La necesidad de construir software seguro

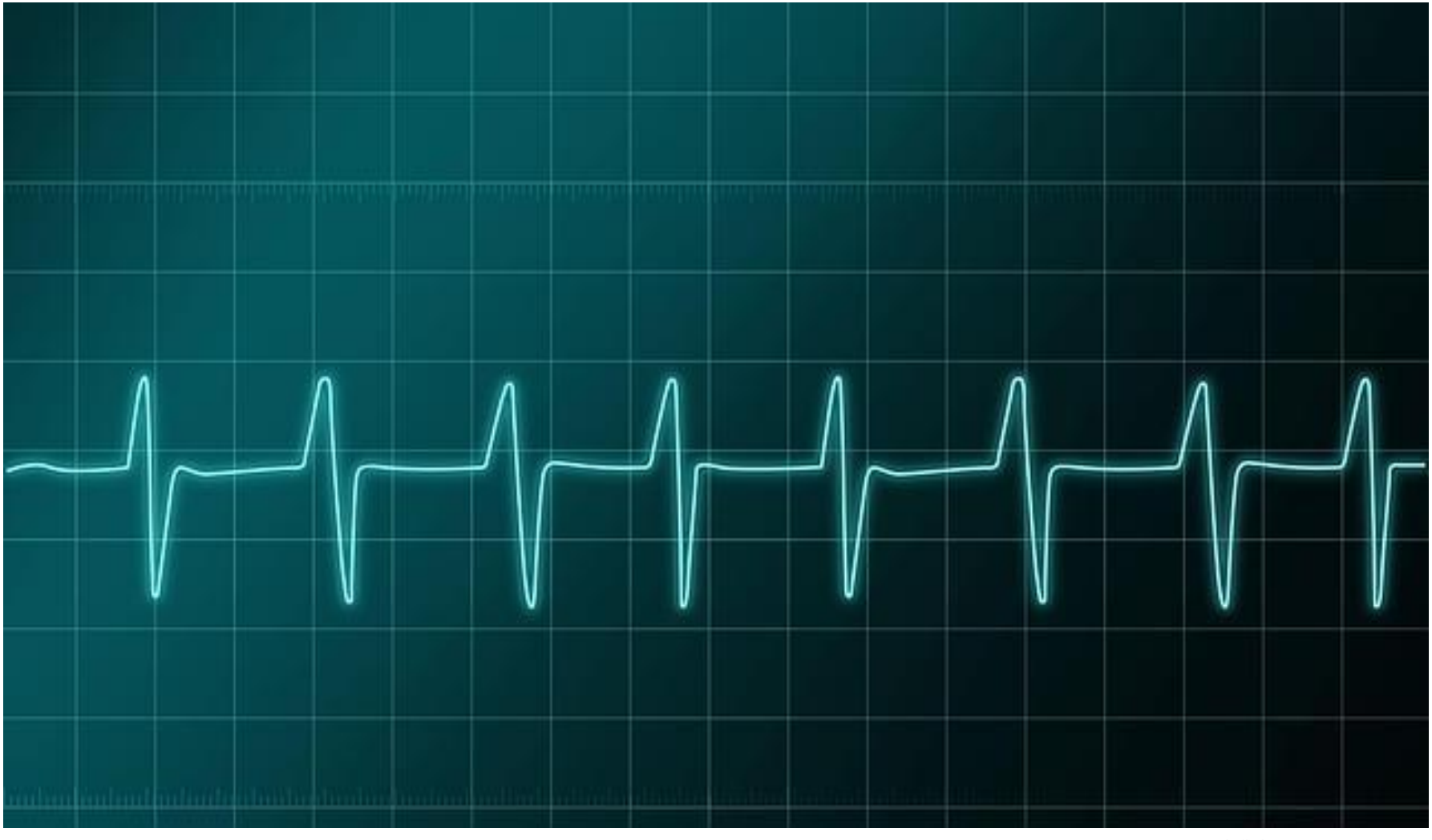
Vicente Aguilera Díaz
vicente.aguilera@owasp.org
OWASP Spain Chapter Leader
Socio de Internet Security Auditors

IBM Software Summit #START013. Madrid 06/11/2012.

