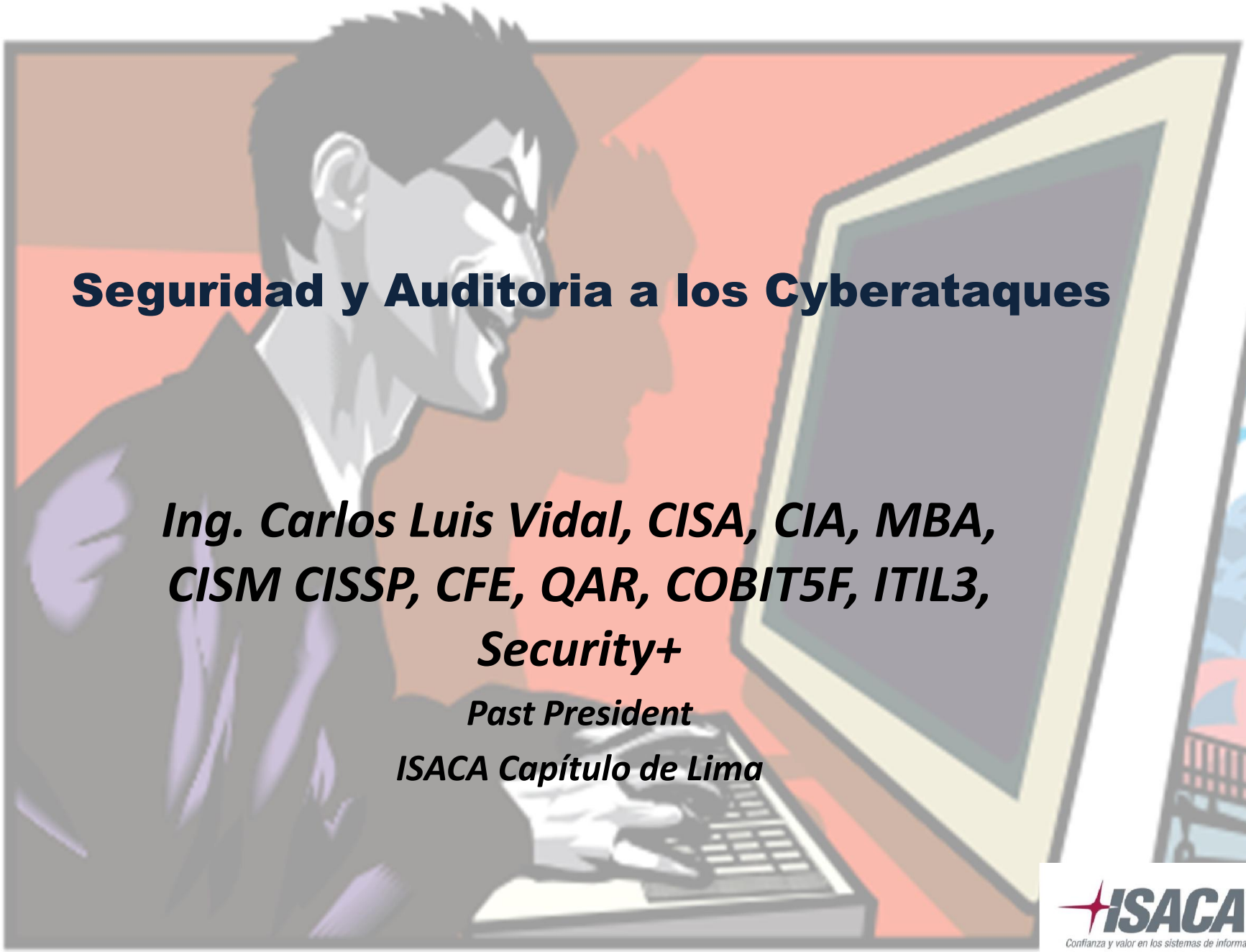


Seguridad y Auditoria a los Cyberataques

Ing. Carlos Luis Vidal, CISA, CIA, MBA, CISM CISSP, CFE, QAR, COBIT5F, ITIL3, Security+

Past President

ISACA Capítulo de Lima

ISACA®
Confianza y valor en los sistemas de información
Lima Chapter

ACERCA DE ISACA

- Asociación internación profesional sin fines de lucro.
- Posee más de 40 años de fundación y es reconocida a nivel internacional y local.
- **Una Oficina Central en Ilinois, USA**
- **205 Capítulos en 86 Países**
- Miembros que en su mayoría son:
  - *Profesionales en Auditoría de TI*
  - *Profesionales Seguridad de Información*
  - *Profesionales en Riesgos y cumplimiento*
  - *Profesionales en Gerencia y Gobierno de TI*

ACERCA DE ISACA LIMA

ISACA
Confianza y valor en los sistemas de información
Lima Chapter

- Asociación profesional sin fines de lucro.
- Es el capítulo local y oficial de ISACA Internacional en el Perú.
- Fundado en 1997.
- En la actualidad cuenta con más de 570 miembros sus miembros son profesionales de auditoría, seguridad, control, gestión y gobierno de TI.

