Seguridad en el Software y El Monstruo del Lago Ness

Calidad y Seguridad en el Software – Junio 2016

CSX™ CYBERSECURITY NEXUS

COBIT 5

ISACA® Sistemas de información fiables y valiosos Valencia Chapter

Agenda

- ¿Quién y qué es ISACA?
- Seguridad del Software
- Ciberataques: mapas, ejemplos, principales ciberataques
- Consejos prácticos
- Mas información

ISACA Sistemas de información fiables y valiosos Valencia Chapter

2

¿Quiénes somos?

ISACA es el acrónimo de Information Systems Audit and Control Association (Asociación de Auditoría y Control de Sistemas de Información), una **asociación internacional sin animo de lucro** que apoya y patrocina el desarrollo de metodologías y certificaciones para la realización de **actividades auditoría y control en sistemas de información**.

3

Objetivos

La misión de los capítulos de ISACA es de promover la educación y la mejora del conocimiento y las habilidades de sus miembros, ayudándolos a lograr y mantener sus certificaciones que los acreditan como profesionales de primer nivel y calidad, a través de diversas actividades, tales como foros, conferencias, talleres y seminarios.

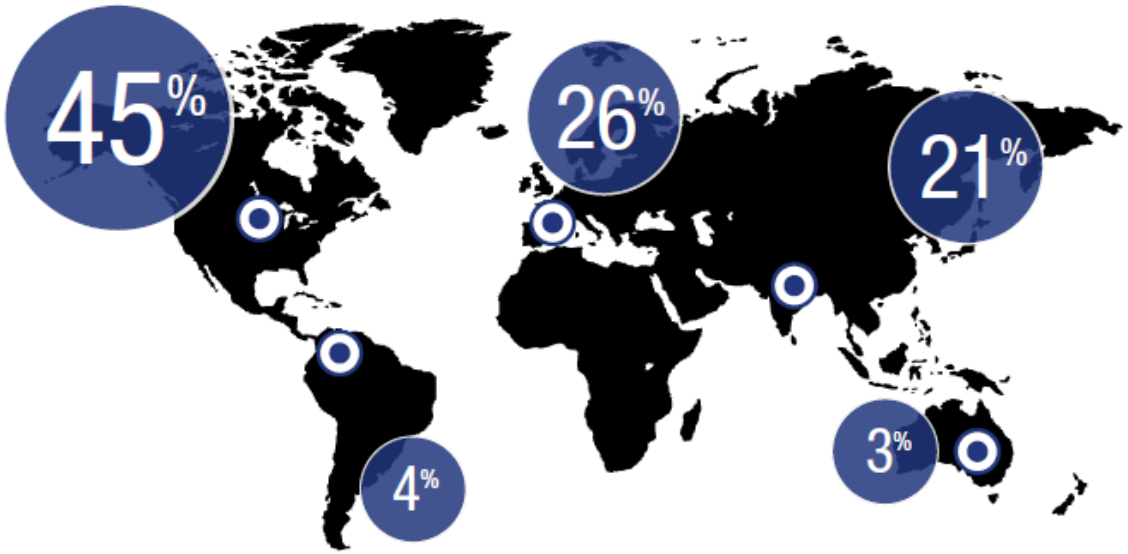
4

ISACA en el mundo

CYBERSECURITY NEXUS

Más de 140.000 miembros, 200 capítulos y 180 países

Socios en más de 180 Países



45% EE.UU. y Canadá	26% Europa y África	21% Asia y Oriente Medio
4% Centro y Sudamérica	3% Australia y Nueva Zelanda	

