



# Curso de Ethical Hacking

---

Alan J. Baeza Meza

Bienvenida y panorama general

---

# Introducción y bienvenida

---

# Alan J. Baeza Meza

- Director de Ciberseguridad en el sector público.
- Profesor de asignatura en la Universidad Autónoma de Baja California Sur.

---

# Temario

- Panorama general
- Introducción al Ethical Hacking
- Pentesting
- Estándares y aspectos legales
- Casos típicos de ataques
- Controles y mecanismos de seguridad.

“

El único sistema totalmente seguro es aquel que está apagado, desconectado, guardado en una caja fuerte de titanio, encerrado en un bunker de concreto, rodeado de gas venenoso y cuidado por guardas muy bien armados y pagados. Aun así, no apostaría mi vida por él

”

*Profesor Eugene Spafford*

Bienvenida y panorama general

---

# Conceptos básicos

Seguridad Informática

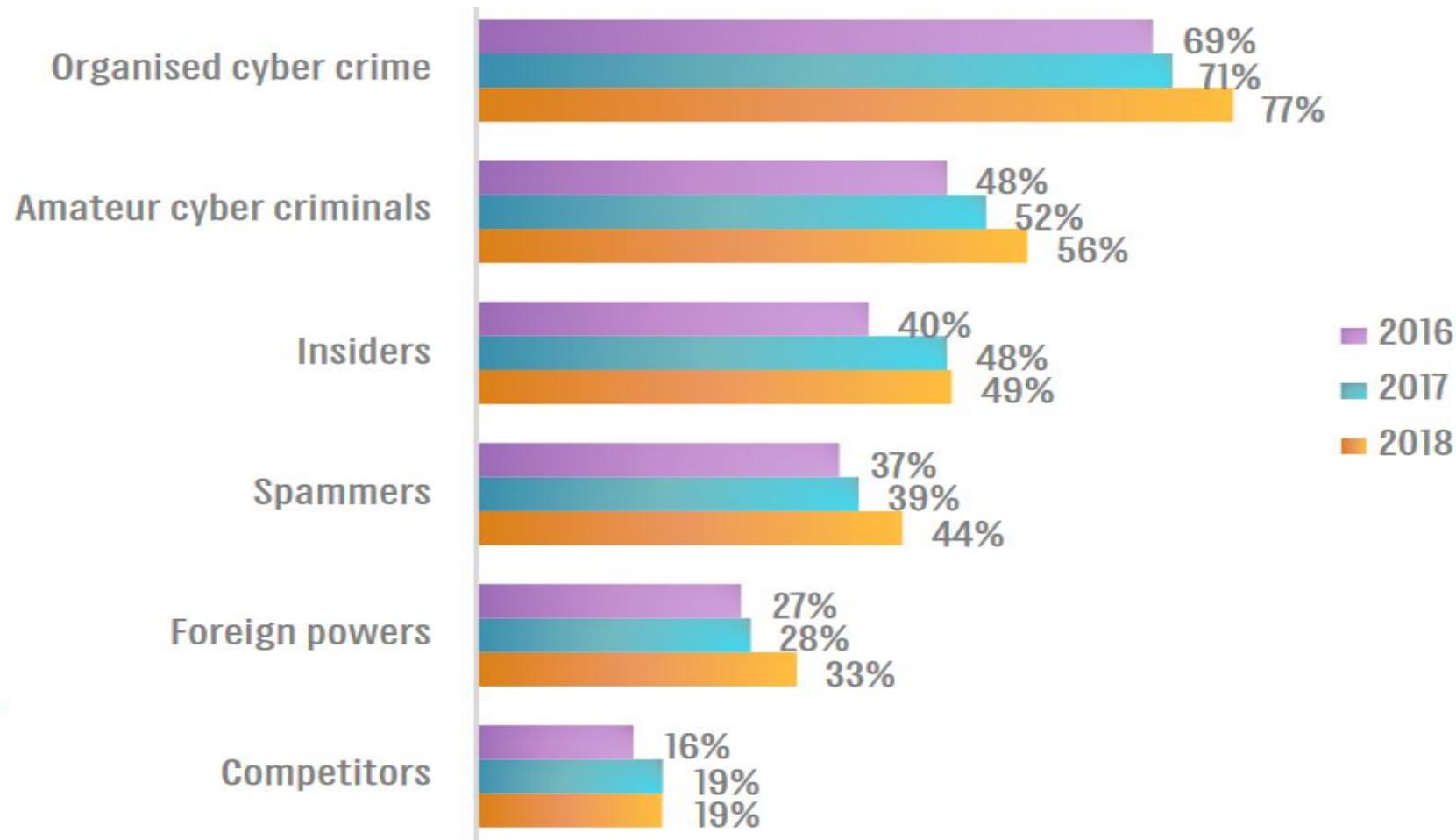
---

# Seguridad informática

Se encarga de proteger los activos de informáticos, entre los que se encuentran:

- Información.
- Infraestructura.
- Usuarios.

