CLAIN 2018
XXII Congreso Latinoamericano
de Auditoría Interna y Evaluación
de Riesgos PANAMA, 17-18 de Mayo 2018

ASOCIACION BANCARIA DE PANAMA
ABP

FELABAN
FEDERACION LATINOAMERICANA DE BANCOS

Panel: El Rol del Auditor en un Mundo Móvil:

Plataformas Móviles, Nube, BYOD, Redes Sociales, etc

José Marangunich - Perú

Gerente del Área de Seguridad Integral para los Negocios del Banco de Crédito del Perú – CREDICORP, es Abogado por la Universidad de San Marcos con especialización en riesgos financieros y Compliance, Master of Business Administration de la Ecole Sup de Co Montepellier (Francia), Maestría en Administración de Negocios de la Universidad San Ignacio de Loyola y estudios de Planeamiento Estratégico en Lehigh University Pensilvania EEUU. Doctor en Desarrollo y Seguridad Estratégica del Centro de Altos Estudios Nacionales – CAEN Participó en programas de capacitación en Banca, riesgos operativos, Cumplimiento, Seguridad integral, Auditoría, Ciberseguridad, Control Interno y Prevención integral en los EE.UU., Francia, México, España, Panamá, Colombia, Chile, Argentina, Perú, Corea del Sur, Taiwan, entre otros países. He liderado proyectos diversos a nivel local y regional sobre riesgos de seguridad integral y Compliance para la industria bancaria y riesgos informáticos.

El Rol del Auditor en un Mundo Móvil

Beneficios de la Tecnología Móvil

EFICIENCIA

Muchos procesos internos pueden ser optimizados gracias al uso del móvil. Acceso a información y transacciones desde cualquier lugar en cualquier momento: logística, ventas, control de gestión, etc.

VISIBILIDAD Y MARCA

El uso del móvil es diario, si alguien tiene una App de la empresa la estará viendo continuamente. Las Apps transmiten la imagen de tu empresa en su diseño y a mayor interacción con ella más inclinación del usuario a comprar tu producto/servicio.

CANAL DE MARKETING

Una App puede tener muchas funcionalidades (información general, precios, pedidos, búsquedas, notificaciones, noticias, etc.) creando un canal directo donde interactuar y ofrecer toda aquella información y servicios que tus clientes demanden.