ISACA Sistemas de información fiables y valiosos Valencia Chapter

5

ISACA en España

Capítulos en Madrid, Barcelona y Valencia

6

Nuestras certificaciones

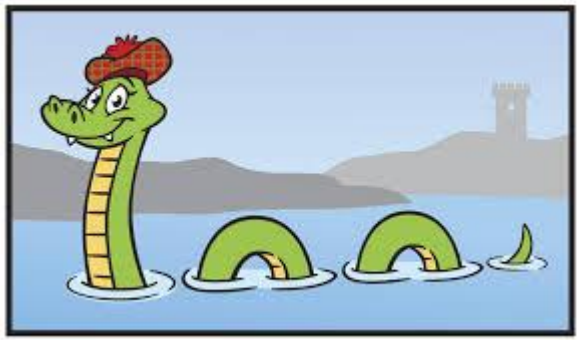
CYBERSECURITY NEXUS

ISACA ofrece certificaciones lideres en la industria

7

Seguridad del Software

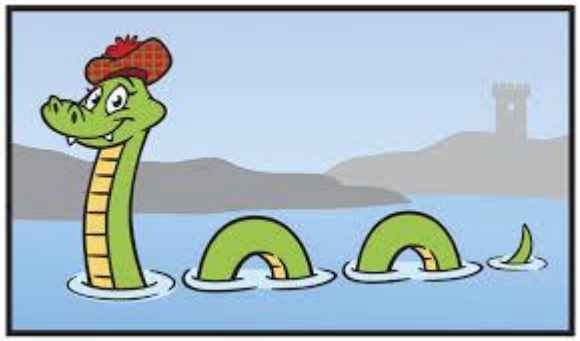
Software. **Miles** de líneas de código que ofrecen unas funcionalidades concretas. A veces el software está **relacionado** con otras programas y/o es **dependiente** de otras programas o librerías **desarrolladas por otras** empresas hace años.



Contra medidas

Revisión o pruebas del código

- Pruebas de concepto
- Pruebas unitarias
- Pruebas funcionales
- Pruebas de integración
- Pruebas de aceptación



9

Algunos casos

Se obtiene los datos de tarjetas y compras de los clientes almacenados en una aplicación donde están todas las órdenes de compra de los clientes de una importante empresa.

10

Algunos casos

Se consigue acceder a la aplicación que controla una máquina de transporte pudiendo variar su comportamiento en directo.

Algunos casos

La información almacenada en una aplicación sanitaria no se graba teniendo en cuenta las unidades de medida que el usuario utiliza. La aplicación espera kilogramos y el usuario introduce libras. NO EXISTE LOCALIZACIÓN.

Ciberataques

España, tercer país del mundo en ciberataques. Madrid, Barcelona y Valencia principales objetivos.

http://cadenaser.com/ser/2014/11/25/ciencia/1416920321_278876.html

13

Mapa Norse

http://map.norsecorp.com/

Mapa Norse de Ciberataques en Tiempo Real

14

Principales ciberataques de la historia

1) El gran *hack* de EE.UU.: 160 millones de usuarios. 2005-2012
2) Adobe: 152 milllones de usuarios. Octubre del 2013
3) eBay: 145 millones de usuarios. Mayo 2014
4) Heartland: 130 millones de usuarios. 2008
5) TJX: 94 millones de usuarios. 2007
6) AOL: 92 millones de usuarios. 2004
7) Sony PlayStation Network: 77 millones de usuarios. Dic 2014
8) Veteranos de EE.UU.: 76 millones de usuarios
9) Target: 70 millones de usuarios. Noviembre 2013
10) Evernote: 50 millones de usuarios. Marzo 2013

http://es.gizmodo.com/los-10-mayores-ataques-informaticos-de-la-historia-1580249145

15

Guerra Cibernetica entre estados

Guerra Cibernética EEUU-Irán:

https://www.youtube.com/watch?v=YuNyfKGCbHo

16

Guerra Cibernetica entre estados y empresas privadas

Sony – Corea del Norte:

https://www.youtube.com/watch?v=D36e7msySfs

17

Hacking de entidades bancarias

JP Morgan:

https://www.youtube.com/watch?v=5E7yhQe9fTc

18

Hackear un coche

Hacking Car:

https://www.youtube.com/watch?v=dHZImzD1CbY

19

Hackear un avión

Hacking Avión:

https://www.youtube.com/watch?v=j4Cm9S6T3MA

20

Hackear una cadena de supermercados.

