

XXXV ENCUESTO NACIONAL DE AUDITORES INTERNOS



Yves B. Desharnais,
MBA, CISSP, PCIP

Organizaciones Bajo Ataque - Ciberseguridad



XXXV

ENCUENTRO NACIONAL
DE AUDITORES INTERNOS

Sobre Yves...

- Comenzó a trabajar en Seguridad de la Información (Cyberseguridad) en 2001 en Guadalajara, Jalisco (México)
- Experto en TI/InfoSec con más de 18 años de experiencia en seguridad de la información, auditoría de TIC, desarrollos, Unix/Linux
- Ingeniero en Computación, U. de Sherbrooke (Canadá)
- MBA, Universidad de Notre Dame (EUA)
- Certificado como CISSP y PCIP
- Autor de diversos libros en la materia (www.pciresources.com)

Agenda

- Transgresiones recientes
- Tríada de controles
- Dónde puede ayudar la Auditoría Interna
- Principios básicos de seguridad
- (Algunas) Tendencias actuales de tecnología – pros y contra, y papel de la AI

Contexto: Nuestro mundo cada vez más conectado

- Vivimos en un mundo:
 - Con luces automatizadas que minimizan el costo de la electricidad
 - Con refrigeradores que nos indican cuándo hay que comprar leche, o detectan la ausencia de personas en casa (ya que nadie ha abierto la puerta en días)
 - Con bombas médicas que automáticamente administran medicamentos, o que pueden causar sobredosis (por malicia o error)
 - Con autos automatizados que reducen los errores humanos y aseguran que llegues a casa con seguridad, o que pueden desviarnos del camino
- Todo avance tecnológico trae cosas buenas y malas, según el uso e implementación que le demos
- Todos debemos asegurarnos que el saldo sea positivo