# CIO SURVEY



Fuente: Harvey Nash y KPMG, "CIO SURVEY"

# VERIZON “DBIR”

Fuente: Verizon DBIR  
“Data Breach  
Investigations Report”

## Top 20 action varieties in incidents

DoS (hacking)

21,409

Loss (error)

3,740

Phishing (social)

1,192

Misdelivery (error)

973

Ransomware (malware)

787

C2 (malware)

631

Use of stolen credentials (hacking)

424

RAM scraper (malware)

318

Privilege abuse (misuse)

233

Use of backdoor or C2 (hacking)

221

Backdoor (malware)

207

Theft (physical)

190

Pretexting (social)

170

# VERIZON “DBIR”

Fuente: Verizon DBIR  
“Data Breach  
Investigations Report”

## Top 20 action varieties in breaches

Use of stolen credentials (hacking)

399

RAM scraper (malware)

312

Phishing (social)

236

Privilege abuse (misuse)

201

Misdelivery (error)

187

Use of backdoor or C2 (hacking)

148

Theft (physical)

123

C2 (malware)

117

Backdoor (malware)

115

Pretexting (social)

114

Skimmer (physical)

109

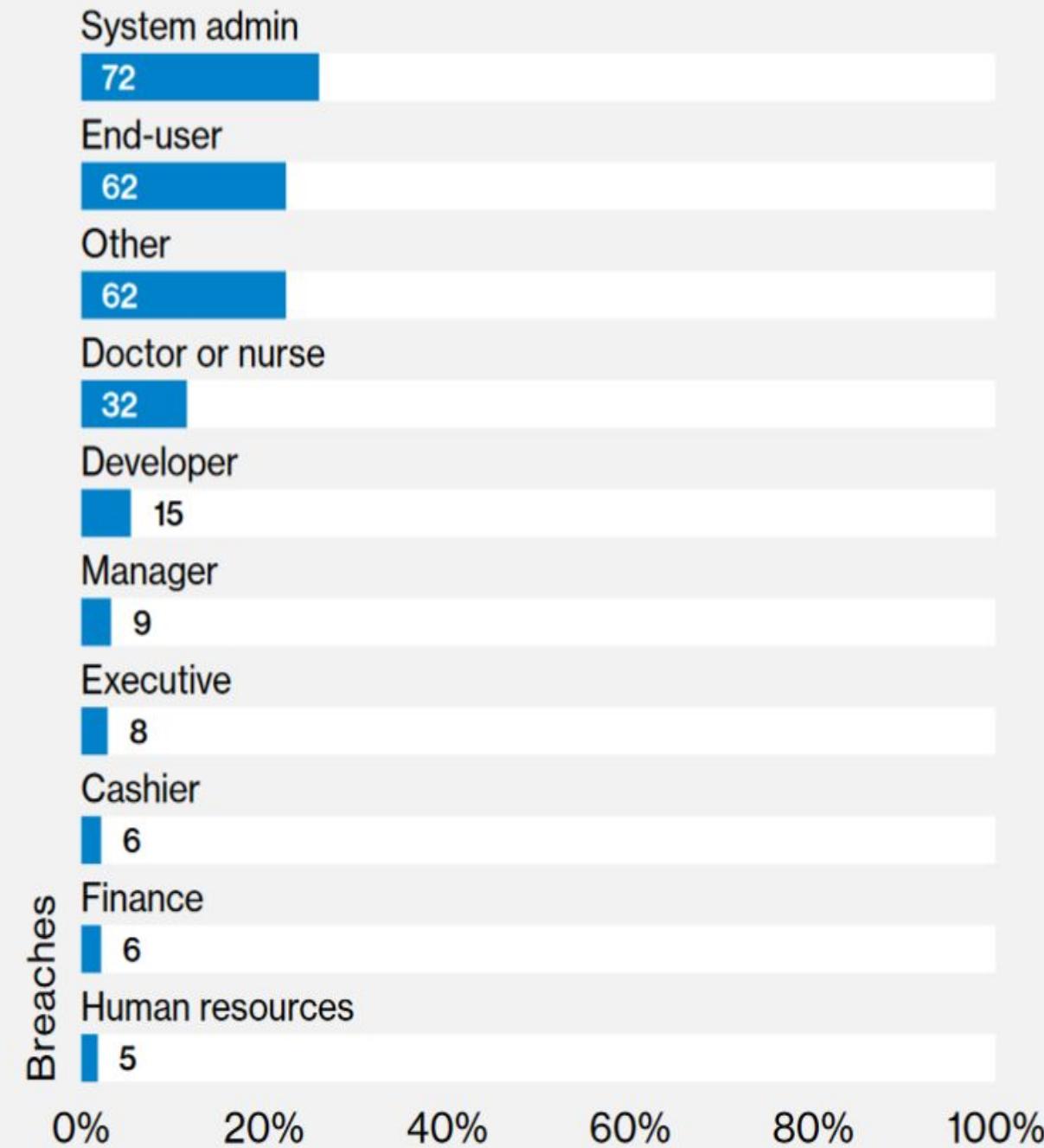
Brute force (hacking)