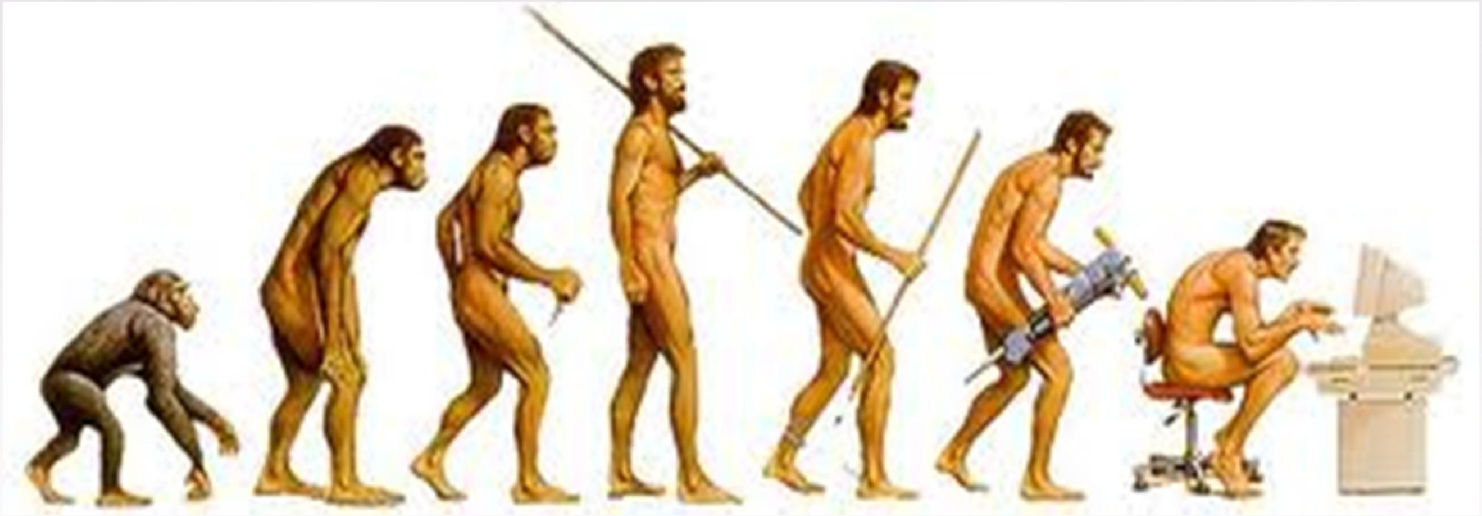
Agenda

1. EVOLUCIÓN DE CYBER ATAQUES
2. DEFINICION DE CLIENTE SIDE ATTACK(Cyber ataques del lado del cliente)
3. ¿POR QUE ES EXITOSO UN CLIENT SIDE ATTACKS
4. RECOMENDACIONES A:
   a) GERENCIAS DE TI(CIO's)
   b) SEGURIDAD DE SISTEMAS DE INFORMACIÓN
   c) AUDITORIA DE SISTEMAS DE INFORMACIÓN