Agenda

- Dependencia del software
- Construcción de software seguro
- OWASP
- Conclusiones y recomendaciones

Dependencia del software



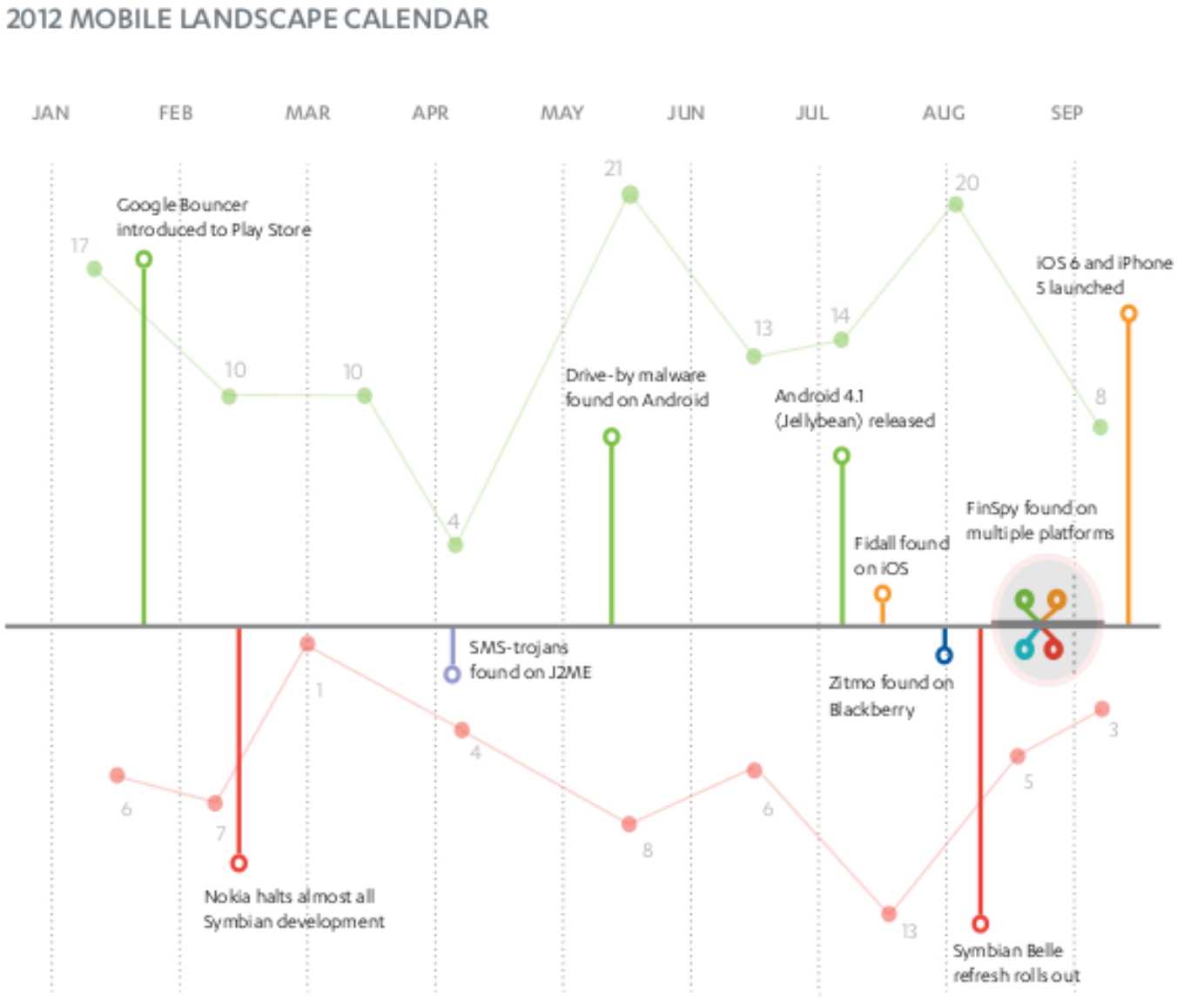
Dependencia del software

- Es crítico crear software seguro:
  - Conectividad
  - Complejidad
  - Extensibilidad
  - … y requerimientos normativos

Dependencia del software

- ¿Y el mundo de los dispositivos móviles?