92

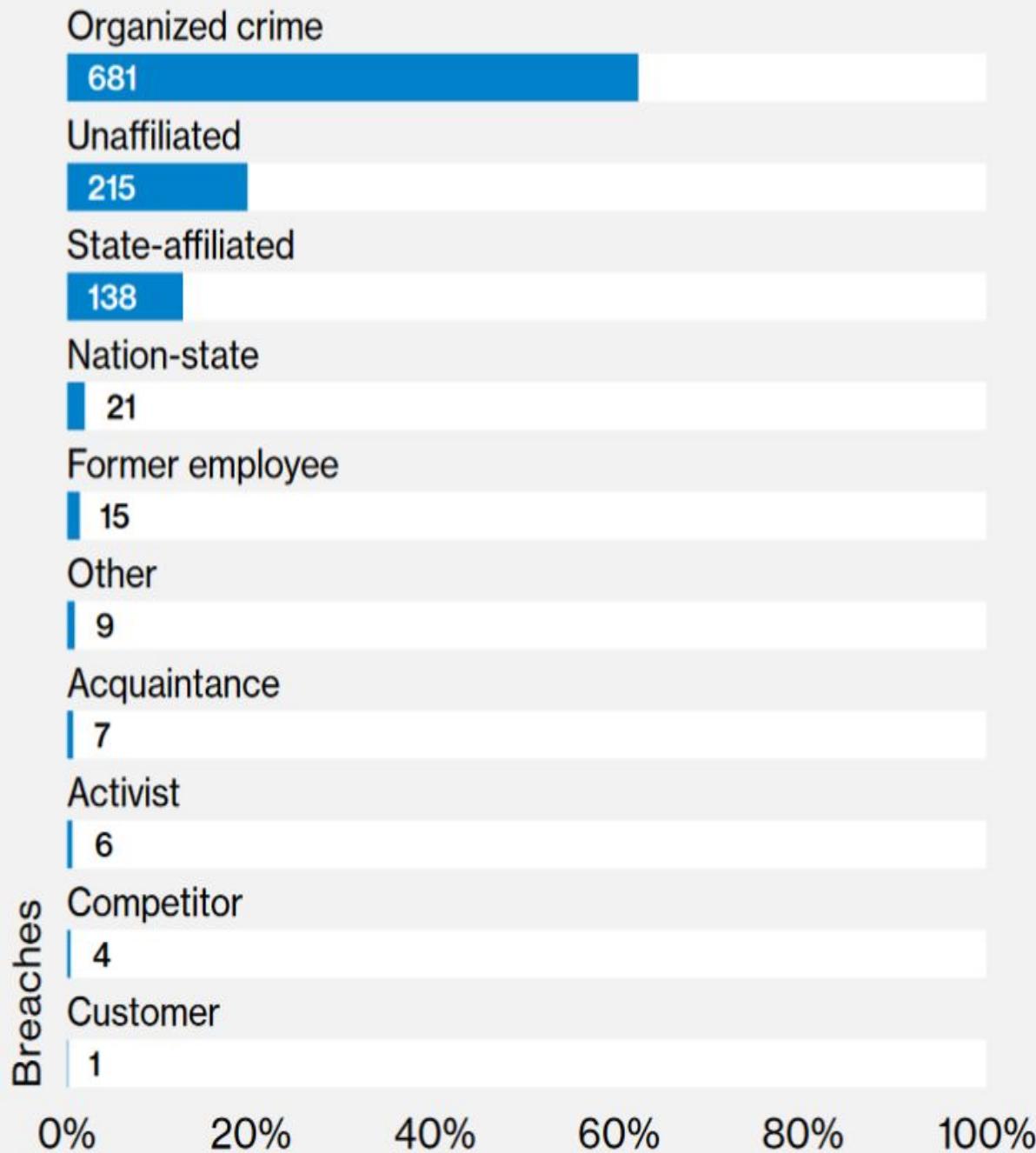
Spyware/keylogger (malware)