ISACA®
Confianza y valor en los sistemas de información
Lima Chapter

INTRODUCCION

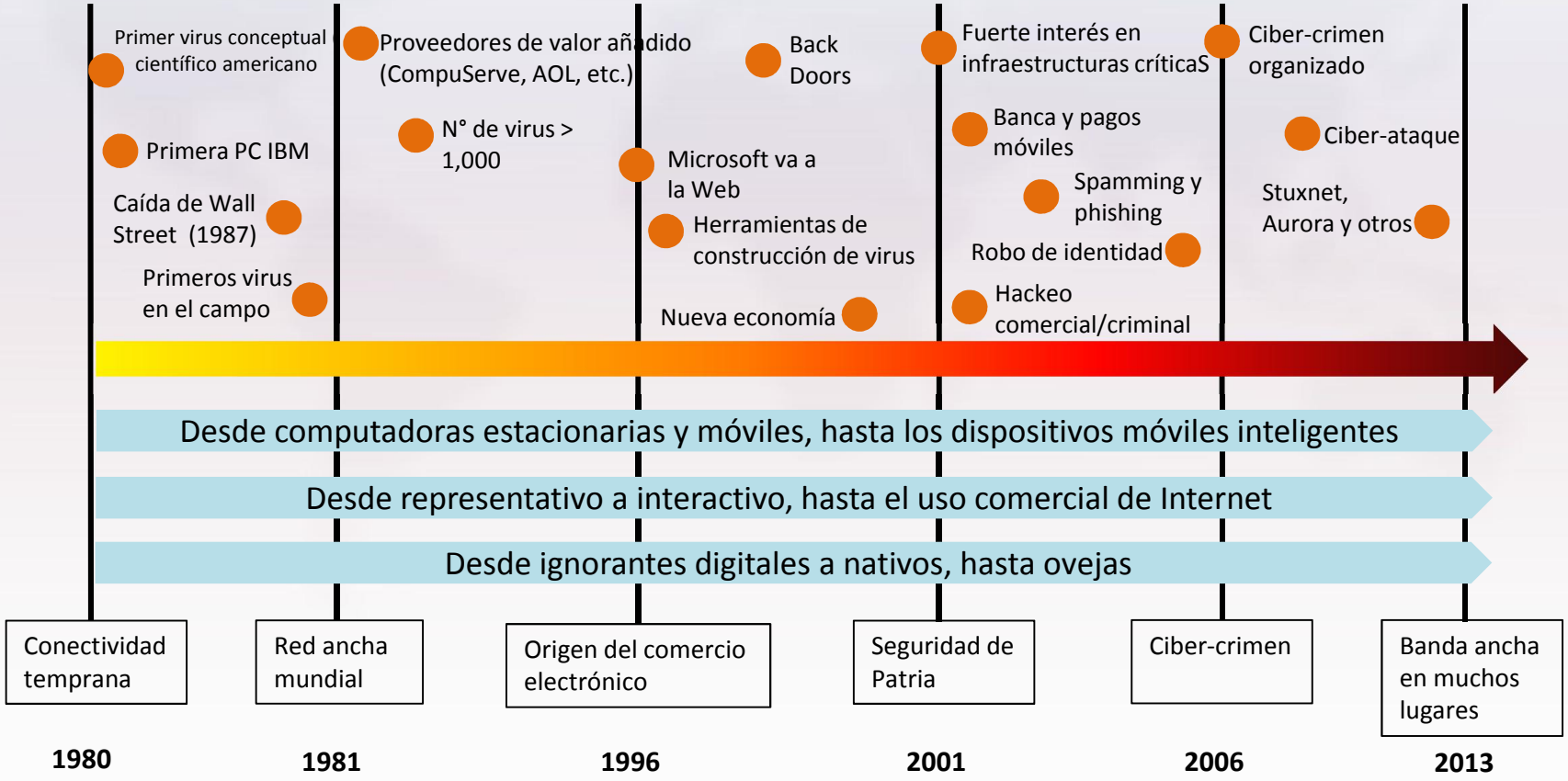
EVOLUCION DE LOS ATAQUES



ISACA®
Confianza y valor en los sistemas de información
Lima Chapter

INTRODUCCION

¿DONDE ESTAMOS EN LINEA DE TIEMPO DE CIBERATAQUE?

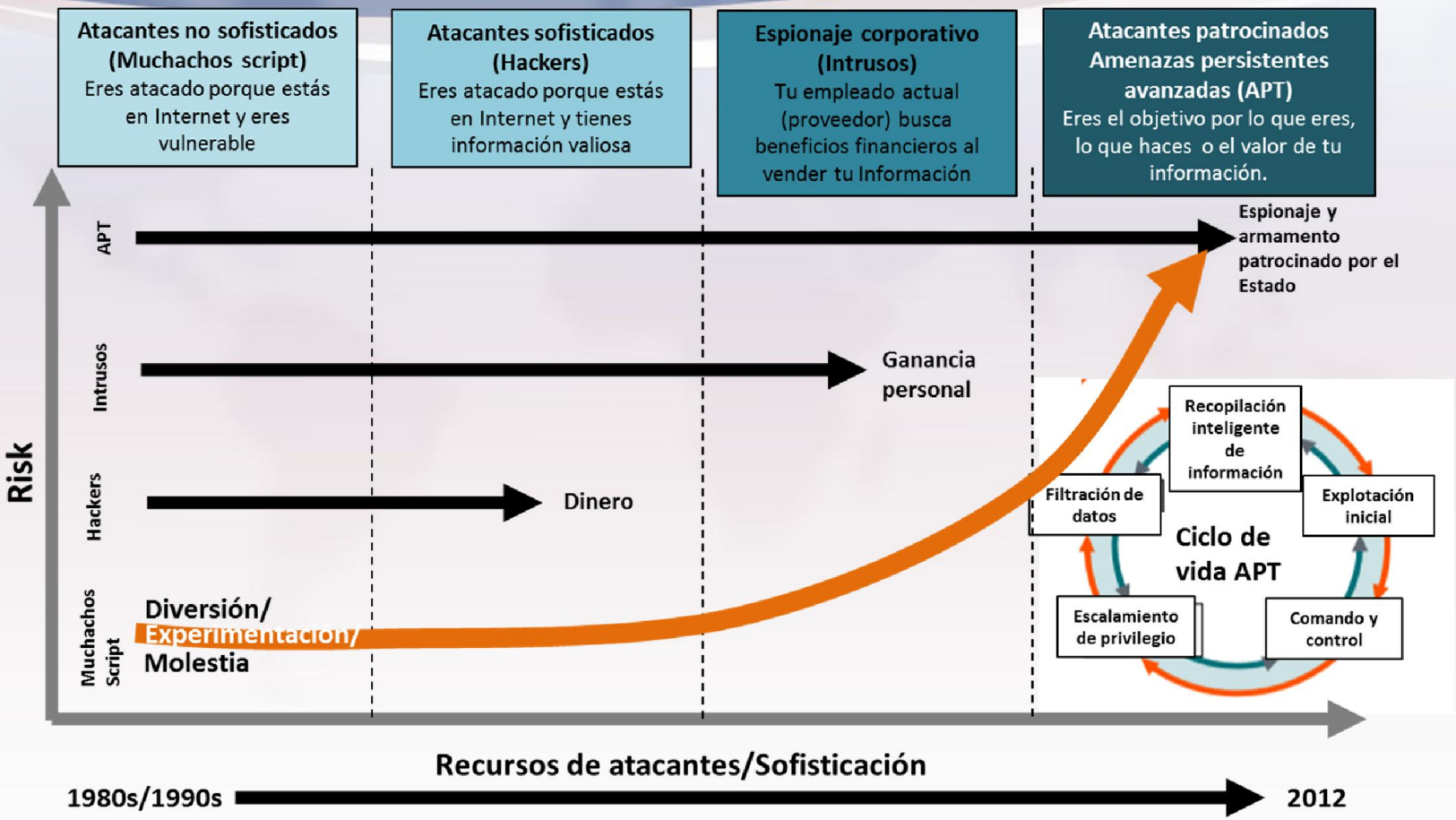


Fuente: Transformando la Ciberseguridad usando COBIT 5- ISACA HQ- 2014

ISACA® Confianza y valor en los sistemas de información Lima Chapter

INTRODUCCION

Evolución del panorama de amenazas



- Morris Worm
- Virus polimorfos
- MiguelAngel
- Concepto de macro virus
- Melissa
- "Te amo"
- Anna Kornikova
- Sircam
- Código rojo y Nimda
- MyDoom
- Netsky
- Sasser
- Storm bonet
- Koobface
- Conflicker
- Aurora
- Mariposa
- Stuxnet
- Wikileaks
- Anonymous
- LutzSec
- SpyEye/Zeus
- Duqu
- Flame

Fuente: Transformando la Ciberseguridad usando COBIT 5- ISACA HQ

ISACA®
Confianza y valor en los sistemas de información
Lima Chapter

Para tomar en cuenta

Retos Actuales en Seguridad de TI

- **62%** incremento en brechas de seguridad de TI durante el 2013.
- **1 de cada 5** organizaciones han sufrido un ataque avanzado de cómputo.
- 3 Trillones de $ es el impacto anual por Cibercrimen.
- **7 y ½ meses** es el tiempo que permanece en promedio una ataque avanzando de cómputo sin detectarse
- **2.5 Billones** registros han sido expuestos debido alguna brecha en los últimos 5 años.

