Informe de Misión Oficial

De: Melissa Suárez

Jefe de Proyectos Especiales

Asunto: Jornada de Ciberseguridad en los mercados financieros Iberoamericanos

La Jornada sobre Ciberseguridad en los mercados financieros Iberoamericanos se celebró en la Ciudad de Cartagena, Colombia del 14 al 16 de noviembre de 2017, organizadas por el Instituto Iberoamericano de Mercados de Valores (IIMV) y la Agencia Española de Cooperación Internacional para el Desarrollo (AECID).

Los temas cubiertos durante la jornada fueron los siguientes:

DÍA 1

Ciber amenazas y tendencias 2017

Sesión en la que se expuso de parte de Pablo López, la evolución en las iniciativas de parte de España para fortalecer la ciberseguridad a nivel nacional.

Losataquesalacadenadesuministroseestánconvirtiendoenunatendenciapreocupante, siendo una forma muy efectiva de distribuir software dañino aprovechando la confianza entre usuarios y proveedores de software.

Se indica que las tendencias a considerar durante este año están el ciberespionaje, cibercrimen, hacktivismo y ciberyihadismo.

Debemos mejorar la vigilancia ya que los ataques seguirán creciendo y las tecnologías hay que utilizarlas pero se debe implementar la seguridad para combatir las vulnerabilidades.

Factores Facilitadores de los ciberataques:

- Falta de concienciación (éxito de la ingeniería social).
- Existencia de vulnerabilidades día cero.
- Sistemas heredados (legacy).
- Poco personal dedicado a seguridad.
- Mayor superficie de exposición: redes sociales, servicios en la nube, BYOD, movilidad.
- Poco proclives a comunicar incidentes.
- La atribución es complicada.

Infraestructuras críticas. Los mercados de valores

Ponencia por José Zuazua que abarca el marco legal en donde se establecen las infraestructuras críticas para el España (infraestructuras que proporcionan servicios esenciales) cuyo funcionamiento no puede ser alterado ya que tendrían un grave impacto en los servicios. También se establece el centro nacional para la protección de infraestructuras críticas el cual es responsable de la protección de las mismas.

Se recalca la importancia en realizar pruebas de seguridad a manera de encontrar vulnerabilidades internas.

En el ámbito de ciberseguridad con el Consejo Nacional del Mercado de Valores de España, se tienen riesgos tanto por las entidades emisoras, empresas de servicios de inversión y el propio supervisor. Un ciberataque a una de estas pueden repercutir con efectos negativos desde el registro de cuentas de valores y efectivo de los clientes como afectaciones a sistemas de pago.

En España el plan estratégico del sector financiero comprende una estructura en cuatro subsectores:

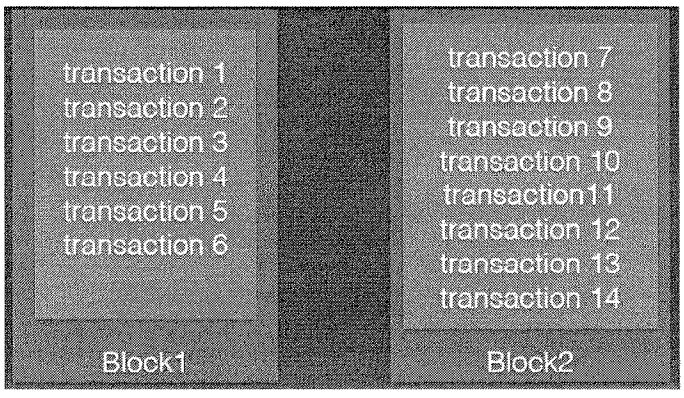
1. Sistemas y servicios de pagos.
2. Crédito y liquidez.
3. Servicios de inversión.
4. Seguros (cobertura de riesgos).

Bitcoin y Blockchain.

Ponencia por Alejandro Beltrán en donde se explica el origen del bitcon mediante un paper de Satoshi Nakamoto (seudónimo ya que la identidad es desconocida) en donde plasma el concepto de una versión peer to peer para transferir efectivo digital sin pasar por una institución financiera.

Se indica de parte del expositor que se introducen firmar digitales para que se pueda realizar un tracking de las partes que participan de esta transferencia. Una firma digital viene siendo una clave matemática cifrada que permite identificar a la persona y esta clave permite que cualquiera pueda comprobar a quién pertenece. Las firmas digitales resuelven parte del problema, pero el principal beneficio se pierde si se necesita un intermediario de confianza para prevenir "gastar la plata dos veces".

Con los blockchain se crean bloques para agrupar las transacciones de la siguiente manera:



Es decir es una base de datos en donde se van a almacenar las transasccciones.