74

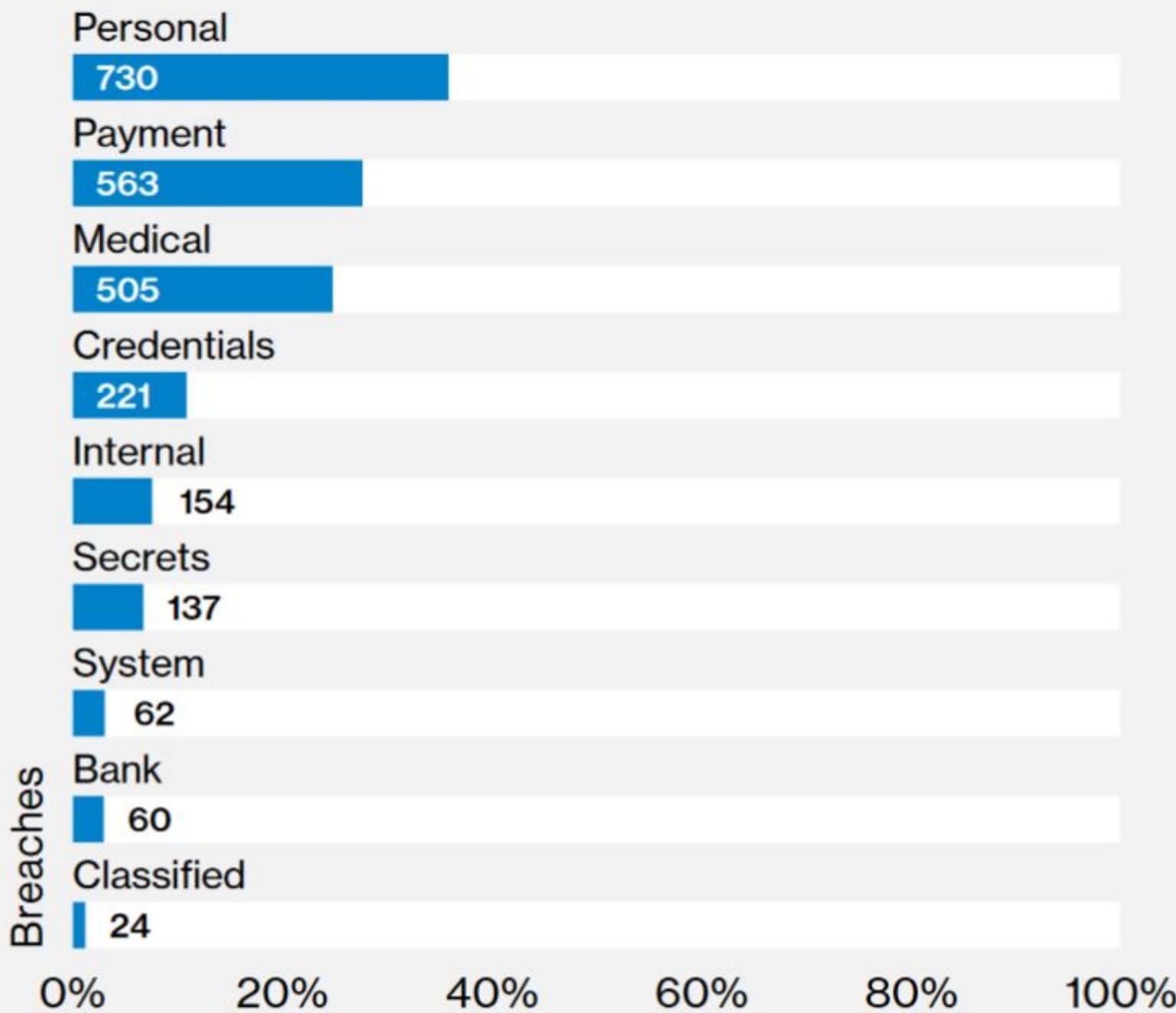
## Top internal actor varieties in breaches