Fuente: Internet Security Theat Report 2014.

¿Qué es una APT?

- Las amenazas persistentes avanzadas son fenómenos relativamente nuevos para muchas organizaciones.
- Un APT es una amenaza que es avanzada y persistente. Es ataque con un objetivo específico que busca mantenerse en la victima.

CASO AURORA

- *Se le considera como uno de los ciberataques más sofisticados, pues se trata de un robo detalladamente planeado y muy bien dirigido hacía Google y otras más de 30 empresas para robar información usando un malware.*
- *Se trató de sabotaje corporativo*

HAZ CLICK AQUÍ
PARA ACCEDER

ISACA®
Confianza y valor en los sistemas de información
Lima Chapter

Noticias

Europe News

ECB hacked: Data stolen from central bank

Matt Clinch | @mattclinch81
Thursday, 24 Jul 2014 | 5:25 AM EDCNBC.com
SHARES

Email addresses and other contact information stored at the European Central Bank (ECB) have been stolen, the organization confirmed on Thursday.

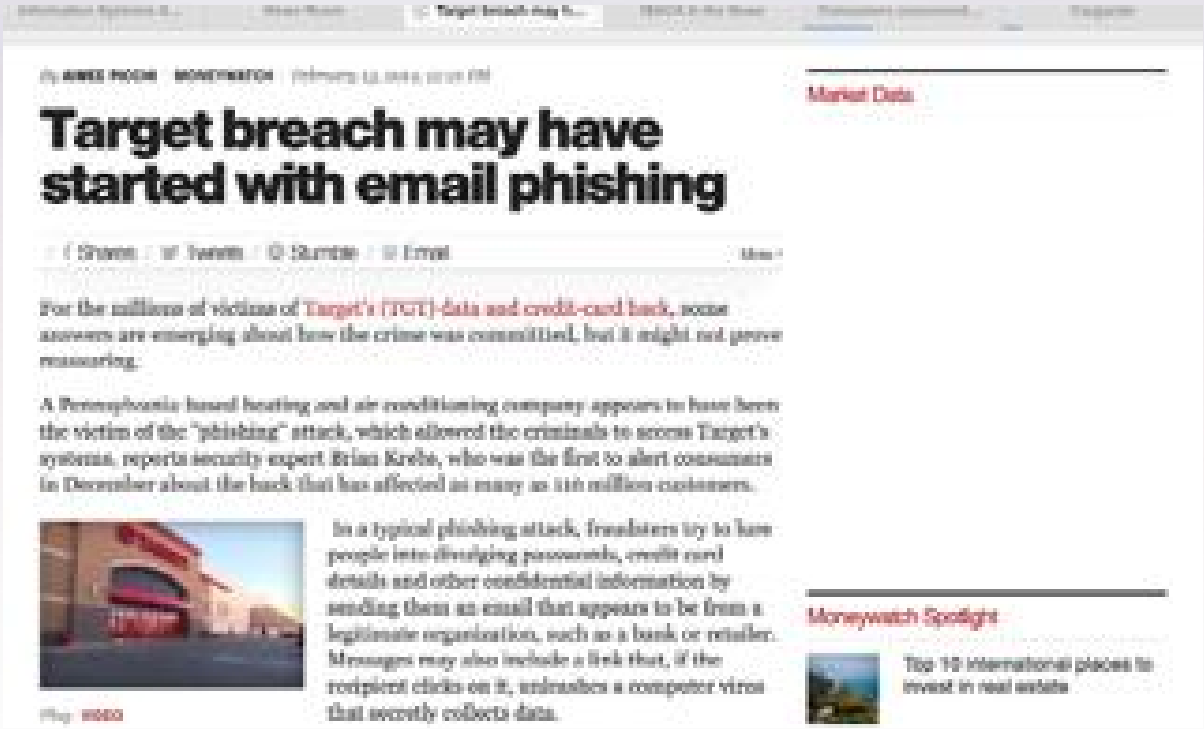
Security that protects a database serving its public website has been breached, it said in a statement published on its website, meaning users registering for information on conferences and visits at the ECB have been compromised.

Read MoreEuro zone business activity rebounds, France lags

It stated that no "internal systems or market-sensitive" information had been part of the data theft and was physically separate from the compromised data.

ISACA
Confianza y valor en los sistemas de información
Lima Chapter

Noticias



By JAMES PICOH · MONEYWATCH

Target breach may have started with email phishing

For the millions of victims of Target's (TGT) data and credit-card hack, some answers are emerging about how the crime was committed, but it might not prove reassuring.

A Pennsylvania-based heating and air conditioning company appears to have been the victim of the "phishing" attack, which allowed the criminals to access Target's systems, reports security expert Brian Krebs, who was the first to alert consumers in December about the hack that has affected as many as 110 million customers.

