Gestión del Riesgo de Cibernético y el Rol de Auditoría

...

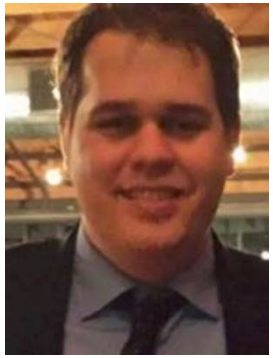
Mayo de 2017

Organizan

FELABAN
FEDERACION LATINOAMERICANA DE BANCOS

Asociación Bancaria Costarricense

Introducción



David Ware

- Socio Asociado de la Oficina de Atlanta
- Parte de Digital McKinsey y la Práctica Ciberseguridad
- 5 años en McKinsey
- Enfocado en temas de Transformaciones en Proveedores de Servicios de Tecnología y en el Sector Público

Los bancos están enfrentando amenazas crecientes de riesgo cibernético – los ataques son cada vez más frecuentes y sofisticados

Los ataques se están volviendo cada vez más frecuentes y severos

- En el 2016…
  - El **número de ataques** confirmados **creció en 30%**
  - Los **sistemas de detección del fraude** están quedando **rezagados** – en el 2015, **se detectaron menos del 20% de los ataques** (vs. 75% en el 2005)
  - El **costo promedio por ataque** a datos fue de **$4Mn USD** – aumento del 6% respecto al año anterior

Los "puntos de ingreso" a ser atacados se han incrementado

- Los **dispositivos personales** (p.ej., teléfonos celulares) representan aproximadamente la **misma proporción de ataques que los servidores** (~35%)
- Más del **75% de los sitios web poseen vulnerabilidades** que pueden ser infectadas
- Aproximadamente el **15% de la gente testeada hará clics en links dentro de un email extraño**

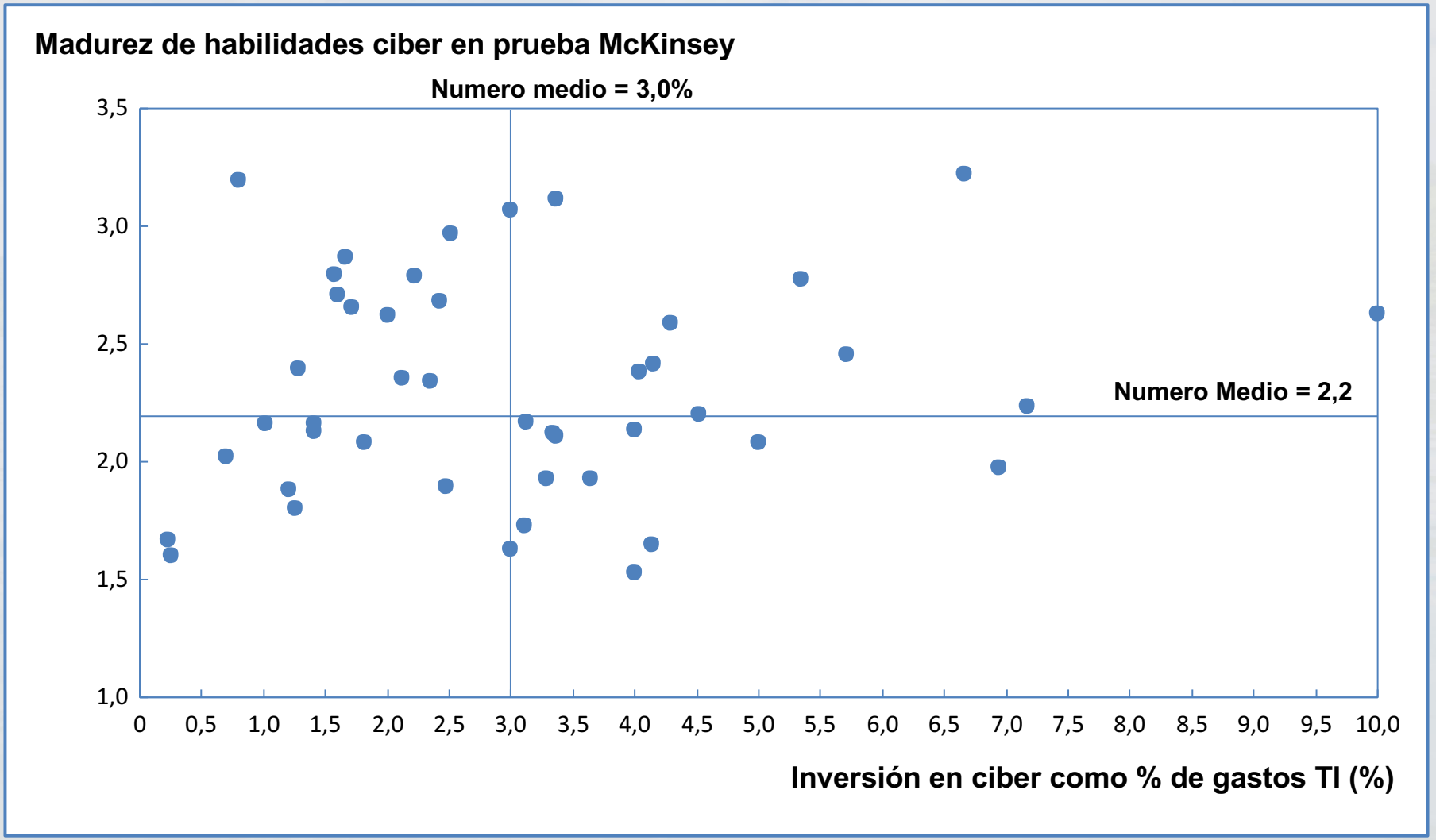
FUENTE: Reporte de Ataques de Datos de Verizon del 2016; Informe de Investigación del Ponemon Institute del 2016; Momentum Partners, Reporte de Amenazas a la Seguridad de Internet de Symantech