## Top external actor varieties in breaches

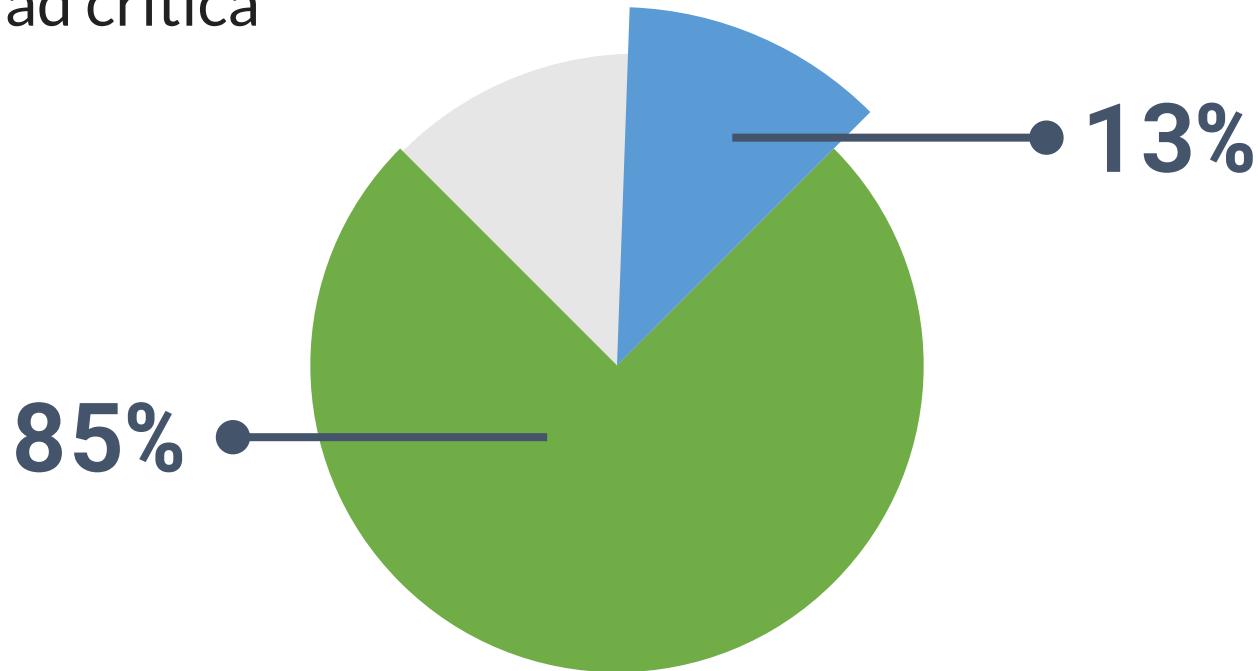


## Top data varieties compromised



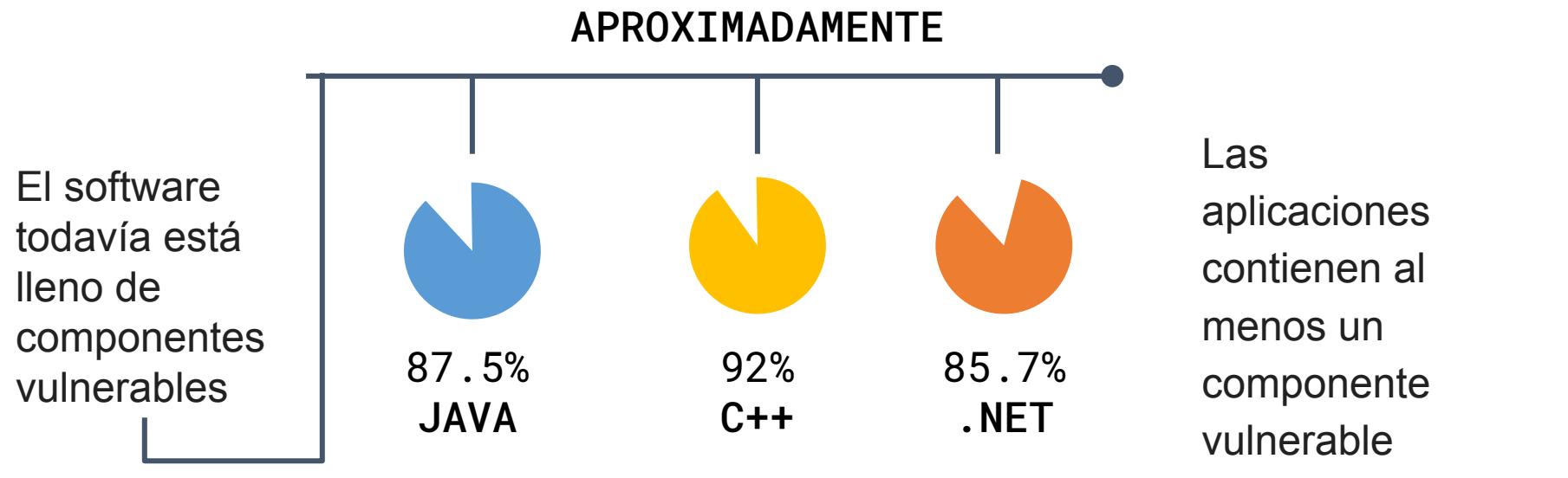
# VERACODE “Estado de seguridad del software”

Más del 85% de todas las aplicaciones tienen al menos una vulnerabilidad en ellas; más del 13% tiene al menos un defecto de gravedad crítica