In a typical phishing attack, fraudsters try to have people into divulging passwords, credit card details and other confidential information by sending them an email that appears to be from a legitimate organization, such as a bank or retailer. Messages may also include a link that, if the recipient clicks on it, unleashes a computer virus that secretly collects data.

Market Data

Moneywatch Spotlight

Top 10 international places to invest in real estate

ISACA®
Confianza y valor en los sistemas de información
Lima Chapter

Introducción- Premisa

La ciberseguridad es un área en constatante cambio y crecimiento.

Es crucial que los conceptos centrales que enmarcan y definen esta área sean entendidos por los profesionales que están involucrados con las implicaciones de seguridad.

ATAQUES DE LADO CLIENTE

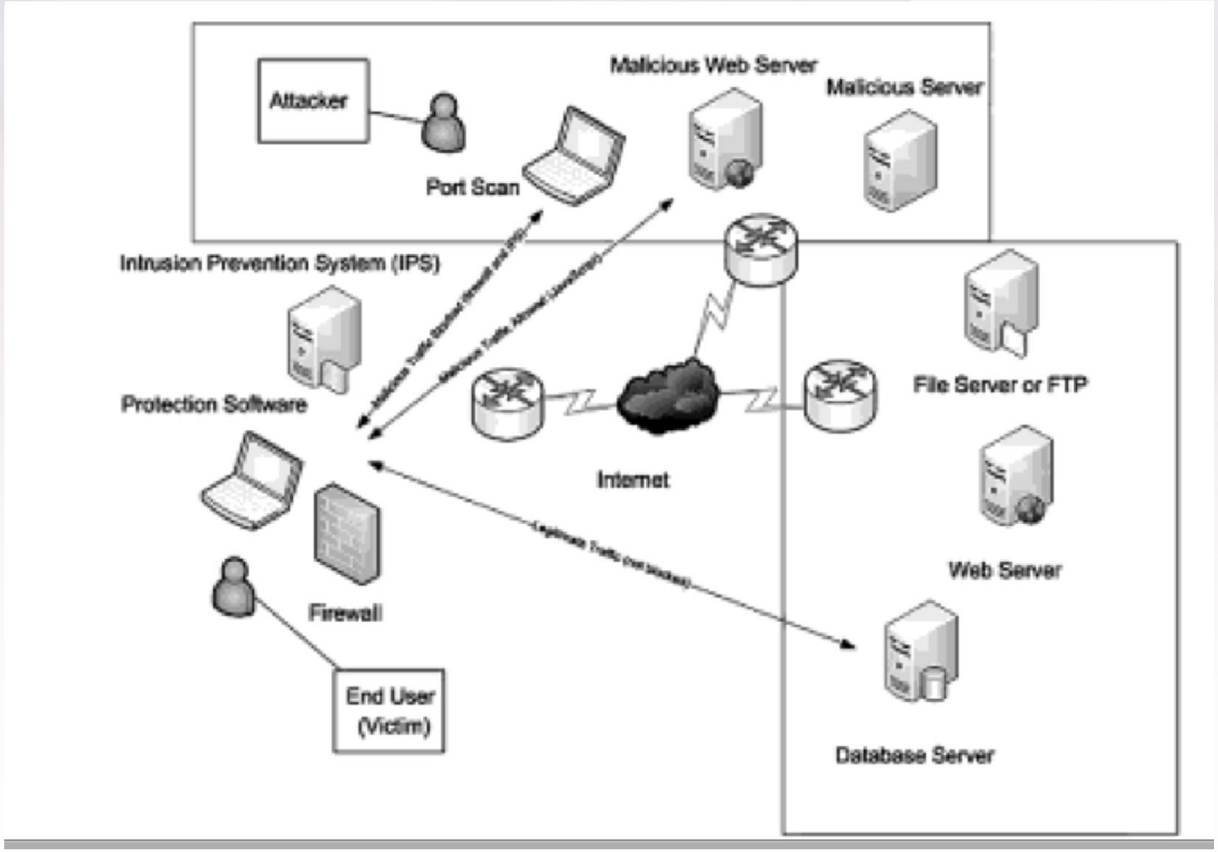
- Antes: Server Side Attack

  Router, Servidor Web, Servidor Base de Datos, Servidores Aplicaciones y similares.

Fuente: Client Side Atacks, 2012

ATAQUES DE LADO CLIENTE

Ahora también: Cliente Side Attack



Fuente: Client Side Attacks, 2012

ATAQUES DE LADO CLIENTE

Navegadores, Lectores PDF, Aplicaciones Ofimáticas, entre otras.

Fuente: Client Side Attacks, 2012

ATAQUES DE LADO CLIENTE

Tipos de Client Side Attack

i) CSA asociados a una vulnerabilidad técnica

ATAQUES DE LADO CLIENTE

Tipos de Client Side Attack

ii) CSA que utilizan también la ingeniería social

ATAQUES DE LADO CLIENTE

¿Que será mejor tener cualquier cuenta de usuario o la de los administradores y altos funcionarios de los sistemas de una empresa?

ATAQUES DE LADO CLIENTE

¿En este tipo de ataque sólo se aprovechan de temas técnicos?

NO, Sino además los atacantes buscan la motivación de las personas que quieren atacar, así como su falta de concientización en seguridad de información.

ATAQUES DE LADO CLIENTE

Vulnerabilidad

Es la debilidad de un sistema que permite que un atacante logre concretar sus ataque.