Dependencia del software



Construcción de software seguro

Construcción de software seguro

- ¿Qué entendemos como software seguro?
  - Diseñado, construido y probado para su seguridad
  - Continúa ejecutándose correctamente bajo ataque
  - Diseñado con el fallo en mente

Construcción de software seguro

- ¿Porqué ha cobrado tanta relevancia?
  - Proliferación de modelos de negocio en la web
  - Las aplicaciones resultan muy atractivas
  - Auge de los dispositivo móviles
  - La mayoría de aplicaciones son vulnerables
  - Nuevos requerimientos normativos

Construcción de software seguro

- ¿Porqué ha cobrado tanta relevancia?

Philippines appeals to hackers to cease attacks

Recomendar 7 personas han recomendado esto. Sign Up para ver qué recomiendan tus amigos.

By Agence France-Presse
Saturday, October 6, 2012 19:00 EDT

Bank Cyber Attacks Originated From Hacked Data Centers, Not Large Botnet

05 Oct 2012 / Comments Off / in News / by Sera-Brynn

THE CYBERCRIME ECONOMY

'Massive' credit card data breach involves all major brands

CNNMoney

603 comments

By Julianne Pepitone and Leigh Remizowski @CNNMoneyTech April 2, 2012: 6:53 AM ET

Construcción de software seguro

- Todo es posible en la web

Inglaterra subasta el portaaviones "HMS Invincinble" en internet

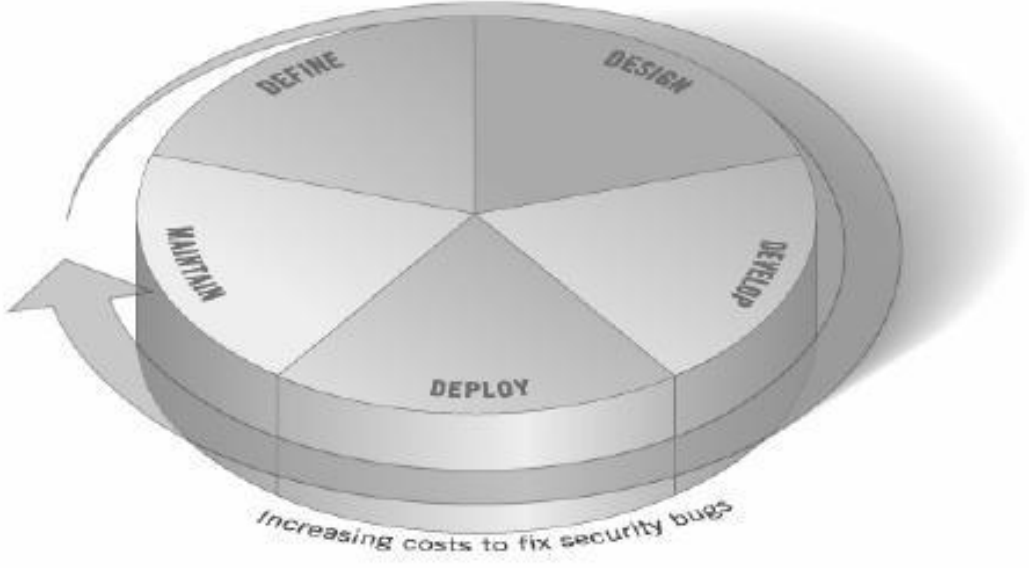
El Ministerio acepta pujas por el Invencible, que participó en la guerra de las Malvinas de 1982, en su página web de "servicios de disposición" (**www.edisposals.com**), creada para vender equipo militar excedente.