Fuente: VERACODE “State of Software Security 2018

# VERACODE “Estado de seguridad del software



## LAS VULNERABILIDADES MÁS COMUNES QUE ESTÁN PRESENTADAS EN LAS SOLICITUDES PERMANECIERON A LO LARGO DEL MISMO

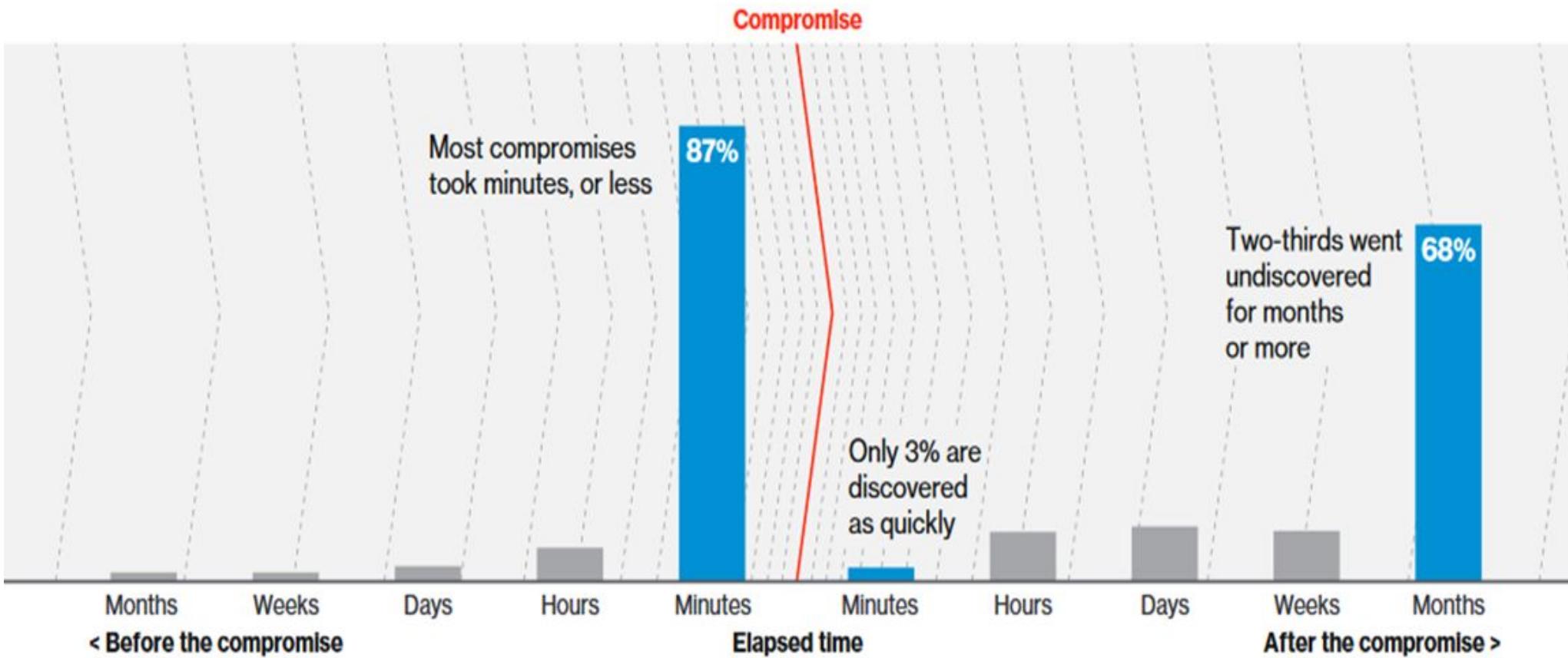


Las fallas de **SQL injection** todavía están presentes en casi una de cada tres aplicaciones



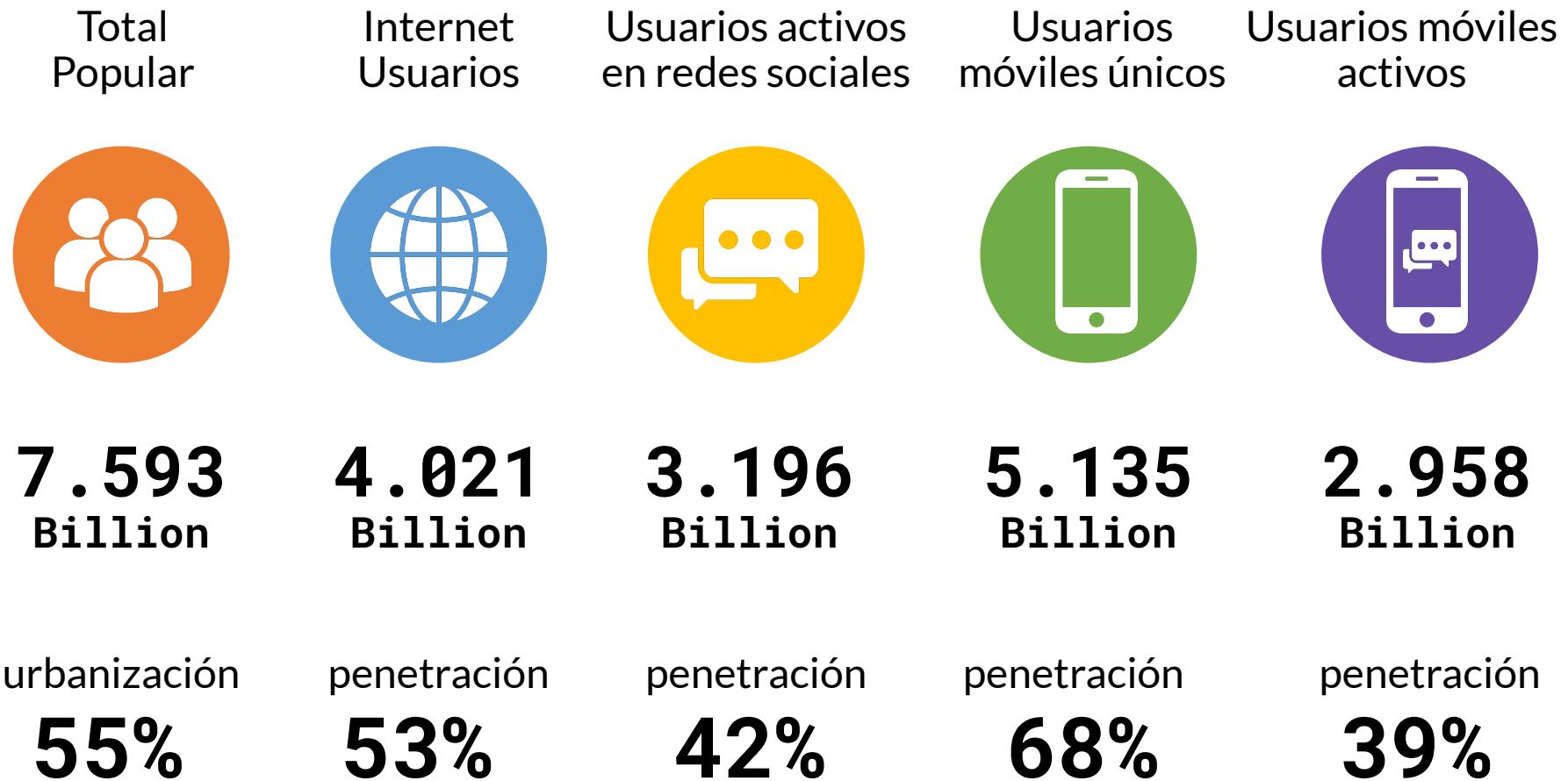
**Cross-Site Scripting (XSS) vulnerabilities** Se encuentran en casi el 50% de las aplicaciones.