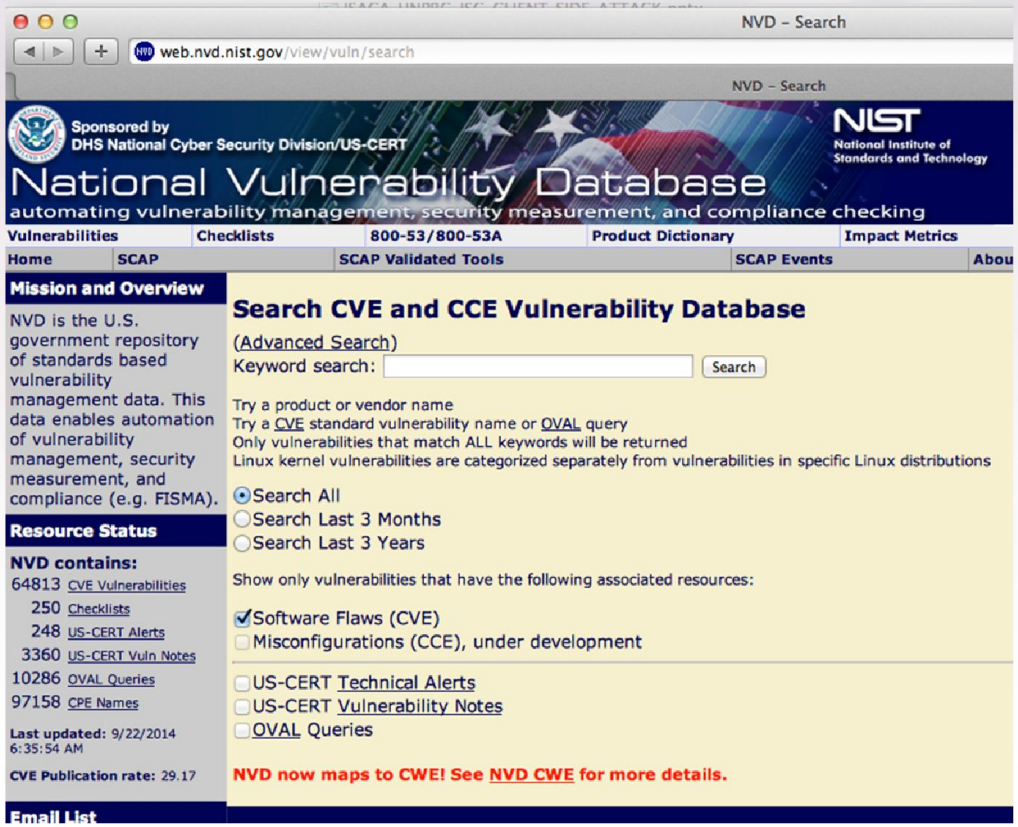
P.E: Tener instalado sistemas con fallas de seguridad, no tener o tener un antivirus desactualizado, otros

Vulnerabilidades

Busqueda de vulnerabilidades

Base de Vulnerabilidades:

http://web.nvd.nist.gov/view/vuln/search



ISACA
Confianza y valor en los sistemas de información
Lima Chapter

Exploits

Búsqueda de vulnerabilidades y exploits

Base de Exploits On-Line:

http://www.exploit-db.com

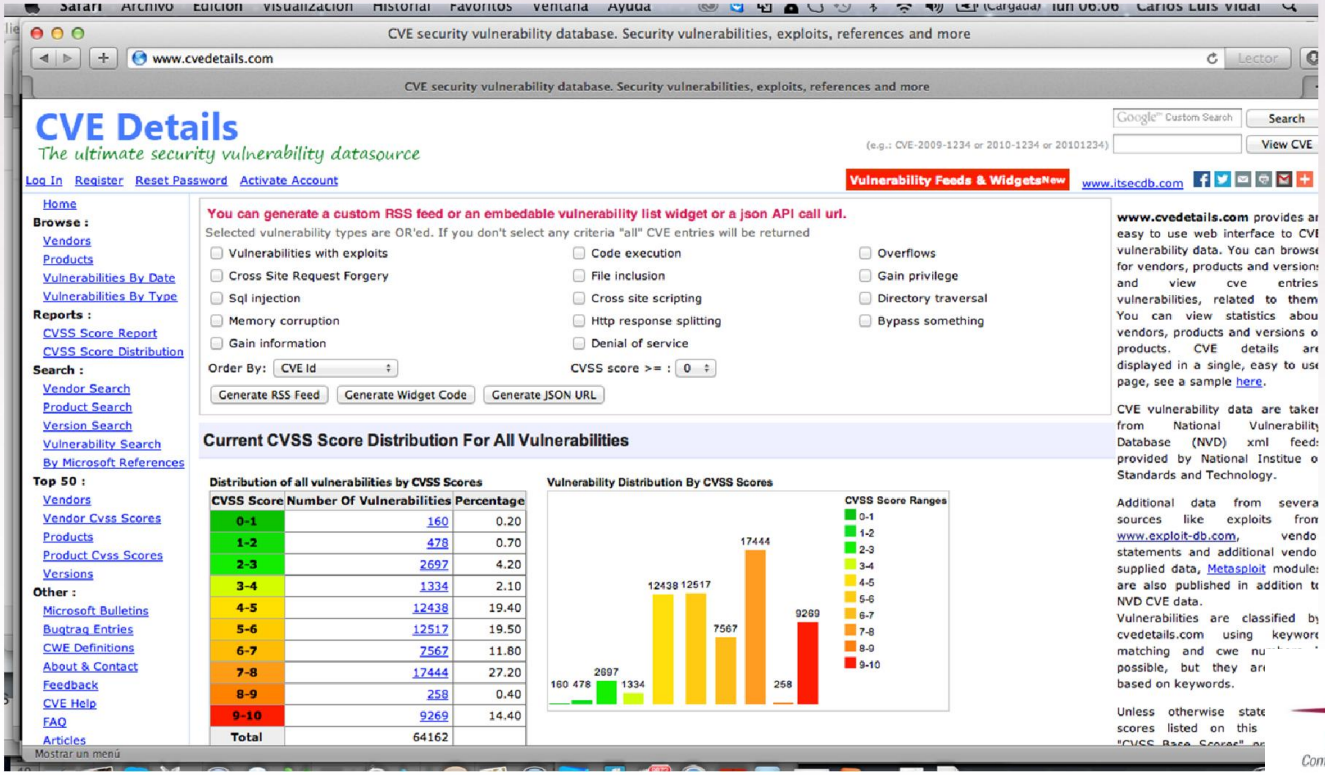
ISACA
Confianza y valor en los sistemas de información
Lima Chapter