El 23 de enero del 2009 se registra la primera transacción por un valor de 0.10 centavos.

Se conversa sobre los riesgos asociados al bitcoin:

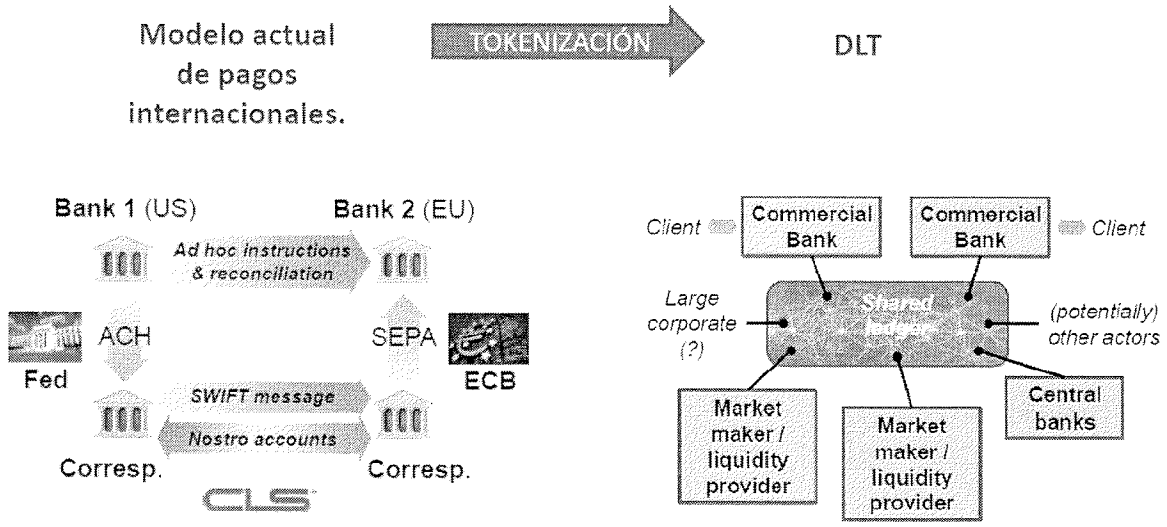
1. La compra de bitcoins y que luego el precio de los mismos caiga.
2. No almacenar o guardar correctamente los mismos lo que ocasione la pérdida mediante un robo.
3. Ciber delito y ciber lavado de dinero.

América Latina según las estadísticas nombradas tiene en puesto número uno a Chile con un 39% de ciberataques. Panamá ocupa el puesto número 3 con un 38%.

GAFI ya cuenta con recomendaciones relacionadas con el uso de tecnologías y nuevos métodos de pago.

Blockchain en los Mercados Financieros.

Esta ponencia se explica de parte de Francisco Del Olmo, el caso de uso del modelo actual vs el uso de DLT o blockchain:



Beneficios de contar con el uso de DLT en os mercados se pueden mencionar la inmediatez y el registro único ya que se utiliza una reconciliación de transacciones y se cuenta con una trazabilidad de las mismas.

Riesgos asociados está la información replicada (siempre que la red sea débil), las claves privadas, robo de llaves y tecnología basada en la criptografía entre otras.

Consideraciones y Panorama legal de Criptomonedas

Daniel Villaroel es el expositor de este tema en donde se enfoca los riesgos asociados a las cripto monedas.

Riesgos de las Cripto – Caso de ETH

Tipo	Valor tomado (USDMillones)	Número de víctimas
Phishing	115	16.900
Exploit	103	11.000
Hack	74	2.100
Ponzi Schemes	0.004	260
Total	225.4	30.260

Implementación de SGSI en la SMV y regulación para supervisados del Perú

Olga Suárez y Martín Heredia nos hablan sobre la experiencia de implementar el sistema de gestión de seguridad de la información para lograr la certificación en ISO 27001 en la SMV del Perú.

Entre las principales motivaciones para implementar la creación del SGSI se encontraban el aumento de amenazas y vulnerabilidades de software, entidades que se han convertido en el blanco de ciberataques, evolución de las tecnologías, nuevas regulaciones en la seguridad de la información entre otras.

Parte de las actividades preliminares para esta implementación consistieron en el diagnóstico de la situación actual, identificación de limitaciones y riesgos, factores críticos de éxito.

Se recalca que para lograr el éxito del proyecto se requirió de un alto sentido de liderazgo y compromiso al conformar el comité de gestión de seguridad de la información el cual fue presidido por el Superintendente.

La implementación del SGSI y certificación les tomó desde el año 2012 al 2016 (4 años).