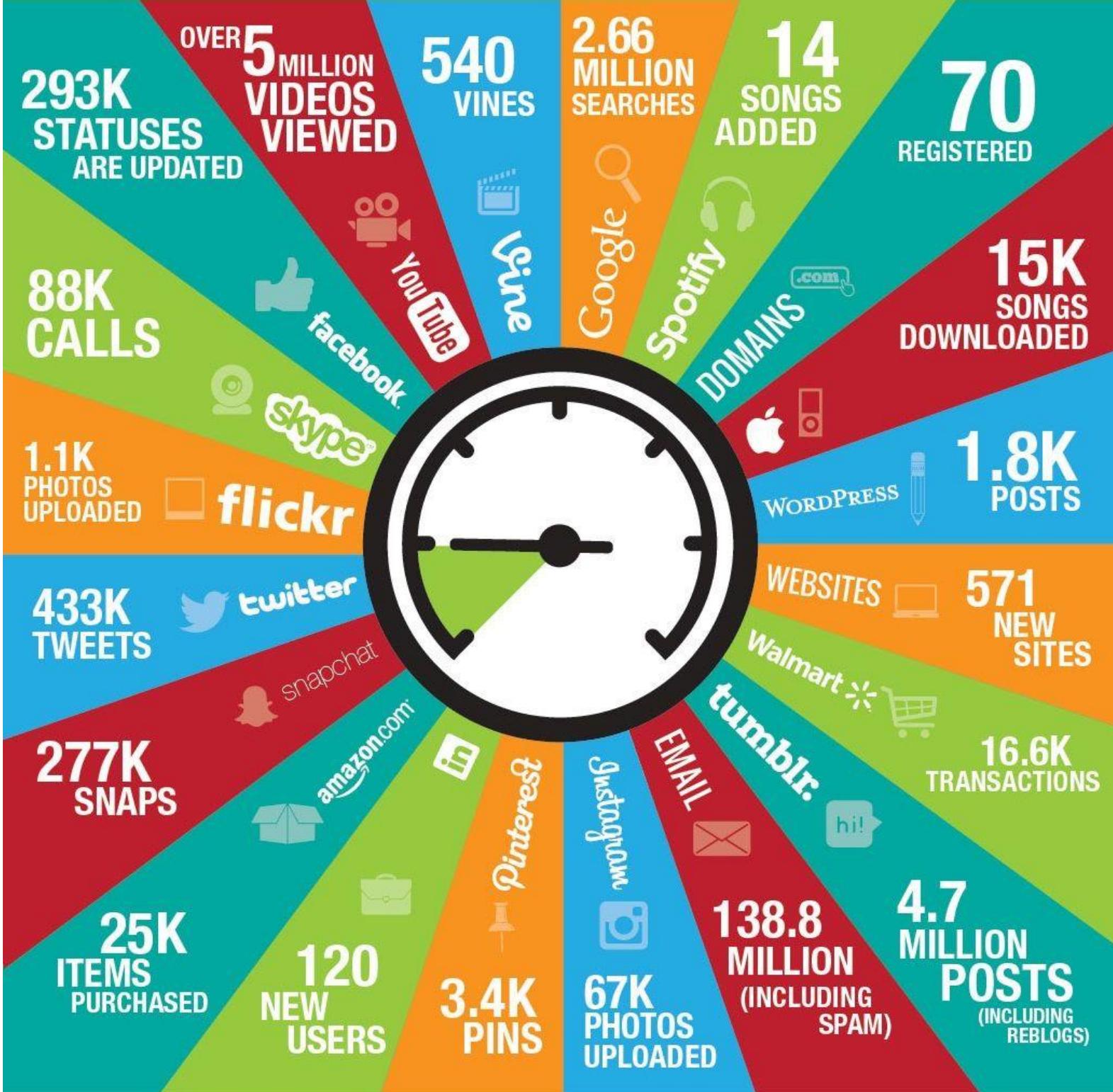
# It's time to act.