Incluso las organizaciones más sofisticadas han sido objeto de ataques cibernéticos en los últimos años

Caso real de un banco en EEUU

- Un criminal cibernético vigiló a un administrador de sistemas senior de un banco en redes sociales y supo que participaría en una reunión con sus compañeros universitarios
- La semana posterior a la reunión le envió un *email* prometiendo mandarle fotos del evento – el *email* incluyó un link a un sitio *web* (con fotos reales) – a través de este sitio instalaron un programa de registro de pulsaciones en su computadora
- El banco poseía capacidades de gestión de acceso privilegiado, pero éstas no habían sido implementadas completamente debido a preocupaciones sobre las capacidades de TI
- El sistema de registro de pulsaciones recogió credenciales de *log-in* para ingresar a 20-30 bases de datos con información sensible de clientes – el banco debió pagar decenas de millones de dólares para evitar que esta información fuera publicada

No hay correlación entre la inversión en ciber y la madurez



FUENTE: McKinsey Digital Resiliency Assessment

Temas para la discusión de hoy:
Cuatro elementos críticos para una gestión apropiada del riesgo cibernético

A Identificar activos, riesgos y controles	• Identificar los activos de información críticos "*business-back*" en lugar de "*TI forward*" • Comprender cómo los activos de información están diseminados a lo largo de los sistemas y qué tipos de controles existen
B Gestionar los riesgos de los proveedores	• Desarrollar habilidades requeridas para realizar "*trade-offs*" entre los requerimientos de seguridad y el apalancamiento de proveedores (p. ej., desarrollo de *RFPs*, generación de listas reducidas, negociaciones)
C Realizar escenarios de juegos de guerra para prepararse a una respuesta	• Incluir a ejecutivos de una amplia variedad de funciones del negocio, no sólo a gerentes de TI y Seguridad • Desarrollar escenarios realistas y personalizados con base en los activos de información más importantes y vulnerabilidades identificadas
D Desarrollar un Modelo de Gestión del Riesgo de TI integrado	• Crear un modelo de gobierno de riesgo consolidado que involucre a toda la organización • Establecer procesos de definición de políticas, monitoreo y evaluación • Implementar métricas y sistemas de reporte cohesivos

A Crear una taxonomía de activos…

1	Información de recursos corporativos	Instalaciones / bienes inmuebles	4	Información del cliente	Información básica
		Recursos humanos			Autenticación de clientes
2	TI y Operaciones	Información de aplicaciones			Información derivada
		Información de infraestructura			Información de portafolio y actividad
		Políticas de seguridad de TI	5	Información de producto y transacciones	Libros del banco
		Compras			Modelos de precios
		Operaciones de servicios			Catálogo de productos y servicios
		Información de proveedores			Información transaccional
3	Información de gestión	Cumplimiento y regulación			
		CRM y Marketing			
		Información de finanzas			
		Información legal			
		Información de riesgo			
		Infromación estratégica y del Directorio			

A …y de vulnerabilidades

A Uso de criterios jerarquizados para evaluar riesgos de activos de acuerdo a los tipos de impacto

EJEMPLO

	1	2	3	4
	Insignificante-Menor *Riesgo estable*	**Moderado** *Mayor riesgo*	**Importante** *Riesgo más alto*	**Severo** *Riesgo más alto*
Impacto sobre el cliente	• Menos del 1% de los clientes impactados	• Entre 1-5% de los clientes impactados • Demoras significativas en el servicio	• Entre 5-10% de los clientes impactados • Información privada para una cantidad menor de clientes hecha pública • Grandes demoras en el servicio	• Más del 10% de los clientes impactados • Información privada para una cantidad moderada de clientes hecha pública • Grandes demoras en el servicio impactando la calidad del servicio
Impacto financiero	• Menos de $10Mn o Menos de 5bps de rentabilidad	• $10Mn-100Mn o 5-10 bps de rentabilidad	• $100Mn-500Mn o 10-15 bps de rentabilidad	• >$500Mn de impacto o >15 bps de rentabilidad
Impacto reputacional / de mercado	• Limitado o ningún riesgo reputacional	• Impacto cuantificable en la percepción del cliente • Cierto riesgo de cobertura de medios locales	• Gran impacto en la percepción de marca del cliente • Cobertura de medios regionales generalizada o limitada cobertura de medios nacionales	• Daño de marca duradero y/o gran impacto directo en todo el sistema financiero • Cobertura prominente de parte de medios nacionales e internacionales
Impacto regulatorio	• Limitado riesgo de acción regulatoria	• Moderado riesgo de acción regulatoria localizada • Moderado error de reporte financiero	• Moderado riesgo de acción regulatoria global • Posible acción contra la alta gerencia • Error de reporte financiero material, una aclaración es requerida	• Alto riesgo de acción regulatoria global • Posibilidad de una acción significativa contra la alta gerencia, incluyendo prisión • Error de reporte financiero severo, una aclaración es requerida
Impacto en la productividad de los empleados	• Menos de 100 horas hombre de empleados experimentando una parada o un aumento en la carga de trabajo	• 100-1,000 horas hombre	• 1,000-100,000 horas hombre • Moral de los empleados afectada debido a la publicación de datos personales de empleados	• Más de 100,000 horas hombre • Violación significativa de la confidencialidad de datos personales de empleados

Es necesario contar con un *framework* de gestión de riesgo empresarial amplio

A Evaluación estructurada de los controles vinculados a cada riesgo

EJEMPLO

Framework de evaluación de controles para los principales tipos de riesgo

Identificación y gestión de accesos

1. Derechos de acceso
2. Autenticación

Seguridad de Datos

3. DLP y seguridad de la *web*
4. Encripción en movimiento y en descanso
5. Seguridad de documentos físicos
6. Resiliencia de datos

