino después de conocerse el rumor de que el mismo poseía el problema. Estos mismos equipos especificaron que entraron en contacto directo con el CISO del Banco Atacado (banco Z en el ejercicio).*

Hallazgos en las comunicaciones:

- *Los dos sectores internos que lideraron la comunicación con los entes externos en cada equipo fueron los siguientes:*

A	**Prensa** | 33,3%	**Red de sucursales** | 28%
B	**Prensa** | 27%	**Comité de crisis** | 20%
C	**Prensa** | 21%	**Productos** | 21%
D	**IT** | 35%	**Prensa** | 26%
E	**Prensa** | 44%	**Negocio** | 22%

- *los canales más utilizados por todos los equipos fueron el teléfono y el mail*

Hallazgos en las comunicaciones de la Actividad 2:

- *Todos los equipos se comunicaron con el BCRA de forma directa.*
- *En esta actividad solamente un equipo se contactó con la compensadora.*
- *Todos los equipos se comunicaron con otros bancos, dos equipos especificaron haberse contactado directamente con los CISOs de otros bancos.*
- *Dos equipos formalizaron denuncias ante organismos de Justicia y Fuerzas de Seguridad.*

Hallazgos en las comunicaciones de la Actividad 2:

- *Los dos sectores internos que lideraron la comunicación con los entes externos en cada equipo fueron los siguientes:*

A	**Prensa** | 57%	**Comité de crisis** | 29%
B	**CISO Banco Z** | 55%	**Negocio** | 18%
C	**Legales** | 25%	**Banco Z** | 25%
D	**Prensa** | 40%	**IT** | 20%
E	**Áreas involucradas** | 44%	**CISO Banco Z** | 22%

- *Los canales más utilizados por todos los equipos fueron el teléfono y el mail*

¡ Muchas gracias !

Mara Misto Macias

Gerencia Principal de Seguridad de la Información para Entidades

E-mail: mmisto@bcra.gob.ar