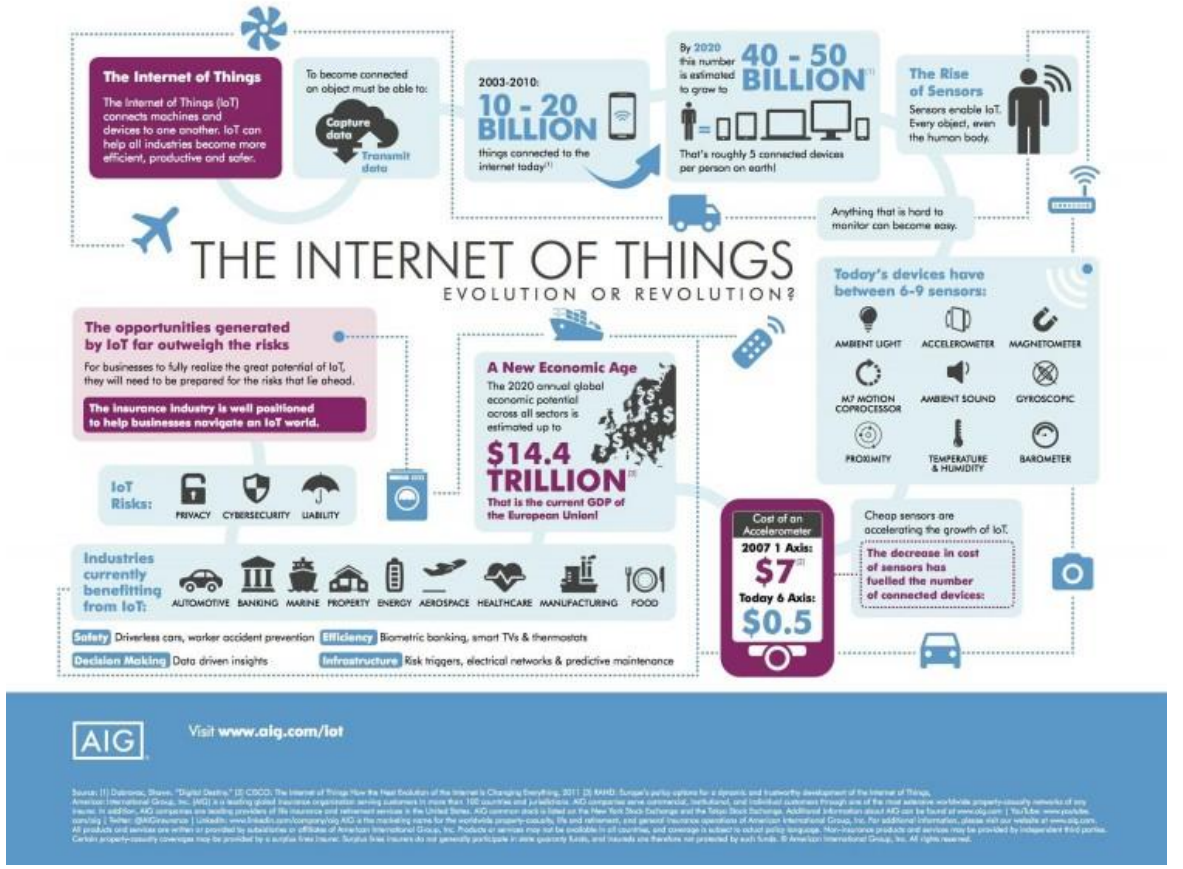
VENTAS

Con disponibilidad 24/7, desde una App el cliente puede realizar compras directamente, pudiendo mantenerse también al tanto de ofertas y novedades.

FIDELIZACIÓN

A un 'clic de todo' estamos más cerca de nuestros clientes para escucharles. Canal de comunicación bidireccional. Programas de fidelización apoyados en Apps.

Fuente: Itop Solutions, Mobile and IoT, 2015



El Rol del Auditor en un Mundo Móvil

Escenarios de riesgos cibernéticos asociados a la tecnología móvil

Principales formas explotadas por los defraudadores en los dispositivos móviles

Fuente: Pew Research Center, Forbes, Cisco Mobile Data Traffic, Baymand Statistica, FTC, Idology Fraud Report - 2017

Mantener los dispositivos actualizados

77,3% de los dispositivos iOS tenían instalada la versión principal más reciente en 2017, una disminución de 2,1%. Con Android, apenas 20% de los dispositivos ejecutaban la versión principal más reciente, un aumento en este número de 5% en relación a 2016.

Año	Dispositivos iOS en la versión principal más reciente (Porcentaje)	Dispositivos Android en la versión principal más reciente (Porcentaje)
2016	79,4	15,0
2017	77,3	20,0

Nuevas variantes de malware para dispositivos móviles

Nuevas variantes de malware para dispositivos móviles

En 2017, el número de nuevas variantes de malware para dispositivos móviles aumentó 54%.