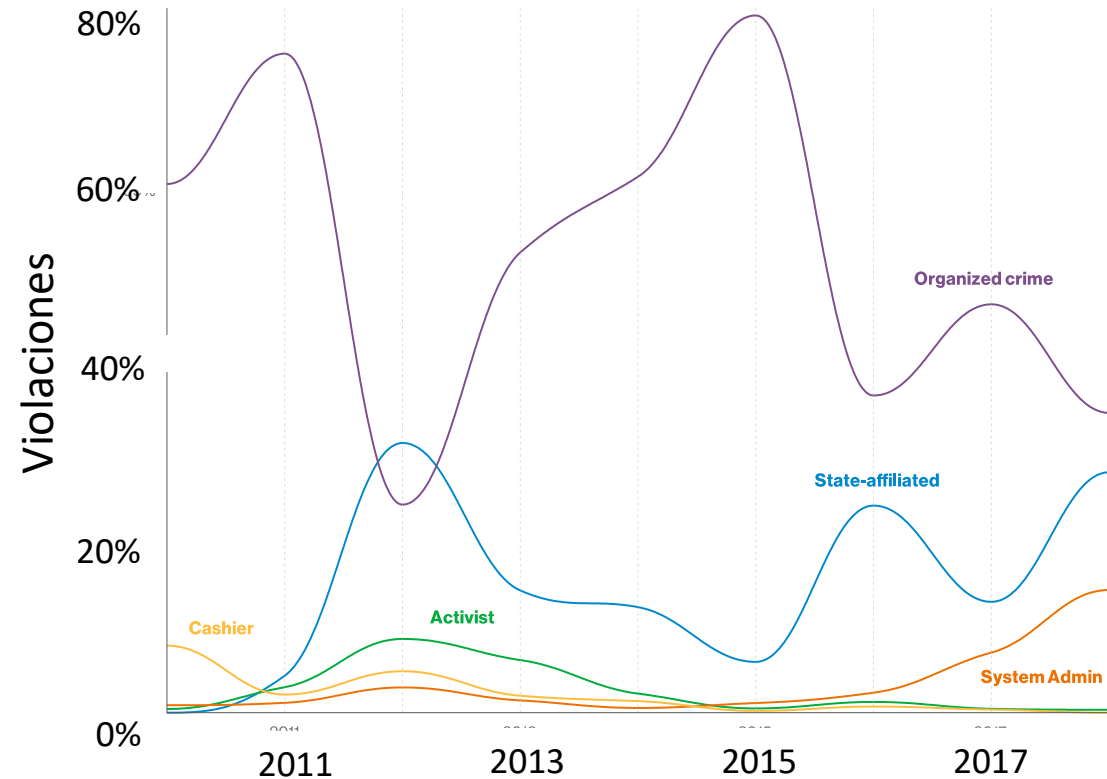
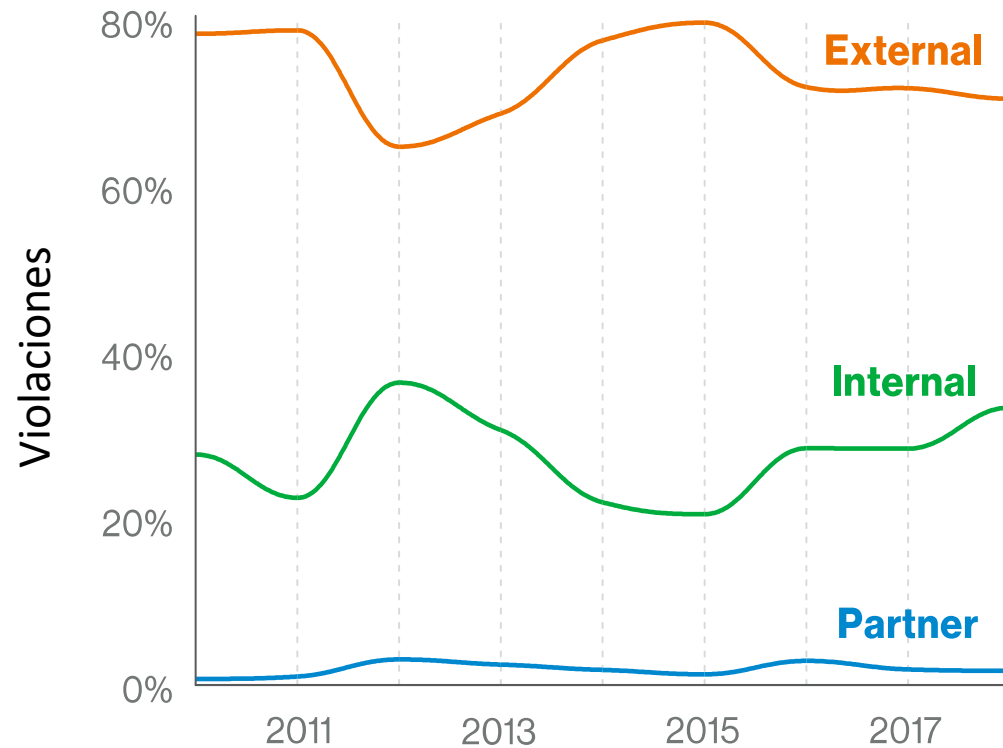
Transgresiones recientes

Cuándo	Quién	Dónde	Qué	Cómo	Causa-raíz
Julio 2019	Capital One	EUA	Datos de más de 100 millones de cuentas	Robo por alguien de adentro	USO INDEBIDO
Abril 2019	KPMG	México	Datos de nómina de 41 clientes	Configuración inadecuada de base de datos	ERROR HUMANO
Abril 2019	Facebook	México	Archivo de 146 GB de una compañía de medios con base en México	Configuración inadecuada de AWS S3	ERROR HUMANO
Abril 2018	5 compañías	México	~ 300 millones de pesos (\$15.33 millones de dólares)	Explotación de una vulnerabilidad de la aplicación SPEI	Explotación de controles básicos de seguridad y vulnerabilidades

No hay una causa-raíz única, pero en casi todos los casos había ausencia de controles básicos

Transgresiones a bases de datos

Actores a lo largo del tiempo



Fuente: Informe de Investigaciones a Transgresiones de Datos de Verizon 2019, p.6

Dónde pueden ayudar los Auditores Internos

Modelo de las Líneas de Defensa

- The IIA publicó el modelo “Las tres líneas de defensa para una administración de riesgos eficaz”¹
- Se propuso un modelo extendido llamado Las Cinco Líneas del Aseguramiento² para corregir las deficiencias del primero
- El informe “Verizon 2018 PCI Compliance Report” propone un modelo de 4 líneas³:

1	Responsabilidad individual
2	Funciones de gestión de riesgos y cumplimiento
3	Auditoría Interna
4	Auditoría externa, reguladores y agentes externos

Las Cuatro Líneas del Aseguramiento

1. theiia.org/3-Lines-Defense
2. riskoversightsolutions.com/wp-content/uploads/2011/03/Risk-Oversight-Solutions-for-comment-Three-Lines-of-Defense-vs-Five-Lines-of-Assurance-Draft-Nov-2015.pdf
3. Verizon 2018 PCI Compliance Report, p.15

Dónde pueden ayudar los Auditores Internos

Las Cuatro Líneas del Aseguramiento

	Línea de Aseguramiento	Funciones	Roles / Grupos
1	Responsabilidad individual	Funciones que poseen y administran riesgos	Controles gerenciales Medidas de control interno
2	Funciones de gestión de riesgos y cumplimiento	Funciones que supervisan riesgos	Contralor financiero, Administración de riesgos de seguridad, Calidad, Inspección, Cumplimiento
3	Auditoría Interna	Funciones que dan aseguramiento independiente	Auditoría Interna
4	Auditoría Externa, reguladores y agentes externos	Actores externos que supervisan	Reguladores del gobierno y la industria, Consejo Directivo

Tercia de controles y seguridad

Tercia de controles

- Conocidos por los auditores, por su relación con las auditorías financieras
 - Preventivos
 - Detectivos
 - Correctivos

Tercia de seguridad (C.I.A.)

- Objetivos
 - Confidencialidad
 - Integridad
 - disponibilidad

En mi experiencia, la clave de una buena seguridad son procesos sólidos que se aplican de manera consistente. ¡La auditoría interna está bien posicionada para ayudar aquí!

Principios básicos de seguridad (1/2)

Minimización de datos

- Requerido por GDPR* / privacidad
- “Recuerda, si no lo necesitas, no lo almacenes” – PCI DSS 3.2.1, p.37
- Borrar cuando ya no se necesita; si no lo puedes borrar, archívalo (hazlo más difícil de conseguir)
- Controla la distribución de datos: el verdadero secreto es el que nunca se comparte

Privilegio final / Necesidad de saber

- Minimiza quién accede a los datos
- Permite acceso a roles, no a personas
- Desarrolla y aplica una política de sanciones
- Revisa periódicamente quién tiene acceso y confirma que su acceso es requerido
- Revisa periódicamente quién ha ingresado al sistema para negar el acceso tras 30 a 90 días



*GDPR: General Data Protection Regulation

XXXV

ENCUENTRO NACIONAL
DE AUDITORES INTERNOS



Principios básicos de seguridad (2/2)

Defensa profunda

- Tu perímetro de red se ha roto
- Tus datos están en todos lados:
 - Usuario final de laptop
 - Usuario final de teléfonos (incluyendo BYOD)
 - Servidores internos
 - La nube
 - Terceros
- Segmenta las redes, controla cada entrada a las redes

Asegura los procesos y la confiabilidad

- Asegura que puedes medir si los procesos se están cumpliendo
- Genera métricas (KPI, indicadores clave de desempeño) que puedas revisar
- Audita los procesos para asegurar que se siguen (aún mejor si las fallas se detectan automáticamente)



**ENCUENTRO NACIONAL
DE AUDITORES INTERNOS**



Tendencias actuales de tecnología (1/6)

Virtualización : se refiere al acto de crear una versión virtual (no real) de algo, casi siempre Máquinas Virtuales Machines o VMs.