Seguridad de la red

7. Acceso remoto
8. Segmentación de la red

Otros

9. Uso de punto final
10. Dispositivos móviles y *BYOD*
11. Monitoreo y análisis de eventos
12. Arquitectura de aplicaciones
13. Seguridad en cloud (no incluye servicios de gestión)
14. Continuidad del Negocio y Recuperación del Dato
15. Gestión del cambio / patch
16. Gestión del riesgo de proveedores
17. Seguridad física

A El resultado ideal sería una visión altamente objetiva de los activos de mayor riesgo y de los sistemas asociados

Cadena de valor	Activos de información	Sistemas / aplicaciones
Desarrollo de producto	Encuestas de consumidores	
	Detalles de pre-lanzamiento de nuevos productos	
Marketing	Inteligencia de competidores en el mercado ⚠	
	Pruebas de campaña nacional y otros contenidos pre-lanzamiento	
Gestión de canales	Contratos de canal y *SLAs* ⚠	
Equipos de servicio al cliente	Información demográfica del cliente	
	Información de contacto del cliente	
Ventas	Estrategia de gestión de inversiones	
	Datos transaccionales del cliente ⚠	
Cumplimiento de préstamos / créditos	Información de pagos y facturación ⚠	
Funciones corporativas	Comunicaciones ejecutivas y del Directorio	
	Pre-lanzamiento de información financiera	
	Login de administración / palabras clave / códigos ⚠	
	Datos de empleados no estructurados	
	Claves criptográficas ⚠	

A Ejemplo de caso: identificación y priorización de riesgo en una institución financiera en América del Norte

Situación

- La Junta de Directores pidió una **forma de medir el riesgo de ciberseguridad** para la próxima reunión
- El recientemente establecido **equipo de "Riesgo Cibernético" necesitaba un proceso para determinar y abordar el riesgo**
- La **infraestructura de TI era compleja y la cultura organizacional diversa**

Abordaje

Se utilizó una metodología de "dónde estamos ahora" para determinar las necesidades inmediatas y las acciones correctivas necesarias

- Se estableció un enfoque basado en riesgos, apoyado por el negocio para poder identificar la situación actual
- Se ha desarrollado un exhaustivo análisis de costos y una desagregación de actividades para la mitigación de riesgos

Se buscó definir "dónde deseamos estar" para la implementación de una planificación estratégica y de una gestión continua del riesgo

- Se ha detallado el estado futuro deseado en comparación al *framework* de ciberseguridad
- Definición de un camino a futuro para la reducción del riesgo en forma detallada

Implementación de una metodología de "cómo medir el progreso" para una ejecución de riesgo a operaciones

- Desarrollo de hitos clave para cada riesgo, en términos de acciones a ser tomadas
- Desarrollo de una revisión de riesgo y proceso de excepciones
- Estructuración de una nueva organización de riesgo cibernético, incluyendo un modelo de gobierno para autorización inmediata

Resultados obtenidos

- **Plan de trabajo de 3 años para la transformación de $250Mn USD**
- Las iniciativas de remediación fueron priorizadas con base al "*risk buy down*" esperado relativo al costo
- Creación de un ***scorecard* a nivel empresa con métricas de entrega y desempeño clave para monitorear el avance**
- Claro **foco en proyectos con el mayor ROI, con una transparencia sin precedentes**
  - Creación de una **forma de abordar y responder a nuevos riesgos y ataques**, en lugar de solamente combatir incendios
  - Desarrollo de un **nuevo gobierno**
  - Establecimiento de **un monitoreo continuo y de métricas para la implementación del programa**

A Identificación de activos y riesgos: Rol de Auditoría

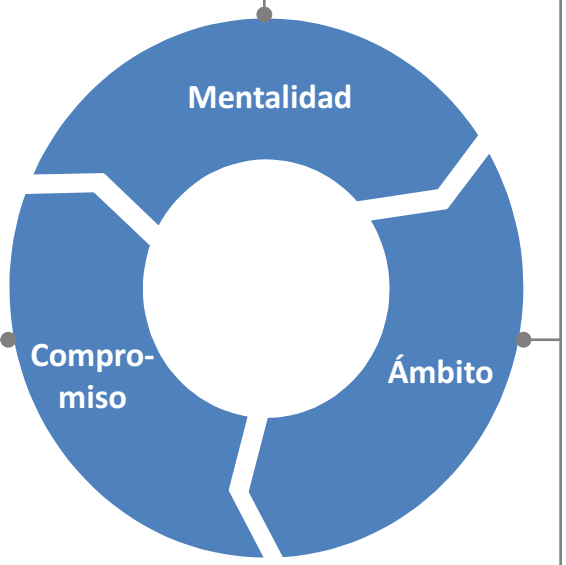
	Pruebas clave para realizar una auditoría
Identificación de activos	• ¿Es la lista de activos lo suficientemente exhaustiva (más allá de TI)? • ¿Han sido identificados activos con el nivel correcto de profundidad - lo suficiente para ser accionables, pero sin ser lo suficientemente profundos para hacerlos difíciles de gestionar? • ¿Se ha comprometido el resto del negocio en la identificación y priorización de activos críticos?
Identificación de riesgos	• ¿Es la lista de riesgos lo suficientemente exhaustiva (más allá de TI)? • ¿Es la lista de riesgos lo suficientemente específica para llevar a cabo decisiones de priorización y realizar *trade-offs*? • ¿Se ha comprometido el negocio en su nivel de apetito de riesgo?
Evaluación del sistema	• ¿Se puede determinar dónde se encuentra cada uno de los activos críticos dentro del sistema? • Si usted habla con usuarios de estos activos del negocio, ¿entienden dónde se encuentran los activos? • ¿Se sabe cuáles activos están contenidos o abordados por cada gran sistema? • ¿Son suficientes los controles? Se piensa en relación a cuánta gente posee acceso a ciertas porciones de datos críticos, ¿son demasiados? • ¿Puede la organización tecnológica ofrecer una prueba que los controles han sido testeados?