Año	Nuevas Variantes
2016	17.214
2017	26.579

Fuente: Symantec, Informe sobre las amenazas para la seguridad de Internet, 2018

El Rol del Auditor en un Mundo Móvil

Escenarios de riesgos cibernéticos asociados a la tecnología móvil

Amenazas contra dispositivos móviles

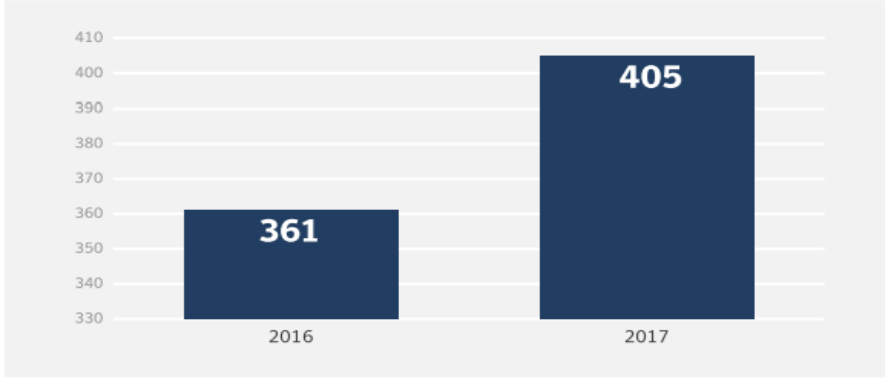
Principales Hallazgos

- La cantidad de nuevas variantes de malware para dispositivos móviles creció 54% en 2017, en comparación con 2016.
- En 2017, fue bloqueado un promedio de 24.000 aplicaciones malintencionadas para dispositivos móviles por día
- 27% de las aplicaciones malintencionadas fueron encontradas en la categoría Estilo de Vida, seguidas por Música y Audio, con 20%.
- 63% de las aplicaciones grayware en 2017 filtraron el número de teléfono y 37% revelaron la ubicación física del teléfono.
- 77,3% de los dispositivos iOS tenían instalada la versión principal más reciente en 2017, una disminución de 2,1% en relación a 2016. Con Android, apenas 20% de los dispositivos ejecutaban la versión principal más reciente, pero hubo un aumento en este número de 5% en relación a 2016.

Fuente: Fuente: Symantec, Informe sobre las amenazas para la seguridad de Internet, 2018

Nuevas familias de malware para dispositivos móviles

El número de nuevas familias de malware para dispositivos móviles aumentó 12,2% entre 2016 y 201.



Información confidencial filtrada por aplicaciones

63% de las aplicaciones móviles filtraron números de teléfono de los usuarios y 37% revelaron la ubicación física de los dispositivos.

Clase de información filtrada	Porcentaje
Número de Teléfono	63,0
Información de ubicación	37,0
Información de aplicaciones instaladas	35,0

Fuente: Symantec, Informe sobre las amenazas para la seguridad de Internet, 2018

El Rol del Auditor en un Mundo Móvil

BYOD: Principales problemas de seguridad y controles

Fuente: Trend Micro "The Case for Making BYOD Safe", 2015

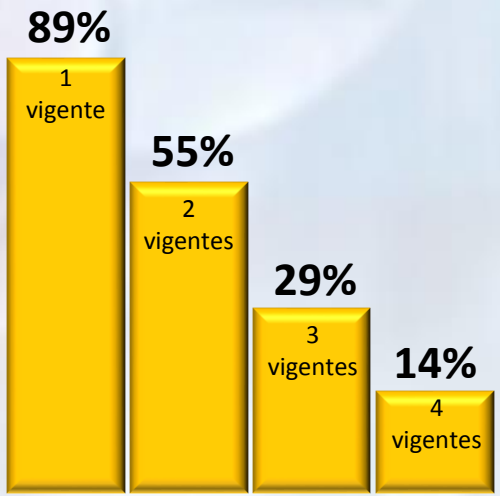
Fuente: csoonline.com, Arcadia 2017

32% de las empresas sacrificaron la seguridad por la conveniencia

45% de ellas sufrió pérdida de datos o tiempo fuera de servicio

4 medidas básicas de seguridad móvil:

- Cambiar todas las contraseñas por defecto.
- Encriptar la data enviada a través de redes públicas.
- Restringir el acceso sobre la base de la "necesidad de saber".
- Probar los sistemas de seguridad de forma periódica.



Solo el 14% de las empresas tenían implementadas las cuatro medidas básicas de seguridad móvil

Solo el **49%** de las empresas tiene una política con respecto al uso de Wi-Fi públicas, e incluso el **47%** cifra la transmisión de datos confidenciales en redes abiertas y públicas.