DÍA 2

Ciberseguridad y Ciberdelincuencia

Ponencia por Elvira Tejada, en donde se expone la regulación de la actividad en el ciberespacio en España en donde en el año 2013 se crea un centro para tratar temas de cibercrimen.

Las iniciativas que se han tomado a nivel de País involucran al sector público y privado. Entre las estratefias de ciberseguridad nacional se han implementado las siguientes:

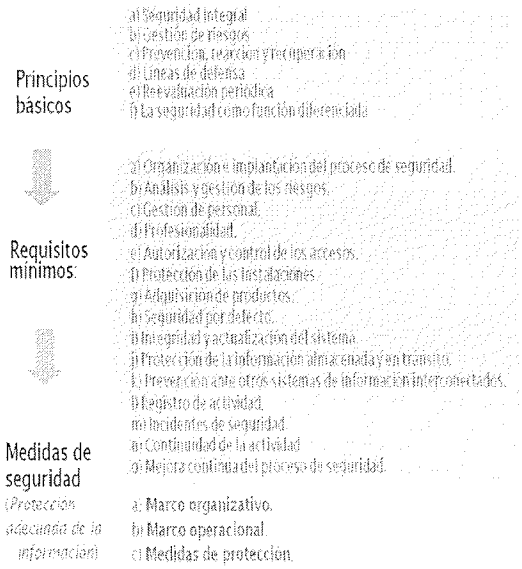
Directrices para uso seguro del ciberespacio-Coordinación de

1. Administraciones Públicas, sector privado y ciudadanos.
2. Reforzar seguridad en Administraciones Públicas.
3. Reforzar seguridad en empresas e infraestructuras críticas.
4. Actuación en ámbito judicial y policial (contra cibercrimen).
5. Sensibilización de todos los ciudadanos.
6. Capacitación tecnológica en todos los sectores.
7. Reforzar cooperación internacional.

Ciberseguridad Aproximación Española

Exposición por José Pablo López en donde se comenta sobre los sistemas de las tecnologías de información y comunicación (TIC) las cuales tienen como esencia que se puedan custodiar correctamente los datos que deben ser utilizados por quien pueda cuando lo requiera.

Entre los temas desarrollados se indica que las redes sociales son una puerta de entrada para realizar ciberataques ya que aprovechan sus vulnerabilidades: sobreexposición de información personal y son autopistas de información, es decir extienden su infección a la mayor cantidad de usuarios posibles.



El centro criptológico nacional de España utiliza formación a distancia, es decir mediante su plataforma virtual para capacitación.

Esquema Nacional de Seguridad (ENS)

José Ramón Zuazua expone sobre la administración electrónica la cual brinda a los ciudadanos de España a tener disponibilidad 24X7, facilidad en el acceso y ahorro de tiempo ya que esta plataforma funciona con una interoperabilidad que evita colas y desplazamientos.

Entre los factores de éxito para la administración electrónica está el implso de la administración mediante la legislación, confianza y seguridad de los ciudadanos y la cantidad y calidad en los servicios ofrecidos.

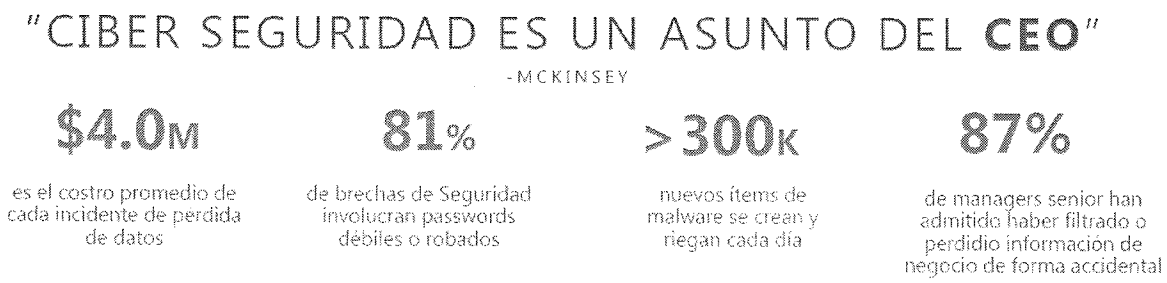
El ENS tiene como objetivo establecer una política de seguridad en la utilización de medios electrónicos a manera de proteger la información y se aplica a:

- Sedes electrónicas.
- Registros electrónicos.
- Sistemas de información accesibles electrónicamente por los ciudadanos.
- Sistemas de información para el ejercicio de los derechos.
- Sistemas de información para el cumplimiento de deberes.
- Sistemas de información para recabar información y estado del procedimiento administrativo.

Elementos Críticos Seguridad en Internet

Erick Sosa de parte de Microsoft en donde expone la situación actual en ciber ataques a las organizaciones los cuales en promedio son 106 al año.

