CIO vs CISO: OWASP al rescate

OWASP

The Open Web Application Security Project

OWASP
The Open Web Application Security Project

- Ing. Mauro Graziosi.
- CISO en Rectorado de la Universidad Nacional del Litoral (Santa Fe).
- Consultor independiente (ISO/IEC 27001).
- Docente de ISO/IEC 27000 en IRAM Litoral.
- Emprendedor.

OWASP
The Open Web Application Security Project

Temario

- CIO vs CISO
- Contenido de la guía OWASP CISO
- Como puede ayudarnos OWASP y esta guía a ganar la batalla
- Recomendaciones

OWASP
The Open Web Application Security Project

*...choque de intereses entre lo **ágil** del negocio , la **rapidez**, etc... con la seguridad...*

*La seguridad va siempre en contra de la **funcionalidad** y **agilidad** que espera el negocio.*

OWASP
The Open Web Application Security Project

Agregar temas de seguridad , implica ***demorar*** *algunas soluciones.*

...el lider de desarrollo no tiene debidamente en cuenta la seguridad porque prioriza lo ***funcional****...*

OWASP
The Open Web Application Security Project

*...el perfil del CISO debe ser la de una persona que piense siempre su trabajo parado desde el punto de vista de la **funcionalidad;***

*y los responsables Desarrollo que tengan en cuenta a la **seguridad** y no la sacrifiquen en pos de lograr una funcionalidad lo antes posible.*

OWASP
The Open Web Application Security Project

¿Y cómo nos deja esto parados?

OWASP
The Open Web Application Security Project

Y llega el pesado de seguridad informática...

S-SDLC,
BSIMM,
Habeas Data,
Cifrado, Data Masking,
Licenciamiento,
Contratos de escrow, NDAs
...

OWASP
The Open Web Application Security Project

OWASP al rescate

OWASP
The Open Web Application Security Project

Contenido de la guía OWASP CISO

- Razones para **invertir** en Seguridad de las Aplicaciones.
- Criterios para gestionar los **riesgos** de seguridad en aplicaciones.
- **Programa** de Seguridad de Aplicaciones.
- **Métricas** para Gestionar Riesgos e Inversiones en Aplicaciones de Seguridad.

OWASP
The Open Web Application Security Project

Riesgos de negocio vs riesgos técnicos

Los riesgos de seguridad pasan a ser riesgos del negocio sólo cuando existen estas tres características:

- Amenaza viable
- Vulnerabilidad que puede ser expuesta
- **Activos de valor**

OWASP
The Open Web Application Security Project

Seguridad en el SDLC (ROI o ROSI)

- 21%, fase de **diseño**: análisis de riesgos de la arquitectura y el modelado de amenazas de la aplicación.
- 15%, fase de **implementación**: análisis de código fuente;
- 12%, fase de **prueba**: pruebas de validación, pruebas de intrusión/hacking ético.