ISACA® *Trust in, and value from, information systems*

- Protección de datos sensibles y propiedad intelectual
- Protección de redes a las que se conectan los dispositivos BYOD
- Responsabilidad y Rendición de cuentas por los dispositivos y la información contenida en ellos
- Eliminación de la data de la organización de los dispositivos de los empleados en caso de cese o pérdida del dispositivo
- Protección contra el malware

Fuente: ISACA, BYOD Audit/Assurance Program, ISACA, 2012

Héctor Estrada Rivera - México

Director Ejecutivo, Auditoría de TI y Transformación del Negocio de Scotiabank México Director de Auditoría de Tecnologías de Información, con 20 años de experiencia en auditoría de TIs y 28 años de experiencia acumulada en actividades relacionadas con las tecnologías de información. Maestro en Dirección de Tecnologías de Información, Ingeniero en Sistemas Computacionales. Auditor Certificado en Sistemas de Información, Certificado en Riesgos y Control de Sistemas de Información y miembro del capítulo Toronto de ISACA. Calificación más alta en Latinoamérica en el examen de certificación CISA en 2005. Ha sido orador en temas relativos a Control y Sistemas de Información en México y Costa Rica.

¿Y cómo auditar en un mundo móvil?

Algunos datos “duros”

Para finales de 2017:

- **8,400 millones de dispositivos conectados a Internet**
- **5,000 millones de teléfonos inteligentes en el mundo**
- **99.6% de los teléfonos inteligentes están basados en Android (80.7%) y iOS (18.9%)**

Fuente: Gartner

Y viendo al futuro…..

- Para el 2019:
  - ✓ **el 20% de las marcas habrán abandonado su app**
  - ✓ **por cada dólar gastado en innovación, se requerirán siete dólares en los sistemas legados (legacy systems) o sistemas core**
- Para el 2020:
  - ✓ **20,400 millones de dispositivos conectados a Internet**
  - ✓ **100 millones de consumidores comprarán a través de realidad aumentada**
  - ✓ **las personas tendrán más conversaciones con Bots que con sus parejas**
  - ✓ **el 30% de la navegación en internet será sin una pantalla de por medio**
  - ✓ **un negocio basado en Blockchain se valuará en 10 billones de dólares**
- Para el 2021:
  - ✓ **el 20% de las actividades digitales en el mundo involucrarán a uno de los 7 "gigantes" digitales (Amazon, Apple, Google, Facebook, Alibaba, Baidu y Tencent)**

Fuente: Gartner

Top 10 consideraciones de auditoría

1. Asegurar que las **apps, servicios en la nube, accesos remotos, smartphones y dispositivos conectados a internet** están completamente identificados en el universo de auditoría y se ha definido un ciclo auditable para cada plataforma en base a una evaluación de riesgos.

2. Asegurar que los terceros son considerados en la evaluación de riesgos y forman parte del universo auditable.

3. Indispensable considerar el riesgo de fraude durante la evaluación de riesgo de cada plataforma tecnológica.

4. Asegurar que se cuentan con políticas, procedimientos y estándares de seguridad actualizados y basados en las mejores prácticas de la industria. Evaluar las plataformas tecnológicas contra dichos estándares.

5. Considerar el proceso E2E. Las **plataformas móviles** son la puerta de entrada a otros servicios y plataformas "dentro" de la organización. La arquitectura que asegure de forma razonable la confidencialidad, disponibilidad e integridad es fundamental.

6. Asegurar que el proceso de control de cambios se aplica de forma homogénea a las plataformas móviles.

7. Considerar todas las **plataformas móviles** compatibles aplicables (iOS, Android, Windows, etc.) en los planes de auditoría.