Target.

https://www.youtube.com/watch?v=g_qeY5qs264

21

Target en detalle

Entre **el 1 y el 15 diciembre de 2013**, los hackers ejecutaron un ataque cibernético contra la empresa **Target**, una de las mayores compañías de venta al por menor en los Estados Unidos. Los atacantes obtuvieron acceso a la red informática de Target, robaron la información personal y financiera de un máximo de 110 millones de clientes objetivo, y luego enviaron esta información sensible de la red de Target a un servidor de Europa del Este.

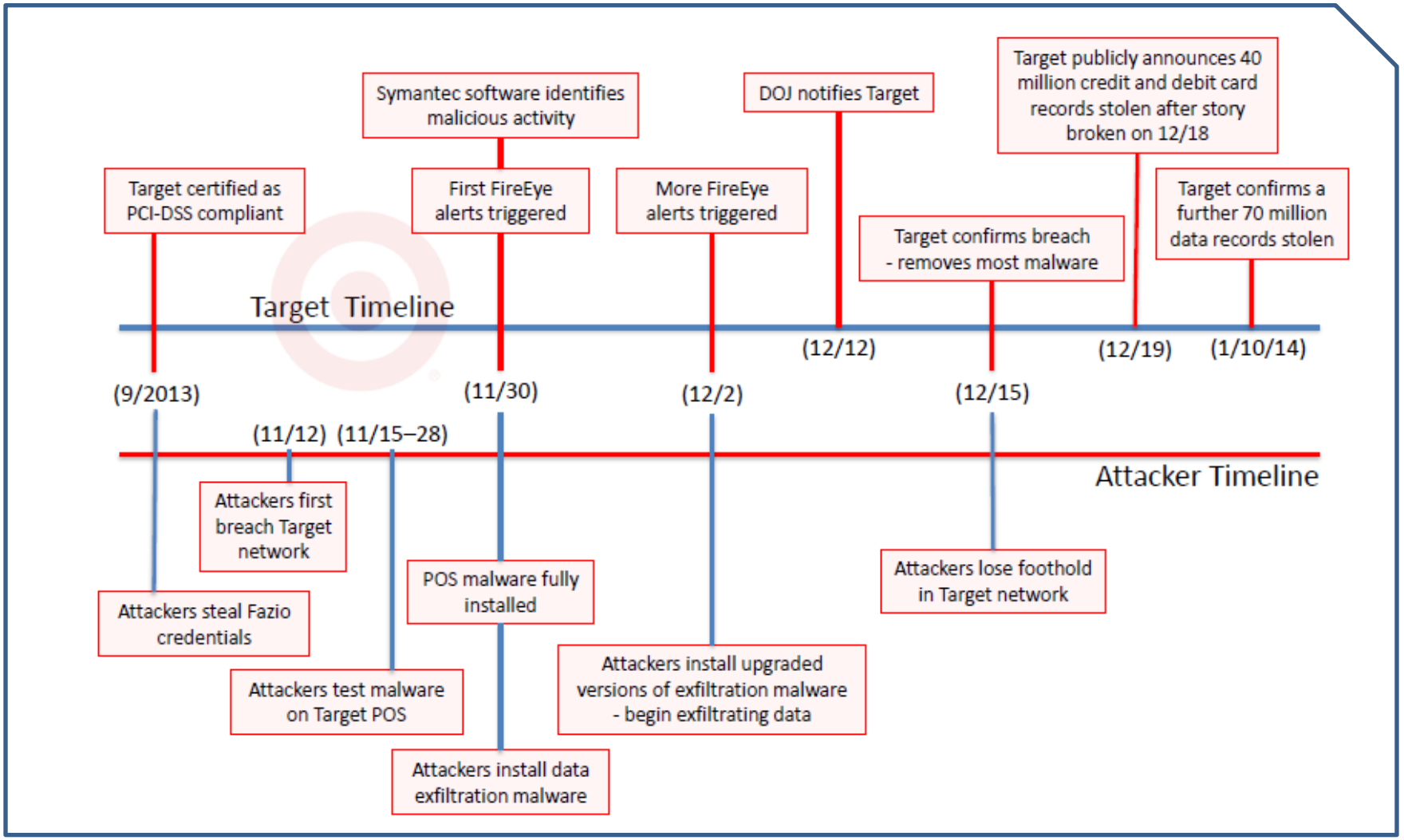
22

Target en detalle

Según fuentes no identificadas, los atacantes instalaron por primera vez sus programas malware en un **pequeño número de terminales** de punto de venta entre el 15 y 28 de noviembre. Una vez realizado este piloto se instalo el malware en **todos los terminales de punto de venta** (POS) el 30 de noviembre. Un informe de The New York Times afirma que los atacantes primero ganaron el acceso a la red interna de Target el 12 de noviembre

23

Target en detalle



24

Recomendaciones para crear Software Seguro

- Adoptar un modelo de madurez

- La seguridad debe ser considerada desde el inicio

- S-SDLC

Recomendaciones para crear Software Seguro