B Creencias clave en Riesgo de Terceros

"Usted puede tercerizar las operaciones, pero no puede tercerizar el riesgo"

- Considerar cuidadosamente el ***trade-off*** **entre compartir datos y protegerlos**
- **Las relaciones promueven el comportamiento, no sólo contactos** - una "alianza" es más significativa que "tener un proveedor"
- **Hacer una evaluación honesta de las fortalezas y debilidades** de la organización propia

- Mucho del riesgo es tomado antes de la decisión final de compra - las evaluaciones de seguridad deberían ser **realizadas de forma anticipada**
- **El equipo completo** (e.g., negocio, TI, riesgo, proveedores) **debería estar alineado en relación a los objetivos futuros**
- **El gobierno, reportes y procedimientos de escalamiento resultan esenciales** para asegurar que los problemas sean abordados por la gente correcta en el tiempo oportuno



- **Una supervisión genérica lleva a pobres resultados** - la supervisión y la recolección de datos deberían estar basados en riesgos específicos
- Los esfuerzos se deben **priorizar con base al tipo de relación** (e.g., tecnología, arbitraje laboral) **y el nivel de riesgo inherente de la tercera parte**
- **Pensar más allá de las alianzas inmediatas**
- El **contrato determina incentivos y penalidades significativas** por incumplimiento
- **Gestionar el riesgo más allá de la contratación** (e.g., reporte de transparencia continua)

B Mejores prácticas en la integración de la Evaluación de Terceros en el proceso de compras

***Setup* del programa**	• **Analizar los niveles de riesgo** de potenciales cargas de trabajo a ser mitigadas por anticipado • **Integrar el proceso de gestión del riesgo** en el proceso de evaluación
Selección de proveedores	• **Realizar una evaluación de alto nivel de los proveedores considerados**, a fin de identificar proveedores con alto riesgo de seguridad antes de que se inicie el proceso
Diligencia detallada y re-evaluación	• **Realizar evaluación detallada de los proveedores finales**, con foco en los principales riesgos • **Usar una combinación de datos objetivo, entrevistas y visitas** para evaluar a los proveedores • **Realizar un seguimiento de acciones correctivas** para su incorporación en el contrato
Negociacion y contratación	• Asegurarse que **acciones correctivas de gestión del riesgo estén incluidas** en el contrato • **Determinar e integrar incentivos / penalidades** apropiadas en el lenguaje del contrato • Asegurarse de que el contrato defina **claros procedimientos para la respuesta a incidentes**
Introducción	• **Dar seguimiento y asegurarse que las acciones correctivas hayan sido completadas** • **Realizar un control de antecedentes** a las personas que están desempeñando el trabajo de alto riesgo
Gestión continua	• **Monitorear / revisar las provisiones para la gestión del riesgo** y las acciones a ser tomadas durante la vida del contrato

B Ejemplo de carga de trabajo y *scoring* de datos en relación al modelo de riesgo

Bajo | Medio | Alto | Severo

Sección	Ejemplo de dato	Nivel de riesgo[1]
Directorio de empleados	Información de contratos de empleados (p. ej., nombre, rol, número telefónico)	
	Información personal (p. ej., esposa, dirección, contacto de emergencia)	
Información de RRHH del empleado	Archivos de RRHH (p. ej., verificación de antecedentes, contratos, cartas de oferta, información sobre ausencias por enfermedad / incapacidad)	
	Evaluación de desempeño del empleado (p. ej., registros de contratación, documentos de revisión, calificaciones, etc.)	
Gobierno / funciones internas	Reportes operacionales (p. ej., resultados de revisión interna, iniciativas de operaciones)	
	Reportes financieros (p. ej., resumen de desempeño financiero mensual)	
	Arquitectura de liderazgo (p. ej., estructura organizacional, líderes clave)	
Documentos internos	Comunicaciones internas (p. ej., *newsletter* interno)	
	Pipeline de oportunidad (p. ej., discusiones continuas con clientes, incluyendo temas de conversación)	
Información del cliente	Información de contacto del cliente (p. ej., nombre, título, email)	
	Información identificable personal del cliente (p. ej., número de identificación)	

1 El riesgo se asume a ser agregado (ej: todos los datos de un tipo específico es incumplido vs una única instancia)

B Ejemplo de caso: Programa de Gestión del Riesgo de Terceros para un banco global de EE.UU.

Situación

- El **banco confiaba en un gran número de proveedores para sus operaciones del día a día** – algunas de las relaciones se habían establecido hace muchos años
- El banco contaba con un **plazo muy corto para implementar mejoras en su proceso de gestión de proveedores**
- El banco **no poseía procesos de supervisión sistémicos para riesgos operacionales y de cumplimiento**
- La **supervisión de procesos estaba basada en el nivel de criticidad del proveedor para el banco** – los proveedores de pequeñas dimensiones que generaban la mayor exposición a riesgo operacional fueron descartados

Abordaje

1. Se estableció la **estructura general del programa**
2. **Se identificaron las categorías de terceros con base en el alcance del servicio** (p. ej., proveedores de datos, proveedores de TI, clasificación de cada categoría en base a la exposición y tamaño del riesgo)
3. Con base en la calificación de la categoría, **se identificaron ciertos grupos de *due-diligence* y *tests* de auditoría** de acuerdo a los requerimientos
4. En paralelo, **se mejoró la gestión de cuadros de mando específicos por proveedor**, con indicadores de cumplimiento y riesgo a fin de asegurar transparencia y visibilidad
5. **Se estableció una estructura de gobierno** independiente del negocio **para continuamente supervisar, ofrecer guía estratégica y actuar como un punto de escalamiento** para actividades de monitoreo de proveedores