8. En desarrollos ágiles, tener en cuenta los controles necesarios que deben estar presentes en este modelo de entrega.

9. En modelos de servicio multiplataforma, asegurar que se incluyen todos los componentes de otros fabricantes.

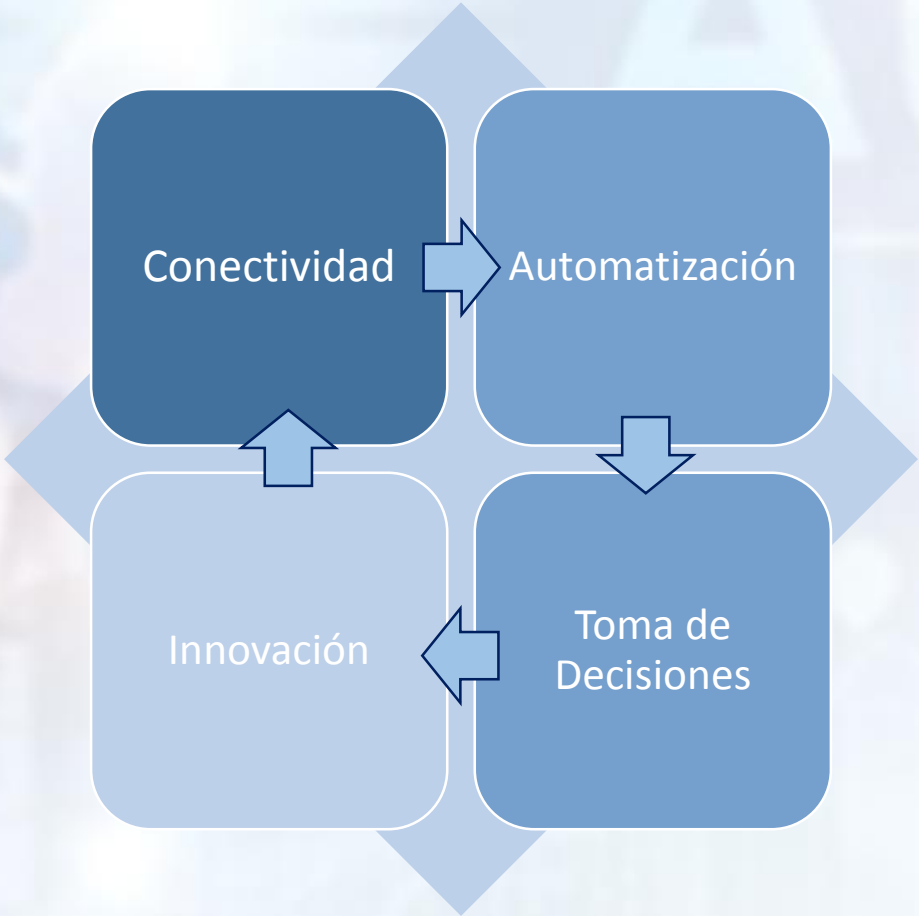
10. Asegurar que existe un proceso satisfactorio de Altas, Bajas y Cambios de cuentas privilegiadas y cuentas de usuario en plataformas móviles.

José Esposito Li Carrillo- Perú

Gerente de División Auditoría del Banco de Crédito del Perú y Auditor Corporativo de Credicorp. Es Licenciado en Economía de la Universidad del Pacífico, Lima; Master en Economía con especialización en Econometría de la Universidad de Wisconsin- EE.UU.; Certified Internal Auditor (CIA) y Certified in Risk and Management Assurance (CRMA) por el Institute of Internal Auditors Global (IIA), EE.UU.; Certified in Risk and Information Systems Control (CRISC) por ISACA, EE.UU.; Anti Money Laundering Certified Associate (AML/CA) por Florida International Bankers Association y la Florida International University, EE.UU. Miembro del Financial Services Guidance Committee Board del Instituto de Auditores Internos Global (IIA). Ha sido Presidente del Comité de Auditoría Interna y Evaluación de Riesgo de la Federación Latinoamericana de Bancos (FELABAN) y Presidente del Comité de Auditores Internos de la Asociación de Bancos .

¿Estamos preparados para el mundo digital?

Contacto con clientes
Comunicación interna
- Móviles
- Redes sociales
- Colaboración



Cambio en procesos
Ahorro en costos y tiempos
- Apps
- Re-diseño
- 100% imágenes

Más, mejor y más rápido
- Digitalización
- Talento y cultura

Cambio en la toma de decisiones hacia el cliente
- Bid data
- Machine learning
- IA

Fuente: Mc Kinsey&Company, What “digiltal really means”, Digital Academy

Qué puede hacer el Directorio para supervisar la "resiliencia digital"?