Fuente: Investigación de Soo Hoo (IBM) del ROSI

OWASP
The Open Web Application Security Project

Gestión de riesgos: proactiva vs. reactiva

organización *seguridad*

OWASP
The Open Web Application Security Project

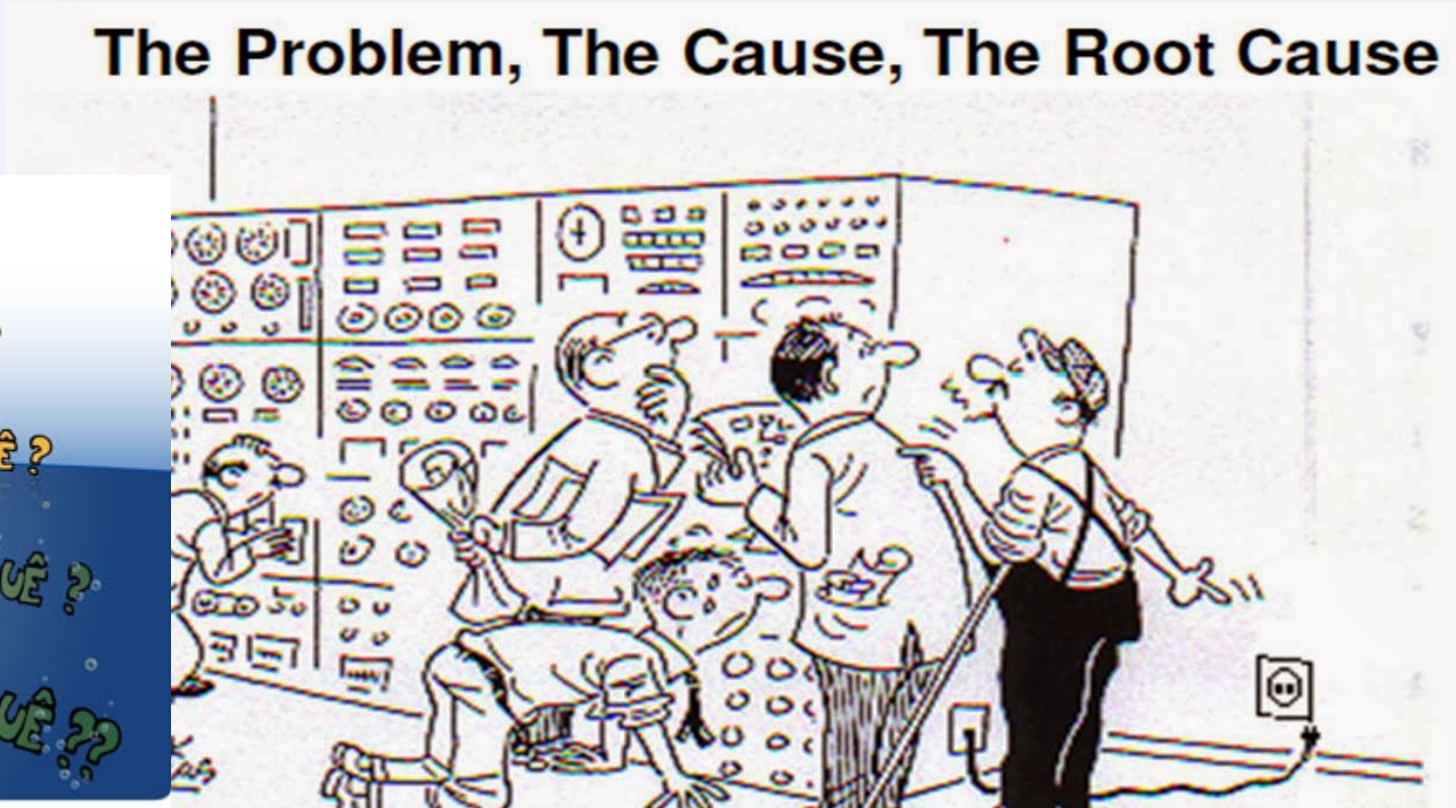
Gestión de riesgos: proactiva vs. reactiva

organización

seguridad

OWASP
The Open Web Application Security Project

La oportunidad de los incidentes...



OWASP
The Open Web Application Security Project

Recomendaciones de la guía

- Concientización y entrenamiento.
- Integrar la seguridad en el ciclo de desarrollo.
- Hacer programas de seguridad que incluyan a:
  - Personas (capacitación y organización)
  - Procesos (gestión de riesgos, S-SDLC, Guías, Políticas, Pruebas)
  - Tecnología (herramientas, desarrollo, frameworks)

OWASP
The Open Web Application Security Project

Beneficio de la guía OWASP CISO

Referencia a los documentos relevantes dentro de OWASP

OWASP
The Open Web Application Security Project

Beneficios de OWASP

Une el QUE con el COMO

Es multiuso

OWASP
The Open Web Application Security Project

Beneficios de OWASP

Es atractiva

OWASP
The Open Web Application Security Project

Cierre

- ¿Qué pasa por la cabeza del CIO y del responsable de desarrollo? entender sus preocupaciones.
- Inversiones: sobre riesgos del negocio, en etapas tempranas del SDLC... y estar preparado para aprovechar los incidentes.
- Usar OWASP para conseguir las inversiones.
- Aprender a escuchar y a persuadir.

OWASP
The Open Web Application Security Project

¡Muchas gracias!

Frase de un CIO:

"Tener una persona que se ocupe de la seguridad ayuda muchísimo ya que no es algo que este en la agenda permanente del CIO".

Mauro Graziosi
mgraziosi@gmail.com