Resultados obtenidos

- **Procesos robustos de gestión de terceros** que excedía los requerimientos regulatorios asegurando la transparencia y visibilidad de riesgos
- **Fuerte modelo de gobierno** que aseguraba la ejecución, responsabilidad y sustentabilidad del programa
- **Mejora del entendimiento del alcance y riesgo de relaciones** individuales con proveedores

FUENTE: Experiencia del cliente McKinsey

B Gestión del Riesgo de Terceros: Rol de Auditoría

	Pruebas clave para realizar una auditoría
***Setup* del programa**	• ¿La Gestión del Riesgo ha estado involucrada de forma lo suficientemente temprana en el proceso de compras para tener impacto? • ¿Hasta qué punto la Gestión del Riesgo y el negocio están comprometidos en un diálogo real en relación a riesgos en lugar de solamente gestionar un producto? • ¿Constituyen los riesgos de tercerización una porción de trabajo que está siendo evaluada por anticipado? ¿Existen distintos tipos de trabajos tratados en forma diferenciada?
Diligencia y re-evaluación detallada	• ¿Las evaluaciones de los proveedores equilibran apropiadamente profundidad y velocidad, abordando los riesgos más importantes, pero no retrasando el proceso de compras en forma innecesaria? • ¿Se ha previsto una prueba de cumplimiento cuando ésta ha sido requerida? • ¿Existe una lista de acciones de mejoras prescriptas como consecuencia de la evaluación? • ¿Cómo son discutidos los resultados de la evaluación con el negocio? ¿Poseen los resultados del negocio un impacto en las decisiones del negocio?
Negociación y contratación	• Para una muestra de contratos, ¿poseen los contratos el tipo correcto de provisiones para mejoras, incentivos / penalidades, y procedimientos en caso de un problema?
Gestión continua	• ¿Hasta qué punto son monitoreadas acciones de mejora continua a lo largo del tiempo? • ¿Con qué frecuencia es el riesgo revisado en forma holística para contratos importantes?

C La creación de escenarios de guerra es el mecanismo más efectivo para realizar asegurar que la capacidad de la institución de responder a una brecha en la seguridad es adecuada

La capacidad de responder a una brecha de la seguridad es tan importante como evitarlas en primer lugar

- Aún los ambientes tecnológicos más sofisticados (p. ej., RSA, US, DoD) han sido penetrados
- La mayor parte del valor destruido en un ataque cibernético es el resultado de una respuesta inadecuada en lugar del ataque en sí mismo
- Los planes de respuesta deben ser sometidos a "tests de presión" simulando la urgencia y ambigüedad de un ataque real
- En la mayoría de los casos, la respuesta de un negocio a una violación de seguridad (p. ej., en funciones legales, operacionales y de comunicación) es tan desafiante como la respuesta técnica

Creación de escenarios de guerra cibernéticos

- Simula un ataque cibernético del mundo real en relación a un escenario de negocios personalizado a las amenazas actuales de la organización
- Es multi-funcional, involucrando participantes que no sólo desempeñan un rol en la seguridad de la información, sino también en infraestructura de TI, servicio al cliente, operaciones, marketing, legales, y comunicaciones corporativas, asegurando claros derechos de decisión y responsabilidad a lo largo de cada uno de ellos
- Está estructurado para simular la experiencia de un ataque real: los participantes reciben información incompleta, y tienen que reaccionar a los eventos en tiempo real
- Va más allá de los enfoques de diagnóstico tradicional de ciberseguridad para testear las brechas en la capacidad de una organización de responder a un ataque
- Va más allá de los enfoques de diagnóstico tradicional de ciberseguridad para testear las brechas en la capacidad de una organización de responder a un ataque
- Un ambiente controlado provee aprendizajes incrementales y aprendizajes en comparación a una respuesta real
- Sin impacto sobre los ambientes de producción

La mayor parte de los bancos han identificado a los riesgos cibernéticos como un riesgo operacional top – los escenarios de juegos de guerra ofrecen una mayor capacidad de estimar potenciales pérdidas e identificar acciones de mitigación para un riesgo cibernético

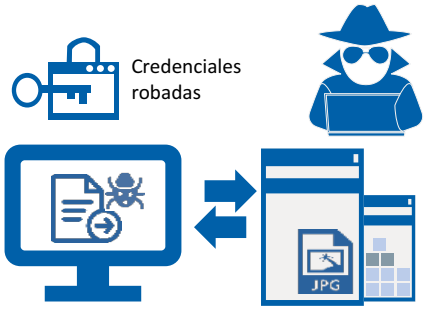
C Ejemplo de escenario de juegos de guerra

- **Perfil del agresor:** Grupo de delincuentes con buena financiación y organización y alcance internacional a través de una red compleja de alianzas, observaba el comportamiento durante meses antes de desarrollar y ejecutar un plan durante aproximadamente 2 años
- **Impacto:** Robo por más de $300Mn simultáneamente a lo largo de múltiples canales (p. ej., todas las 5 UNs de la firma de PE)

1 Ataque del tipo "spear phishing"

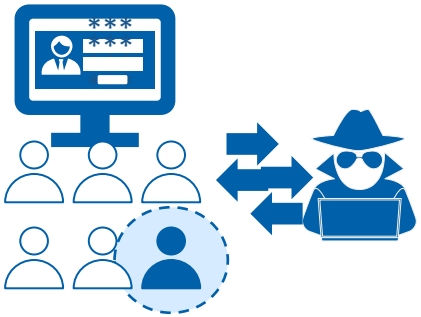
Hackers monitorean a los desarrolladores senior en el gerente de activos institucionales de una firma de PE y determina sus intereses para colocar una fracción definida de malware en un sitio de foro de desarrolladores externos en el cual estos participan

2 Puerta trasera ejecutada - credenciales robadas



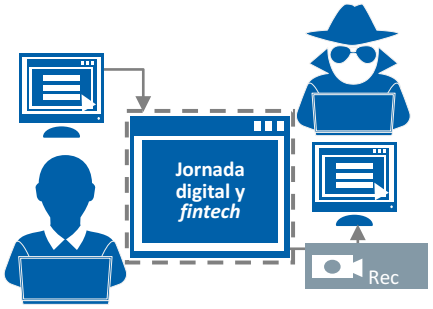
El desarrollador realiza una descarga del documento con malware, el cual se instala en la máquina sin ser detectado ya que el desarrollador ha desactivado Cylance, permitiendo el robo de las credenciales.