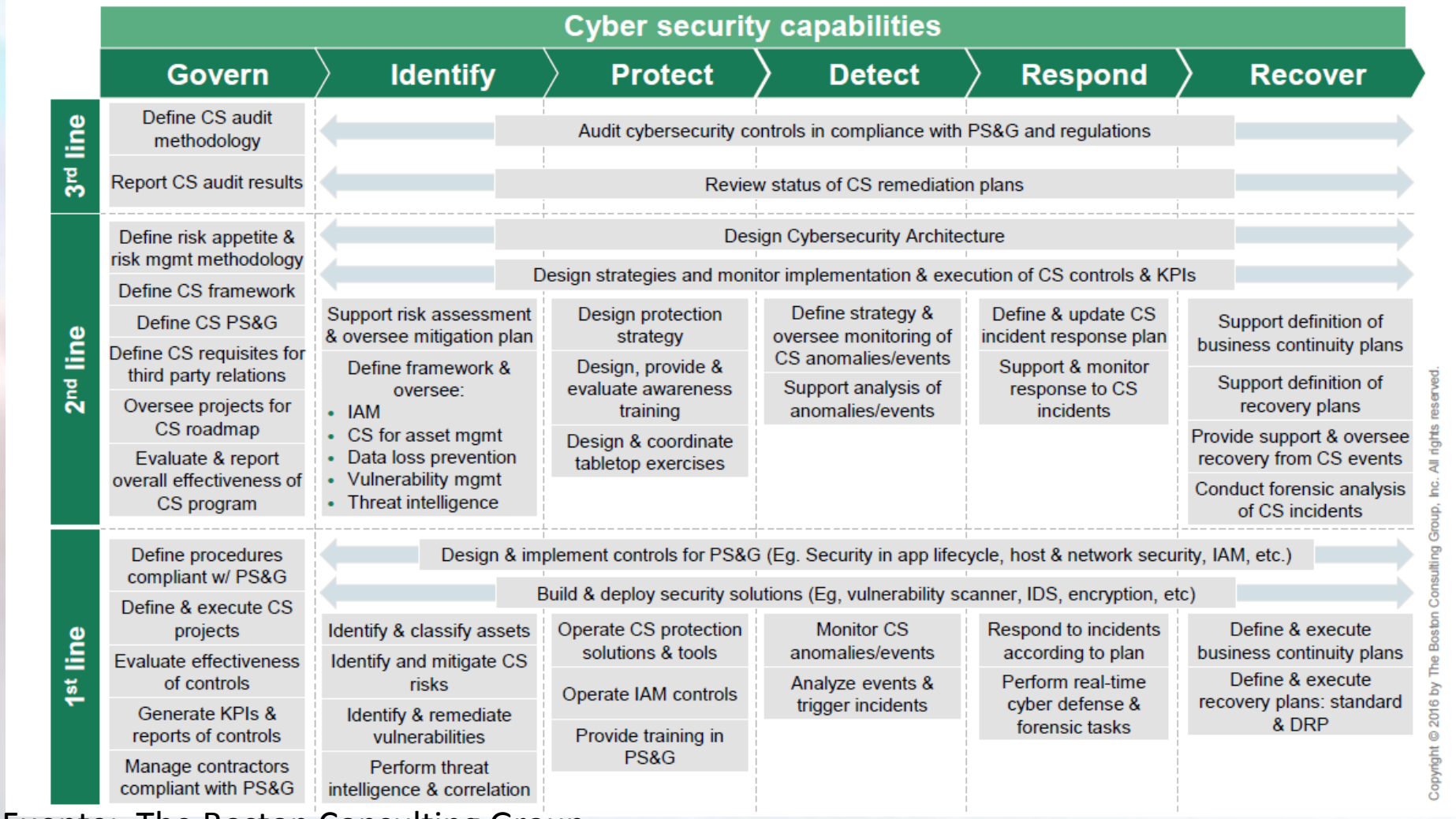
1. **Entender dónde estamos**: se espera que la ciberseguridad sea gestionada y reportada de acuerdo a un marco conceptual
2. **Determinar qué tenemos**: llevar la conversación desde "ciber" hacia riesgos de información
3. Requerir y participar en "escenarios de juegos de guerra" para **Probar qué tanto estamos preparados para responder**
4. Empujar a los líderes para determinar aspiraciones sobre ciberseguridad como primer paso para elaborar una **estrategia integral de ciberseguridad**
5. Implementar un sólido **programa de gestión del rendimiento cibernético**