Construcción de software seguro

- ¿Cómo conseguir crear software seguro?
  - Adoptar un modelo de madurez
  - La seguridad debe ser considerada desde el inicio
  - S-SDLC es la clave

Construcción de software seguro

- Secure SDLC es la clave
  - SDLC basado en principios de seguridad
  - No existe una fórmula única para su implementación
  - Implica a personas, procesos y tecnología



Construcción de software seguro

- Iniciativas de seguridad en el desarrollo de software:
  - Microsoft SDL
  - OWASP CLASP
  - Cigital Software Security Touchpoints
  - OWASP OpenSAMM
  - BSIMM
  - SSE CMM

Construcción de software seguro

- Ejemplos de actividades de seguridad:
  - Clasificar datos y aplicaciones según su riesgo
  - Desarrollar y mantener guías de cumplimiento
  - Realizar formación en seguridad para cada rol
  - Elaborar modelos de amenaza
  - Identificar patrones de seguridad en el diseño
  - Realizar revisiones de código
  - Realizar pruebas de seguridad en las aplicaciones
  - Establecer hitos para la revisión del diseño
  - Crear procedimientos de gestión de cambio

OWASP

OWASP

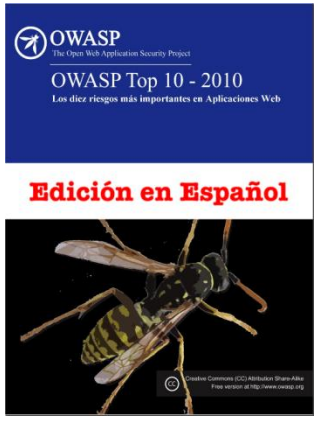
The Open Web Application Security Project

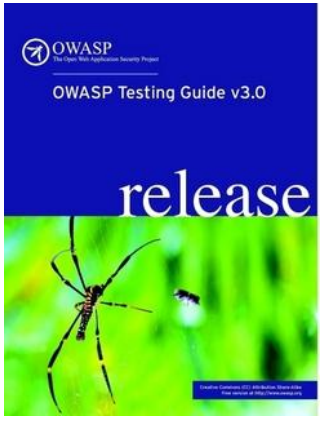
OWASP

- Comunidad libre y abierta sobre seguridad en aplicaciones
- Búsqueda y lucha contra las causas de software inseguro
- Creación de herramientas, documentación y estándares
- Conferencias
- Recursos gratuitos y de código abierto
- 10.000 miembros y 250 capítulos locales en el mundo
- Más de 200 proyectos
- www.owasp.org

OWASP

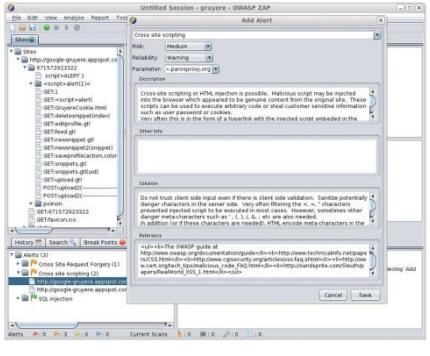
- Principales proyectos a nivel de documentación:
  - Top 10
  - Guía de pruebas
  - Guía de desarrollo
  - Guía de revisión de código
  - ASVS