3 Máquinas infectadas en búsqueda de PC admin; contacto de helpdesk



El desarrollador llama al *helpdesk* para consultar sobre un actualización en su laptop, la cual funciona lentamente – la sesión de acceso remoto le permite al malware infectar la PC

4 Jefe de Servicios al cliente y comportamiento de relaciones con el clinete observados



El atacante observa la pantalla del administrador para familiarizarse y replicar el comportamiento del administrador para manejar los sistemas de transferencia de efectivo del gerente de activos

FUENTE: Kaspersky Labs, Análisis McKinsey

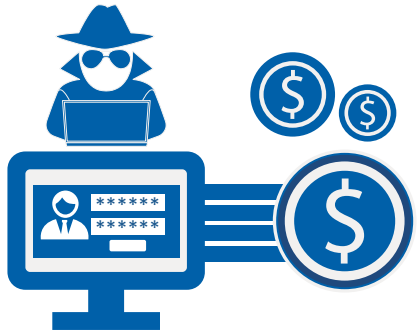
C Ejemplo de escenario de juegos de guerra

- **Perfil del agresor:** Grupo de delincuentes con buena financiación y organización y alcance internacional a través de una red compleja de alianzas, observaba el comportamiento durante meses antes de desarrollar y ejecutar un plan durante aproximadamente 2 años.
- **Impacto:** Robo por más de $300MM simultáneamente a lo largo de múltiples canales (ej.: todas las 5 UNs de la firma PE)

5 Ejecución del ataque inicial

Los atacantes entregan paquetes de datos adicionales, a través de transacciones fraudulentas (ej.: los atacantes cambian el valor de una cuenta de $100k por una de $1Mn, y luego se transfieren a sí mismos la diferencia de $900k)

6 Disrupción del programa colateral



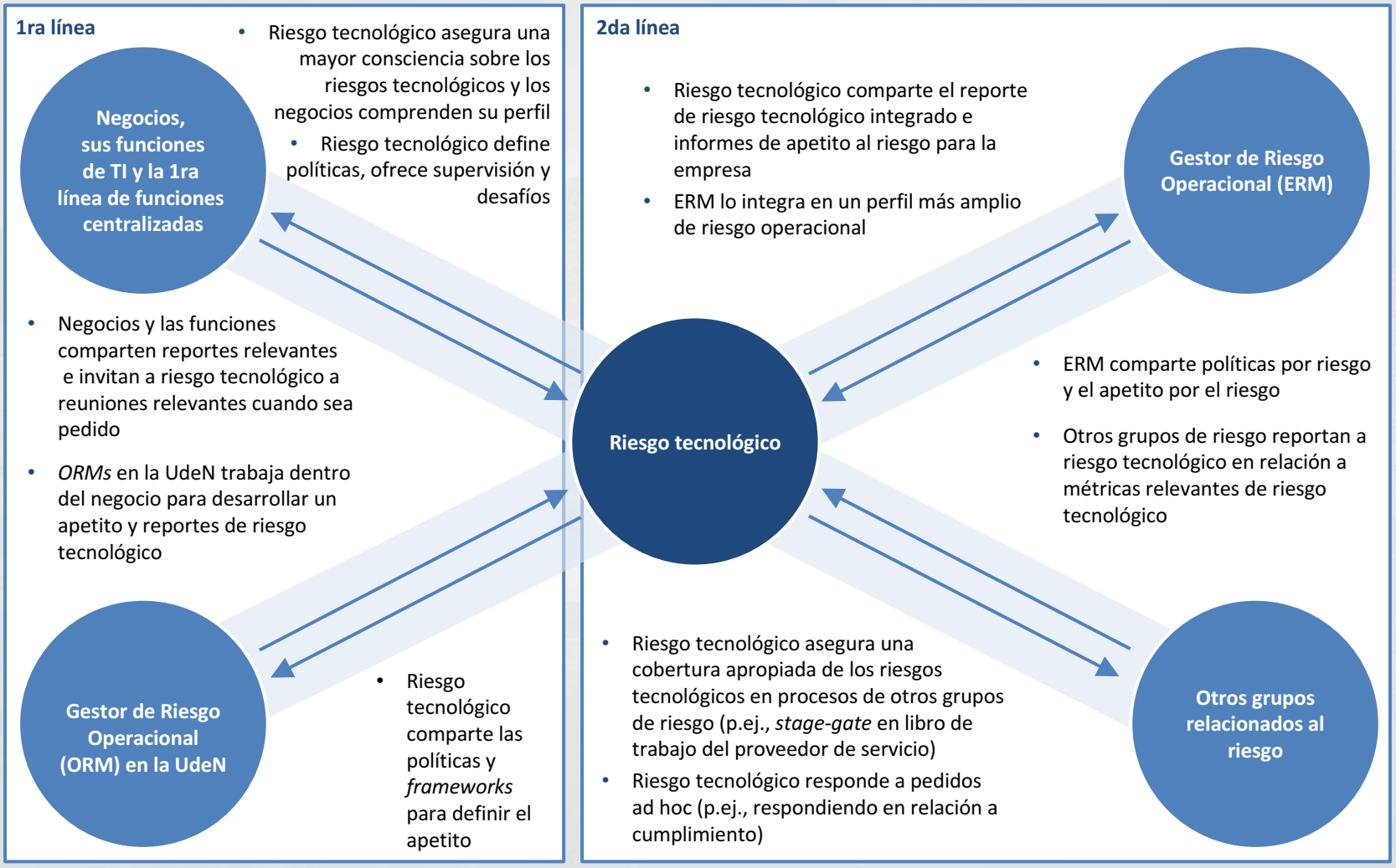
El administrador senior del sistema también llama al *helpdesk*, infectando su computadora Dado que la compañía aún no ha implementado un "*vaulting*" de contraseñas, esto permite un acceso persistente a varios sistemas operativos