Palancas críticas para la Resiliencia Digital

1. Priorizar los activos de información y los riesgos del negocio asociados
2. Conseguir que el personal de 1ra Línea entienda el valor de los activos de información
3. Integrar la resiliencia cibernética en los procesos integrales de gobierno
4. Integrar las respuestas a incidentes entre las funciones de negocio, con test realistas
5. Integración profunda de la seguridad en el ambiente de tecnología, impulsando escalabilidad
6. Proveer protección diferenciada para los activos más importantes
7. Desplegar defensas activas para responder a ataques emergentes en tiempo real

Fuente: McKinsey & Company; Presentación CLAIN 2017, otros

Roles de las 3 líneas de defensa



Fuente: The Boston Consulting Group

IIA: GTAG Evaluando el Riesgo de Ciberseguridad

1. ¿La gerencia y directorio conocen los riesgos clave relacionados con la ciberseguridad?
2. ¿Ha realizado la administración una evaluación de riesgos para identificar activos susceptibles a amenazas cibernéticas o infracciones de seguridad, y ha evaluado el impacto potencial (financiero y no financiero)?
3. ¿Están la primera y la segunda líneas de defensa colaborando con sus pares en la industria para estar al día con los riesgos emergentes, las debilidades comunes y las violaciones de ciberseguridad?
4. ¿Están implementadas las políticas y procedimientos de seguridad cibernética, y los empleados y proveedores reciben capacitación y concientización?
5. ¿Los procesos de TI están diseñados y operando para detectar amenazas cibernéticas? 6. ¿Están funcionando los mecanismos de retroalimentación para dar a la alta gerencia y al directorio información sobre los programas de ciberseguridad?
7. ¿La administración cuenta con una línea directa efectiva o un procedimiento de emergencia en caso de un "ciber ataque "o amenaza?
8. ¿La actividad de auditoría interna es capaz de evaluar los procesos y controles para mitigar las "ciber amenazas"?
9. ¿Mantiene la organización una lista de proveedores de servicios tercerizados que tienen acceso al sistema? ¿Se ha llevado a cabo un examen independiente de ciberseguridad?
10. Auditoría ha identificado las amenazas cibernéticas y las ha incorporado en sus procesos de evaluación de riesgos y planeamiento?