Elaboración de sistema de calidad de desarrollo del software.

- Establecer plazos y presupuestos para pruebas
- Establecer los pasos para las pruebas necesarias
- Puntuar a las empresas de desarrollo
- Revisión de seguridad del software

Recomendaciones para crear Software Seguro

CSX CYBERSECURITY NEXUS™

Separación de entornos

- Ya no solo desarrollo, pruebas y producción, sino por clasificación de información. Incluye separación física para ciertos niveles y desconexión total para otros.

27

Buenas Prácticas Des. Soft. Seguro

CYBERSECURITY NEXUS

- Clasificar los datos y las aplicaciones en función de su riesgo
- Desarrollar y mantener guías de cumplimiento
- Realizar formación en seguridad para los empleados dependiendo de su rol
- Elaborar modelos de amenaza
- Identificar patrones de seguridad en el diseño

28

Buenas Prácticas Des. Soft. Seguro

- Realizar revisiones de código
- Realizar pruebas de seguridad en las aplicaciones
- Establecer hitos para la revisión del diseño
- Crear procedimientos de gestión de cambio

29

Buenas Prácticas Des. Soft. Seguro

CYBERSECURITY NEXUS

Iniciativas de seguridad en el desarrollo de software:

- **Microsoft SDL**
- **OWASP CLASP**
- **Cigital Software Security Touchpoints**
- **OWASP OpenSAMM**
- **BSIMM**
- **SSE CMM**