7 Disrupción futura a través de captura de datos para acuerdos front-run

Mediante el uso de credenciales de *login*, los atacantes obtienen datos sensitivos a nivel comercial y de asociaciones limitadas, borran los servidores de producción, y explotan datos de socios limitados a acuerdos de *front-running*

FUENTE: Kaspersky Labs, Análisis McKinsey

D Un fuerte gobierno sobre el riesgo tecnológico es generado mediante un claro modelo de interacción a lo largo de líneas de defensa dentro del banco



D Se requiere de un exhaustivo conjunto de políticas, supervisión y actividades de evaluación del grupo CRO, CORO y ERM

	Actividades clave
I Políticas, estándares y apetito	1 Prácticas obligatorias de próxima generación, incluyendo protección diferenciada vinculada a la exposición al riesgo - ej.: protección más fuerte para procesos y activos con un mayor riesgo
	2 Asegurar una cobertura exhaustiva de tipos de riesgo de TI más allá de seguridad
	3 Definir apetito al riesgo y tolerancias para métricas clave, consistentes con el apetito general al riesgo a nivel empresa y a nivel operacional
	4 Definir roles y responsabilidades y modelo de interacción para la 2da línea vis-a-vis las funciones de TI y del negocio
	5 Establecer un modelo de compromiso para el gobierno senior, incluyendo entrenamiento y reporte del Directorio y evaluación de medidas de mitigación a nivel empresa (ej.: cíber-seguros)
II Supervisión y desafío	6 Desarrollar una visión sobre los principales riesgos, creando una visión *business-back* sobre activos de información valiosa y procesos de negocios que generan valor (ej: vinculados a sus procesos RCA0RCSA y BIA) para apoyar decisiones en donde la inversión es necesaria y donde los costos usuales del negocio pueden verse reducidos
	7 Definir un conjunto de métricas a futuro en relación a ciber-resiliencia - aquellas que proveerán a usted y al Directorio una visión de la exposición actual y sobre cómo la organización está mitigando el riesgo y mejorando a futuro
	8 Medir y gestionar la cultura al riesgo, incluyendo enrolamiento y educación del personal del *front-line*
	9 Supervisar el programa de gestión de proveedores a fin de asegurar una diligencia previa al *on-boarding*, una robusta estructuración del contrato y un continuo monitoreo
	10 Establecer procesos para el escalamiento de excepciones para requerimientos de control de riesgo tecnológico y monitoreo de los plazos de remediación / resolución
III Evaluación de la efectividad del programa	11 Realizar una evaluación independiente del estado actual y de la trayectoria del programa cibernético mediante la utilización de un *framework* consistente y exhaustivo
	12 Testear el programa de incidentes y respuesta a la crisis a fin de asegurar i) capacidad de respuesta interna y ii) que todos los socios de apoyo crítico sean seleccionados y se encuentren bajo contrato (p.ej., PR, gestión de crisis, *cyber forensics*, especialistas para respuesta a incidentes)
	13 Asegurar que las inversiones de remediación propuestas sean claramente definidas con costos, impacto esperado en el negocio y ajuste del riesgo proyectado
	14 Monitorear y comunicar requerimientos regulatorios y supervisar el reporte de cumplimiento y respuesta a remediación

D Ejemplo de métricas a nivel de Directorio

EJEMPLO DISTORSIONADO DE CLIENTE

	Lo que esto significa…	Métrica	Estado	Medición	Postura al riesgo
Comprender nuestros activos y amenazas	*¿Estamos monitoreando lo que pasa en nuestras redes y si hacemos lo que verdaderamente es importante para nosotros?*	# de nuevos activos inesperados (p.ej., tecnología) descubiertos dentro del ambiente de red	🟡	**xx/100**	**Redactado**
		% de activos que han estado sujeto a un proceso de identificación de "activos críticos"	🟡	**xx/100**	**Redactado**
Construir defensas fuertes	*¿Estamos protegiendo de forma adecuada nuestros activos en línea con el riesgo y fortalecimiento de nuestra cultura cibernética?*	$ de activos críticos evaluados para un nivel apropiado de protección	🟡	**xx/100**	**Redactado**
		% de empleados que demuestran un comportamiento de seguridad cibernética y toma de decisiones apropiado	🔴	**xx/100**	**Redactado**
Monitorear nuestro ambiente	*¿Estamos proactivamente buscando y detectando potenciales incidentes y amenazas?*	% de proyectos de terceros donde los proveedores almacenan datos críticos y cumplen con nuestras políticas de evaluación	🔴	**xx/100**	**Redactado**
		Tiempo promedio para detectar un evento crítico de ciberseguridad	🟢	**xx/0.5h**	**Redactado**
Gestionar incidentes	*¿Estamos planeando y reaccionando apropiadamente a los incidentes detectados?*	Tiempo promedio para responder a un incidente de seguridad crítico de TI	🟢	**x/1h**	**Redactado**
		% de planes de respuesta a incidentes de ciberseguridad materiales testeados/ejecutados, revisados y actualizados en los últimos 12 meses	🟢	**xx/100**	**Redactado**
Restaurar y re-encender	*¿Cómo está nuestro programa de ciberseguridad impactando a nuestro negocio?*	# de horas que los sistemas del cliente están apagados debido a un incidente de ciberseguridad en el último trimestre	🟢	**x/ 0h.**	**Redactado**
		# de incidentes de ciberseguridad materiales en el último trimestre	🟢	**x / 0**	**Redactado**