Actividades comunes de la 3ra Línea de Defensa

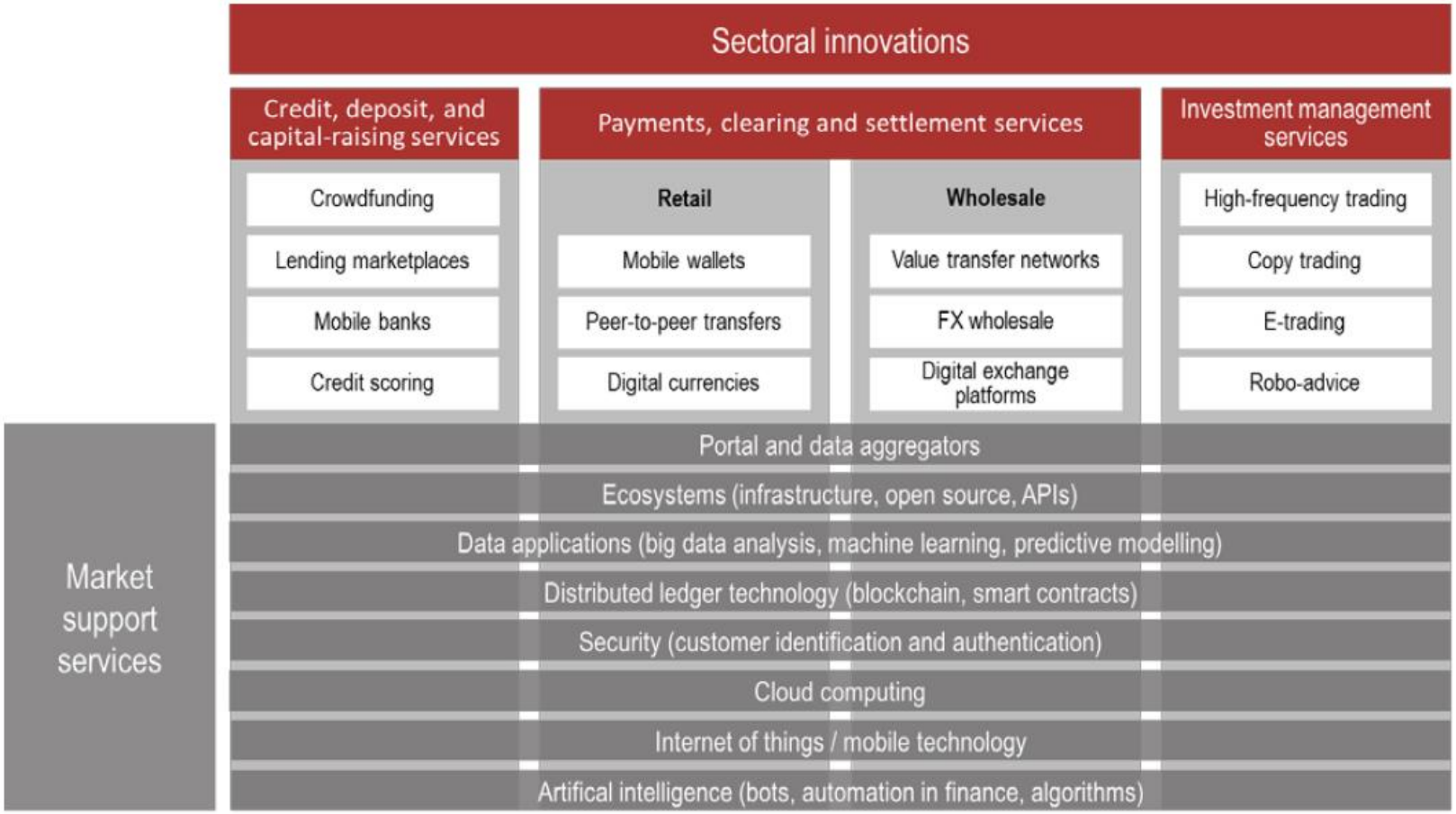
- Proporcionar evaluaciones continuas e independientes de las medidas preventivas y de detección relacionadas con la ciberseguridad.
- Evaluar los activos de TI de los usuarios con acceso privilegiado para configuraciones de seguridad estándar, sitios web problemáticos, software malicioso y extracción de datos
- Seguimiento de la diligencia de remediación
- Realizar evaluaciones de riesgos cibernéticos de organizaciones de servicios y proveedores (nota: las líneas de defensa primera y segunda comparten esta responsabilidad continua)

Ethical Hacker

Fuente: IIA GTAG Assesing Cibersecurity Risk, setiembre 2016

Innovación vs Disrupción

Graph 1: Sectors of innovative services



Fuente: BCBS, Implications of fintech developments for banks and bank supervisors, febrero 2018

¿Tenemos el capital humano necesario?

3 áreas de desarrollo:

- Administración de sistemas
- Diseño y configuración de redes
- Desarrollo de software

Exhibit 5: Skill Level of Internal Audit Teams

Skills	Novice	Intermediate	Advanced
Microsoft Windows and Active Directory Software	30%	52%	17%
UNIX and Linux	74%	22%	4%
Network Design and Implementation	74%	22%	4%
Database Administration	48%	43%	9%
SIEM	30%	57%	13%
Telephony/VoIP	65%	30%	4%
Software Development	48%	43%	9%
IT Governance and Risk	13%	61%	26%
Penetration Testing	57%	35%	9%

Source: Crowe analysis

High Skill Low Skill

Fuente: Crowe Horwath- IA Foundation, The Future of Cybersecurity in Internal Audit, marzo 2018