30

COBIT 5

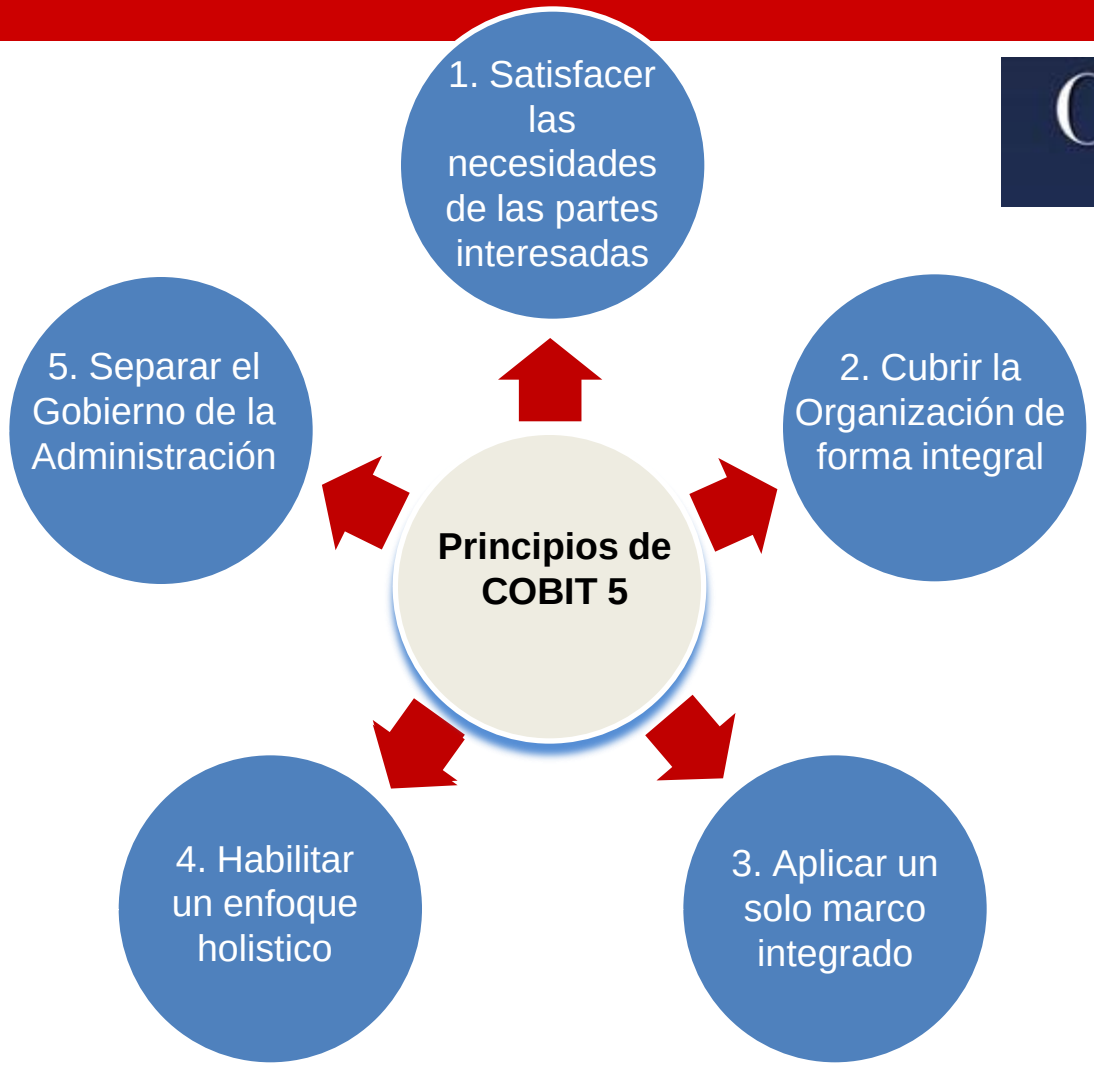
COBIT5 proporciona un **marco integral** que ayuda a las Organizaciones a **lograr su metas** y **entregar valor** mediante un gobierno y una administración efectivos de la TI de la Organización.

Metas corporativas

- Cumplimiento de leyes y regulaciones externas
- Programas gestionados de cambio en el negocio

31

COBIT 5



Fuente: COBIT® 5, © 2012 ISACA® Todos los derechos reservados.

COBIT 5

Metas relacionadas con TI

- Cumplimiento y soporte de las TI al cumplimiento del negocio de las leyes y regulaciones externas
    - Gestionar el Marco de Gestión de TI
    - Gestionar el Riesgo
    - Gestionar la Seguridad
    - Gestionar la Configuración
    - Gestionar los Servicios de Seguridad ...

33

COBIT 5

- Seguridad de la información, infraestructuras de procesamiento y aplicaciones
- Alineamiento de TI y la estrategia de negocio
- Compromiso de la dirección ejecutiva para tomar decisiones relacionadas con TI
- Entrega de Programas que proporcionen beneficios a tiempo, dentro del presupuesto y satisfaciendo los requisitos y normas de calidad

34

Más información

Jorge Edo Juan

Director de Cursos y Certificaciones

CISA, ITIL EXPERT, Auditor ISO 20.000, Lead Auditor ISO 27001, Prince2-P

Roberto Soriano

Presidente

CISA, CISM, CRISC, PMP, Lead Auditor ISO 27001, ITILv3, Prince2, CSX, COBIT

cursos@isacavalencia.org

csx@isacavalencia.org

asociados@isacavalencia.org

presidente@isacavalencia.org

ISACA Valencia Chapter

@ISACAValencia

https://www.facebook.com/isacavalencia

35

GRACIAS POR SU ATENCION

ISACA®
Sistemas de información fiables y valiosos
Valencia Chapter