ATAQUES DE LADO CLIENTE

Búsqueda de vulnerabilidades y exploits

Base de Exploits On-Line:

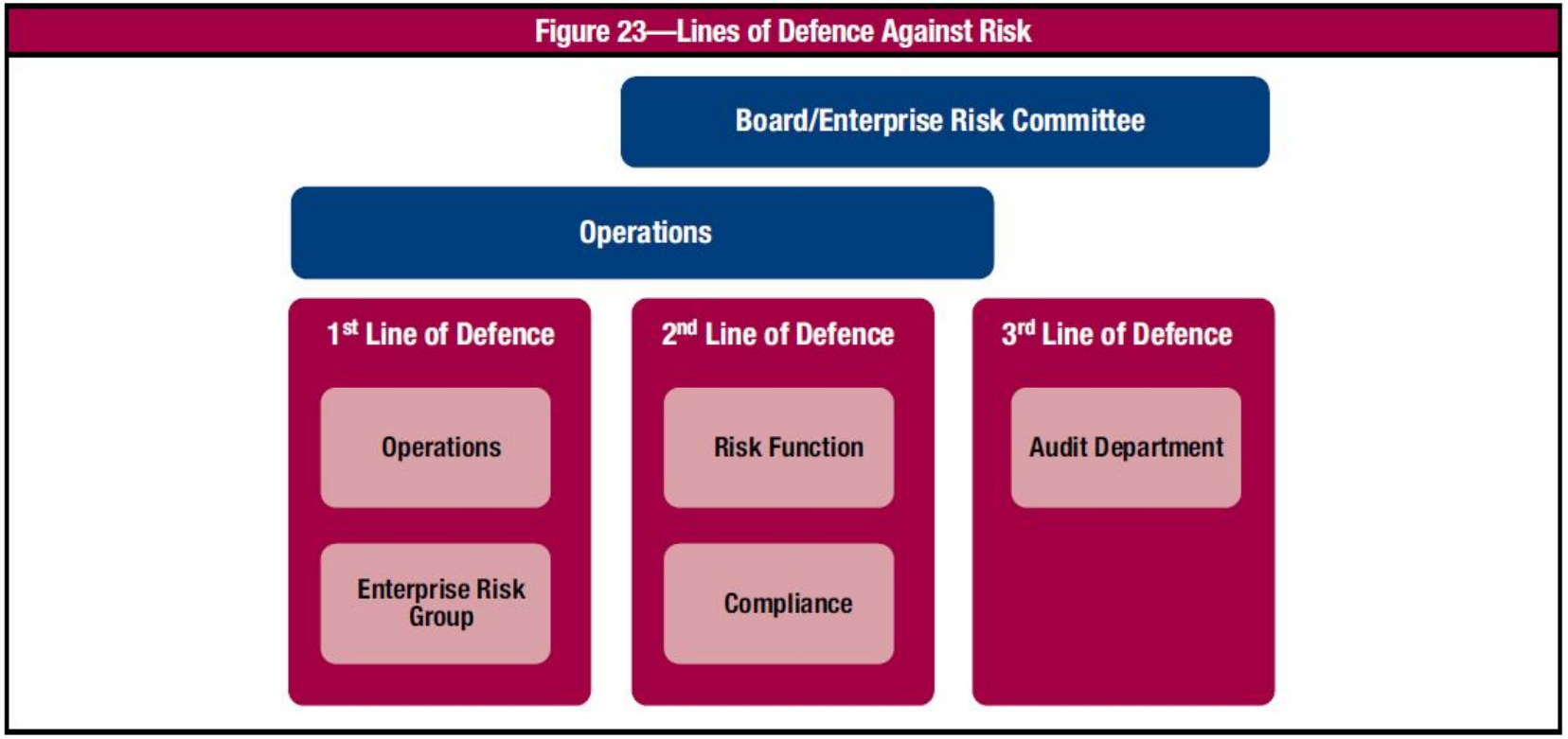
http://www.cvedetails.com



ISACA®
Confianza y valor en los sistemas de información
Lima Chapter

RECOMENDACIONES Y CONCLUSIONES- CSA

Primero tomar es importante tomar en cuenta:



ISACA
Confianza y valor en los sistemas de información
Lima Chapter

RECOMENDACIONES Y CONCLUSIONES- CSA

CIOS(Gerentes de Sistemas y Tecnologías de información

- Actualizar y ejecutar un programa antivirus y un programa anti spyware.
- Actualizar el sistema operativo y los navegadores web de forma regular.
- Actualizar (por ejemplo: Flash, Quicktime), lectores (por ejemplo. Acrobat), y complementos con regularidad.
- Tener cuidado con sitios web sospechosos (por ejemplo. Sitios que ofrecen videos gratuitos y torrent)
- No navegar por la web y abrir correos utilizando la cuenta de administrador(cuenta con altos privilegios).