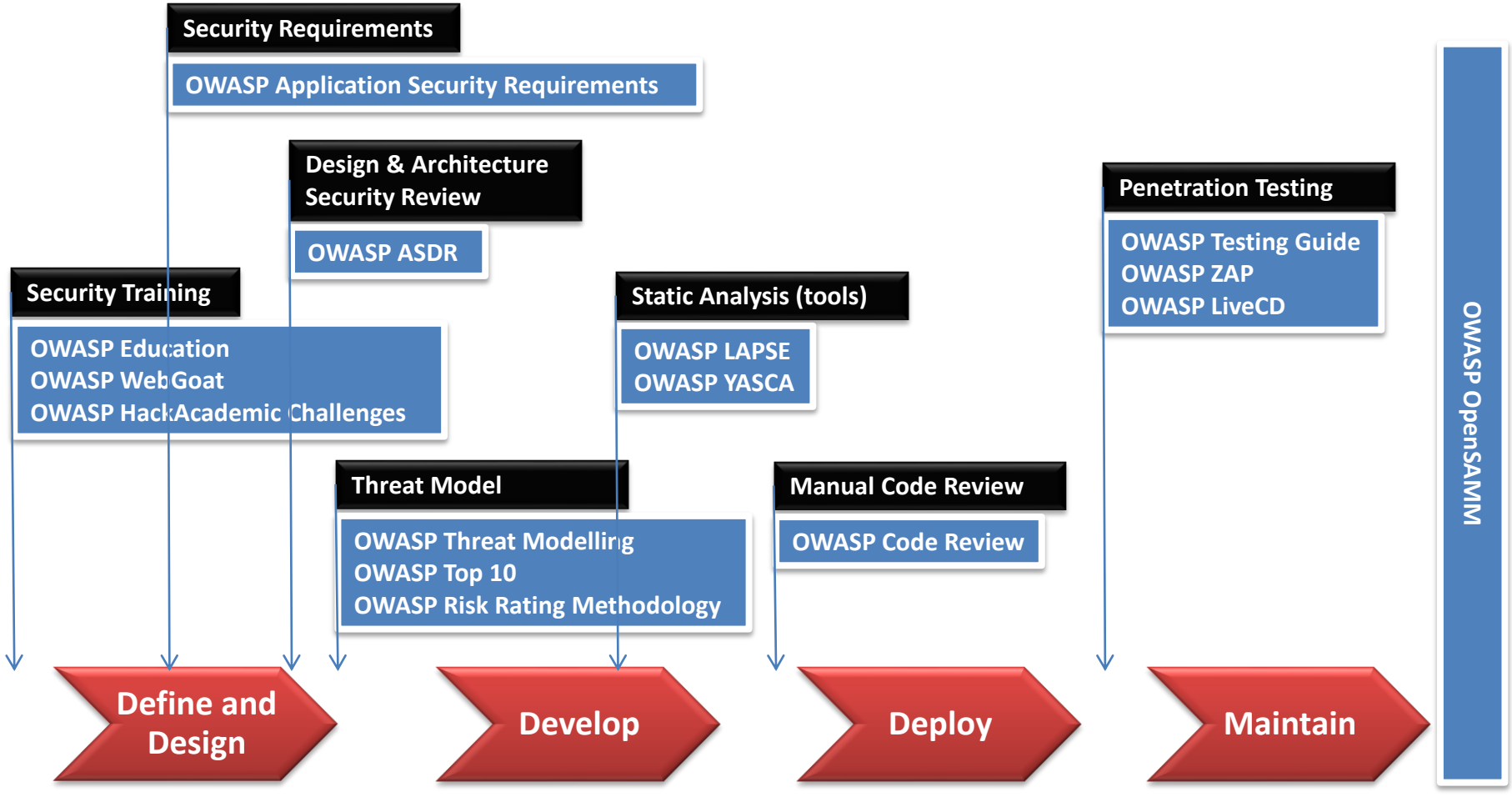


OWASP

- Principales proyectos a nivel de herramientas:
  - ZAP
  - WebGoat
  - ESAPI
  - Live CD



OWASP


Security Requirements
OWASP Application Security Requirements
Design & Architecture Security Review
OWASP ASDR
Penetration Testing
OWASP Testing Guide
OWASP ZAP
OWASP LiveCD
Security Training
OWASP Education
OWASP WebGoat
OWASP Hack Academic Challenges
Static Analysis (tools)
OWASP LAPSE
OWASP YASCA
OWASP OpenSAMM
Threat Model
OWASP Threat Modelling
OWASP Top 10
OWASP Risk Rating Methodology
Manual Code Review
OWASP Code Review
Define and Design
Develop
Deploy
Maintain

Conclusiones y recomendaciones

Conclusiones

- Necesitamos crear software seguro
- Debemos conocer todos los riesgos y cómo mitigarlos
- Necesitamos invertir más en la seguridad del software
- Software seguro ≠ código seguro

Recomendaciones

- Clasificar las aplicaciones y definir niveles de seguridad
- Verificar la adopción de los requerimientos de seguridad
- Crear el software pensando en los casos de abuso
- Huir de la solución “todo en uno”
- Seguir el principio de defensa en profundidad
- Identificar los marcos regulatorios y su cumplimiento
- Equiparar requerimientos de seguridad a los funcionales
- Estar informado sobre las amenazas existentes
- No despreciar soluciones open-source
- Potenciar la cultura de la seguridad en la organización

?

dudas / comentarios/ sugerencias

¡Muchas gracias!