Entre los nuevos puntos ciegos para IT se tienen los cibercrímenes, fuga de data y shadow IT (dispositivos, software y servicios fuera de la jurisdicción de IT).



Ciber Seguridad en el Ecosistema del Mercado de Capitales

Ponencia por Marcelo Gaggino en donde se expone su experiencia en la adopción de ISO 27000, se adopta a nivel de institución como un objetivo estratégico a cumplir a enero de 2018.

Argentina adicional al proyecto de ISO 27001, crearon su Data Center y realizaron un upgrade tecnológico y funcional a los sistemas core de la comisión nacional de valores.

Proyectos de Regulación y continuidad operativa del negocio en México

Arturo Murillo expone los casos en México a nivel de ciber ataques en donde se indica que desde el 2016 a lo que va del 2017 han reportado 16 eventos de intrusiones las cuales han tenido una afectación monetaria de aproximadamente 124.6 millones de pesos.

Controles mandatorios en la regulación vigente en México:

- Pruebas de penetración y detección de vulnerabilidades.
- Funciones específicas de Oficial de Seguridad de la Información.
- Arquitectura de seguridad en servicios electrónicos.
- Sistemas de detección y prevención de fraudes.
- Reportes de eventos de pérdida de información o intrusión.
- Identificación de causas raíz en eventos de riesgo operacional.
- Uso de equipos (hardware) de detección de intrusiones (IDS) y de prevención (IPS).
- Esquemas de continuidad del negocio que prevean escenarios de actuación ante ciberataques.

Día 3

Ciberseguridad en la Supervisión

Francisco Del Olmo de España expone los ámbitos en la supervisión y herramientas que utilizan en la misma como por ejemplo los ciber cuestionarios los cuales tienen como propósito conocer si las entidades están preparadas para repeler o responder un ciberataque.

IOSCO ⇒

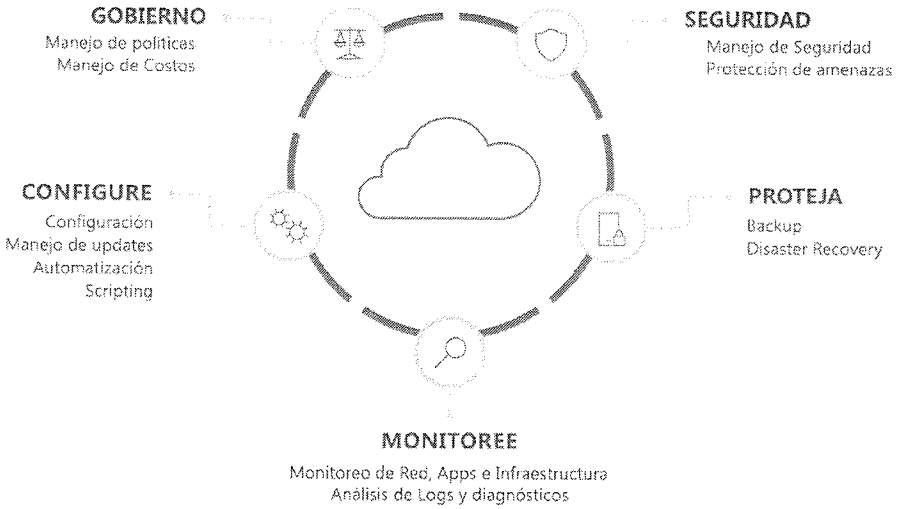
- Razones del ciberataque.
- Origen y naturaleza del ciberataque.
- Consecuencias:
- Reputación.
- Efectos a terceros (accionistas, clientes,..).
- Coste financiero.
- Litigios.
- Adecuadas medidas preventivas.
- Experiencia en anteriores situaciones.

La Seguridad en la nube

Erick Sosa comparte los nuevos retos que traen consigo la expansión a la nube como por ejemplo la administración de las SaaS, seguridad, monitoreo de amenazas, backup entre otros.

Uno de los retos mencionadas es la complejidad con la caída de los servicios y que es importante que el regulador trate de entender en qué tipo de nube se encuentran sus regulados.

Qué debiera buscar a nivel de administración?



Análisis Penales en derecho Penal español Ataques y Fraude

Elvira Tejada expone sobre la respuesta del estado de España sobre las soluciones legales las cuales se basan en tres parámetros:

- Necesaria evolución legislativa para ofrecer respuestas a las nuevas situaciones vinculadas al uso del ciber espacio.
- Evolución armonizada con la de otros Estados y/o de acuerdo con los criterios establecidos por organismos internacionales.
- Respeto pleno a los derechos y libertades de los ciudadanos y a los principios informadores del Estado de Derecho.