ISACA®
Confianza y valor en los sistemas de información
Lima Chapter

RECOMENDACIONES Y CONCLUSIONES- CSA

CISO(Oficiales de Seguridad de Información)

- Definir lineamientos en la política de seguridad de información que establezca la responsabilidad de actualización de los agentes de antivirus, anti malware, sistemas operativos, base de datos y aplicaciones clientes
- Monitoreo de la consola de antivirus tanto en los servidores, estaciones de trabajo y en la actualidad incluso dispositivos móviles.
- Verificar la actualización:
  - Sistemas operativos(servirdores y estaciones)/ BD's
  - Aplicaciones cliente(navegadores, ofimaticas, reproductores de audio, lectores pdf, etc.)
- Verificar que no exista trafico a sitios web sospechosos (por ejemplo. Sitios que ofrecen videos gratuitos y torrent)
- Verificar el uso de las cuentas privilegiadas
- Realizar análisis de vulnerabilidades en servidores y estaciones de trabajo

RECOMENDACIONES Y CONCLUSIONES- CSA

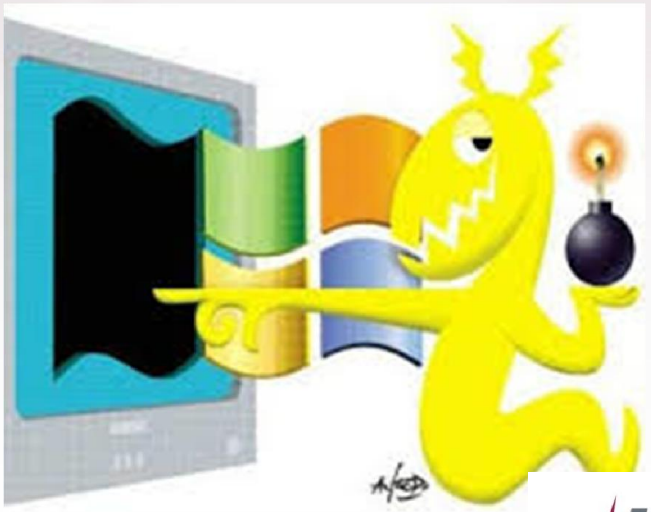
Auditor de Sistemas

- Revisar la existencia y suficiencia de lineamientos en la política de seguridad relacionadas a controlar los cyber ataques tales como la actualización de la infraestructura tecnologíca y antivirus/antimalware.
- Verificar el cumplimiento de los lineamientos definidos en la política(incluso a pesar que no se hayan definido), sino igual revisar que se realice la actualización tanto en servidores , estaciones de trabajo(pcs') y MOBILES de: agentes de anti virus/malware, S.O, BD, aplicaciones finales, navegadores.
- Revisar que se hayan implementado controles de web content (por ejemplo. Sitios que ofrecen videos gratuitos y torrent)
- Verificar los controles en la cuenta de administrador(cuentas con altos privilegios).
- Solicitar el sustento de las charlas de concientización/educación tanto a personal de TI como a usuarios finales, clientes, partners.

RECOMENDACIONES Y CONCLUSIONES

Pero NO OLVIDAR:

CONCIENTIZAR A TODOS LOS USUARIOS Y CLIENTES



ISACA®
Confianza y valor en los sistemas de información
Lima Chapter

MAYOR INFORMACION

http://www.isaca.org/cyber/Pages/default.aspx
(Como implementar la ciberseguridad en la organizacione)

http://www.offensive-security.com/community-projects/kali-linux/
(Descarga de Kali)

http://www.exploit-db.com
(Base de datos de exploits)

http://www.cvedetails.com
(Base de datos de vulnerablidades)

http://web.nvd.nist.gov/view/vuln/search
(Base de datos de vulnerablidades)

ISACA®
Confianza y valor en los sistemas de información
Lima Chapter

PREGUNTAS

ISACA®
Confianza y valor en los sistemas de información
Lima Chapter

ISG PUCP

Conferencias: QAR en AI, Seguridad Web, INFOSOFT 2012, 2013, 2014

Muchas Gracias!!!

Ing. Carlos Luis Vidal, CISA, CIA, MBA, CISM CISSP, CFE, QAR, COBIT5F, ITIL3, Security+
Past President- ISACA Lima
cluis@pucp.edu.pe
celv_83@hotmail.com
cluis@isaca.org.pe

(ISACA LIMA)
E-mail informacion@isaca.org.pe
Facebook: ISACALima
Web: www.isaca.org.pe

(ISACA Internacional)
www.isaca.org

ISACA
Confianza y valor en los sistemas de información
Lima Chapter

Proxima conferencia de ISACA Lima

"Infraestructuras Críticas y Sistemas de Control Industrial - Cómo clasificarlos y protegerlos «

Objetivos:

- **Conocer cuál es la clasificación del DHS (Departamento de Seguridad Interior) para las diferentes infraestructuras críticas**
- **Distinguir las diferencias de la información entre TICs y SCIs**
- **Conocer los servicios de un CSIRT de ICS versus uno de ICT.**

DIRIGIDO A:

CIOS - Gerentes de TI / Sistemas
Auditores Internos y de TI
Oficiales de Gobierno de TI
Oficiales de cumplimiento
Consultores en seguridad de TI

FE**CHA: Martes 20 de octubre de 2015**

LUGAR: Hotel José Antonio - Sala Larco Piso 9 Av. 28 de Julio 398 - Miraflores

Asociados a ISACA : Sin costo*
No Asociados a ISACA : S/.170.00 (Incluye IGV)

Inscripción al: informacion@isaca.org.pe

ISACA®
Confianza y valor en los sistemas de información
Lima Chapter