D Ejemplo de caso: Unificación del Riesgo de TI e integración con ERM

Situación

- Un cliente de la industria financiera global con **múltiples problemas con la gestión del Riesgo Tecnológico**
  - Grupo de Riesgo de Tecnológico **dedicado que reportaba al CIO, desempeñando tanto un rol de primera y segunda línea**
  - **Múltiples sub-disciplinas** de Riesgo Tecnológico (p.ej., ADM, proveedor) **no cubiertas**
  - **Sin integración de actividades de Riesgo Tecnológico con otros grupos de segunda línea** (p.ej., evaluaciones de control, reporte), llevando a un entendimiento conflictivo del estado de la gestión de riesgo

Abordaje

Evaluación del estado de Riesgo de TI en comparación a las mejores prácticas

- Realización de una evaluación a nivel de actividad de la gestión de Riesgo de TI para descubrir solapes y brechas en cobertura del riesgo material
- Evaluación de la estructura organizacional en comparación a lo visto en otras instituciones a fin de determinar potenciales conflictos de interés o estructuras atípicas
- Realización de entrevistas a las principales partes interesadas y revisión de los datos disponibles para comprender los riesgos de TI materiales que enfrentaba la organización

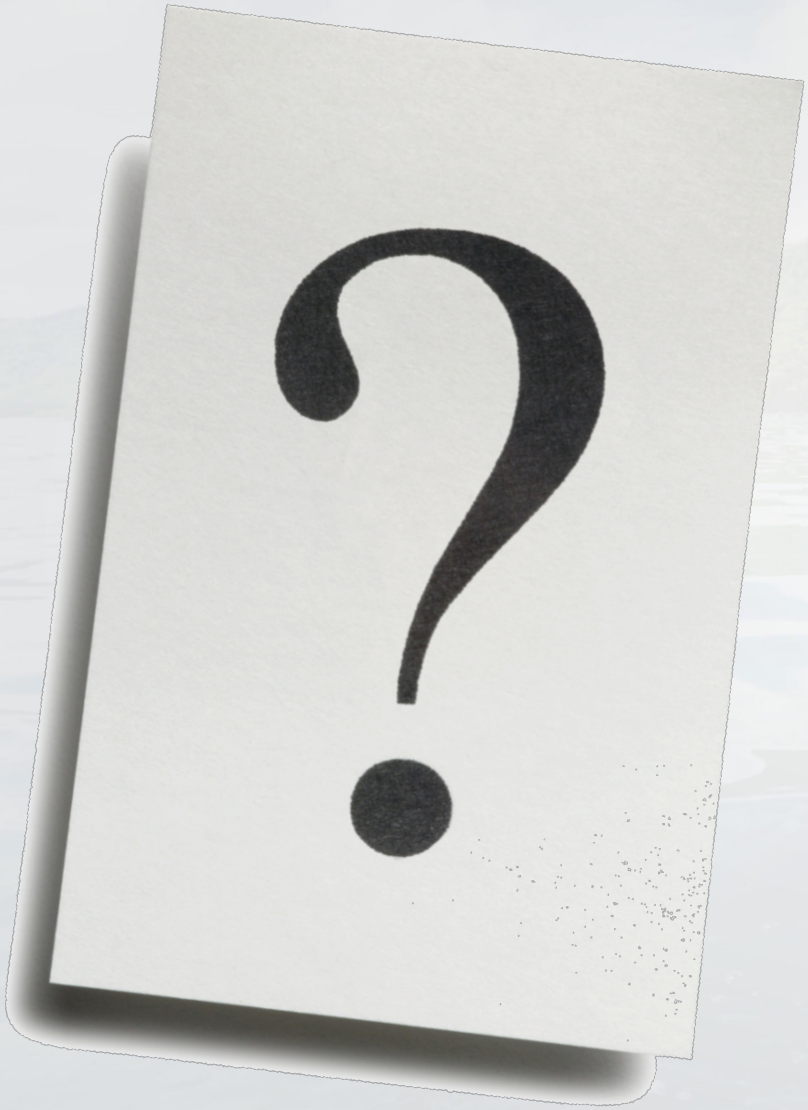
Desarrollar recomendaciones en base a los primeros principios

- Articulación de principios para la gestión del riesgo según mejores prácticas basados en líneas de trabajo de defensa
- Desarrollo de estructuras organizacionales alternativas en base al estado actual y a tendencias de la industria
- Creación de cuadros RACI de nivel de actividad para impulsar una integración más cercana de gestión del riesgo de TI con Gestión del Riesgo Empresarial (ERM por sus siglas en Inglés)
- Desarrollo de un modelo de cobertura para Riesgos de TI a fin de eliminar brechas y duplicación de actividades

Resultados obtenidos

- La **organización dejó de tener múltiples problemas con la gestión de Riesgo de Tecnológico** para implementar prácticas según estándares de la industria
- Comenzar a partir de principios resultó crítico para generar credibilidad en la organización y resaltar los problemas
- El **grupo de Riesgo Tecnológico dejó de estar por debajo de ERM** a asegurar un alineamiento más cercano con gestión del riesgo general y eliminar inconsistencias en reporte y evaluación
- Las **actividades obligatorias del grupo de Riesgo Tecnológico se han expandido y aclarado** a fin de asegurar una exhaustiva cobertura de segunda línea en la institución

Preguntas



Contacto

David Ware
Socio Asociado
David_Ware@mckinsey.com