Pros	Contras	Cómo puede ayudar la AI
<ul style="list-style-type: none">• Permite el uso más eficiente de recursos computacionales• Permite Sistemas Operativos (OS) múltiples• Existe para PC, Mainframe	<ul style="list-style-type: none">• Menos aislamiento que máquinas físicas	<ul style="list-style-type: none">• Asegura que las VMs estén aisladas a nivel de red en diferentes zonas de seguridad (segmentación de redes) con reglas de acceso entre zonas (y la regla de “Negar todo” por algo, que no esté autorizada)

Tendencias actuales de tecnología (2/6)

Contenedores: conocida como virtualización a nivel de sistema operativo; los contenedores son similares a las VMs pero comparten un mismo sistema operativo (no el hardware)

Pros	Contras	Cómo puede ayudar la AI
<ul style="list-style-type: none">• Más ligero (en tamaño y recursos)• Se adquiere más rápido• Permite ambientes dev/non-prod/prod más similares• Adecuada para DevOps	<ul style="list-style-type: none">• Menos aislamiento y seguridad entre contenedores (memoria, sistema de archivos, redes)• Menos flexibilidad en Sistemas Operativos (OS) – generalmente Linux	<ul style="list-style-type: none">• Asegura que los contenedores según roles de seguridad y/o riesgos estén aislados en VM diferentes en distintas redes• Asegura la preservación de un log específico para todos los contenedores creados y destruidos

Tendencias actuales de tecnología (3/6)

La nube: producto de la virtualización con la tercerización

Pros	Contras	Cómo puede ayudar la AI
<ul style="list-style-type: none">• Permite mayor flexibilidad y mejores costos• Puede ofrecer mejor seguridad (C.I.A.) que un centro de datos administrado a nivel local	<ul style="list-style-type: none">• No contar con control total sobre el entorno• Algunos servicios pueden no ser provistos con configuraciones seguras por default	<ul style="list-style-type: none">• Asegura que los roles y responsabilidades estén bien definidos entre el cliente y el proveedor• Asegura que existen procesos rigurosos que son aplicados en todos los ambientes utilizados en la nube

Tendencias actuales de tecnología (4/6)

Modelo de tolerancia cero- modelo de seguridad de TI que requiere de una estricta verificación de identidad para cada persona y aparato que intenta acceder a los recursos de una red privada, sin importar si se encuentran dentro o fuera del perímetro de la red (fuente: Cloudflare) – por lo general requiere del uso de “micro-segmentación”

Pros	Contras	Cómo puede ayudar la AI
<ul style="list-style-type: none">Mucho mejor nivel de detalle de control sobre los flujos de datos de la red (puede ser requerida para redes sensibles y de defensa)	<ul style="list-style-type: none">Alto costo de implementación, mantenimiento (por lo general mediante modelos automatizados)	<ul style="list-style-type: none">Asegura que se ha establecido un caso de negocios apropiado

Tendencias actuales de tecnología (5/6)

Inteligencia Artificial (IA) : la mayoría de soluciones que utilizan el término IA son en realidad Conocimiento de Máquinas (Machine Learning).

Conocimiento de Máquinas (ML) : uso de modelos computacionales para identificar correlaciones estadísticas dentro de un grupo de datos (categorización)

Pros	Contras	Cómo puede ayudar la AI
<ul style="list-style-type: none">• Permiten determinar nuevos conocimiento a partir de la información existente (pero también las regresiones estadísticas tradicionales lo pueden hacer)	<ul style="list-style-type: none">• El valor de negocio no es usualmente evaluado sobre el análisis de datos estándar	<ul style="list-style-type: none">• Asegura que un caso de negocios apropiado existe, y que éste toma en consideración los beneficios, riesgos añadidos (combinar múltiples fuentes de información valiosa), etc.

Tendencias actuales de tecnología (6/6)

- **DevOps** – prácticas que integran desarrollo de software con operaciones de TI, con automatización, para mejorar la velocidad de su comercialización; los DevSecOps, que integran seguridad, han surgido para ayudar a gestionar los riesgos de las DevOps

Pros	Cons	Cómo puede ayudar la AI
<ul style="list-style-type: none">• Mejoran la velocidad con que entran al mercado• Minimizan los errores humanos	<ul style="list-style-type: none">• La mayoría de los desarrolladores no son expertos en seguridad, por lo que introducen nuevos riesgos• Problemas de segregación de funciones (SoD) entre los dev y los ops	<ul style="list-style-type: none">• Asegura que los requerimientos de seguridad (no-funcionales) están implementados antes del lanzamiento• Asegura que exista SoD o controles equivalentes• Asegura el uso de modelado de amenazas por parte del equipo de desarrolladores

Questions? ¿Preguntas?

¡Gracias, Thanks!