# Digital en todo el mundo

Indicadores estadísticos clave para los usuarios de Internet, dispositivos móviles y redes sociales del mundo.





---

# Seguridad de la información

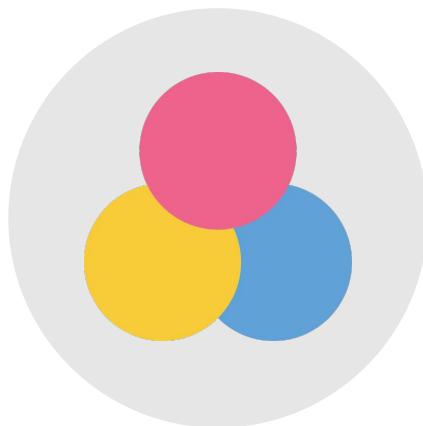
Preservación de la confidencialidad, integridad y disponibilidad de la información.

---

# Seguridad de la información



Confidencialidad



Integridad



Disponibilidad

Bienvenida y panorama general

---

# Vulnerabilidades

CVE, CVSS

---

# ¿Qué es?

Es un fallo de programación,  
configuración o diseño.

---

## Clasificación de vulnerabilidades

**MITRE Top 25**  
Contiene los mayores errores de programación.

**OWASP Top 10**  
Vulnerabilidades de seguridad más críticas en aplicaciones web.

**SANS Top 20**  
Lista de vulnerabilidades que requieren solución inmediata

# OWASP TOP 10

- Inyección.
- Pérdida de autenticación y gestión de sesiones.
- Exposición de datos sensibles.
- U Entidad externa de XML (XXE).
- Pérdida de control de acceso (unido)
- ↗ Configuración de seguridad incorrecta.
- U Secuencia de comando en sitios cruzados (XSS)
- ✗ Deserialización insegura.
- Uso de componentes con vulnerabilidades conocidas.
- ✗ Registro y monitoreo insuficiente.

---

# Gestión de vulnerabilidades

Páginas para encontrar vulnerabilidades:

<https://cve.mitre.org/>

<https://nvd.nist.gov/vuln/search>

<https://www.certsi.es/alerta-temprana/vulnerabilidades>

# CVE

## Common Vulnerabilities and Exposures.

### CVE-ID Syntax Change

#### Old Syntax

**CVE-YYYY-NNNN**

4 fixed digits,  
supports a  
maximum of 9,999  
unique identifiers  
per year

#### New Syntax

**CVE-YYYY-NNNN**

4-digit minimum  
and no maximum,  
provides for  
additional capacity  
each year when  
needed

YYYY indicates year the ID is issued to a  
CVE Numbering Authority (CNA) or  
published.

**Implementation date: January 1, 2014**

Source: <http://cve.mitre.org>

---

# **Common Vulnerability Scoring System (CVSS)**

Es un sistema que pondera la severidad las vulnerabilidades a través de fórmulas.

## Base Metric Group

Access Vector

Access Complexity

Authentication

Confidentiality Impact

Integrity Impact

Availability Impact

## Temporal Metric Group

Exploitability

Remediation Level

Report Confidence

## Environmental Metric Group

Collateral Damage Potential

Target Distribution

Confidentiality Requirement

Integrity Requirement

Availability Requirement



CVE

@CVEnew

Seguir



CVE-2019-10875 A URL spoofing vulnerability was found in all international versions of Xiaomi Mi browser 10.5.6-g (aka the MIUI native browser) and Mint Browser 1.5.3 due to the way they handle the "q" query parameter. The portion of an https URL before... [cve.mitre.org/cgi-bin/cvenam...](https://cve.mitre.org/cgi-bin/cvenam...)



>certuy

**CERTuy** @certuy · 24 oct. 2018



Se ha publicado una vulnerabilidad crítica (9.1) de SSH (libssh) con el  
CVE-2018-10933

[nvd.nist.gov/vuln/detail/CV...](https://nvd.nist.gov/vuln/detail/CVE-2018-10933)



1  
2



Information Technology Laboratory

NATIONAL VULNERABILITY DATABASE

NVD

VULNERABILITIES

## CVE-2018-10933 Detail

### MODIFIED

This vulnerability has been modified since it was last analyzed by the NVD. It is awaiting reanalysis which may result in further changes to the information provided.

## Current Description

A vulnerability was found in libssh's server-side state machine before versions 0.7.6 and 0.8.4. A malicious client could create channels without first performing authentication, resulting in unauthorized access.

**Source:** MITRE

**Description Last Modified:** 10/17/2018

[+View Analysis Description](#)

### QUICK INFO

**CVE Dictionary Entry:**

CVE-2018-10933

**NVD Published Date:**

10/17/2018

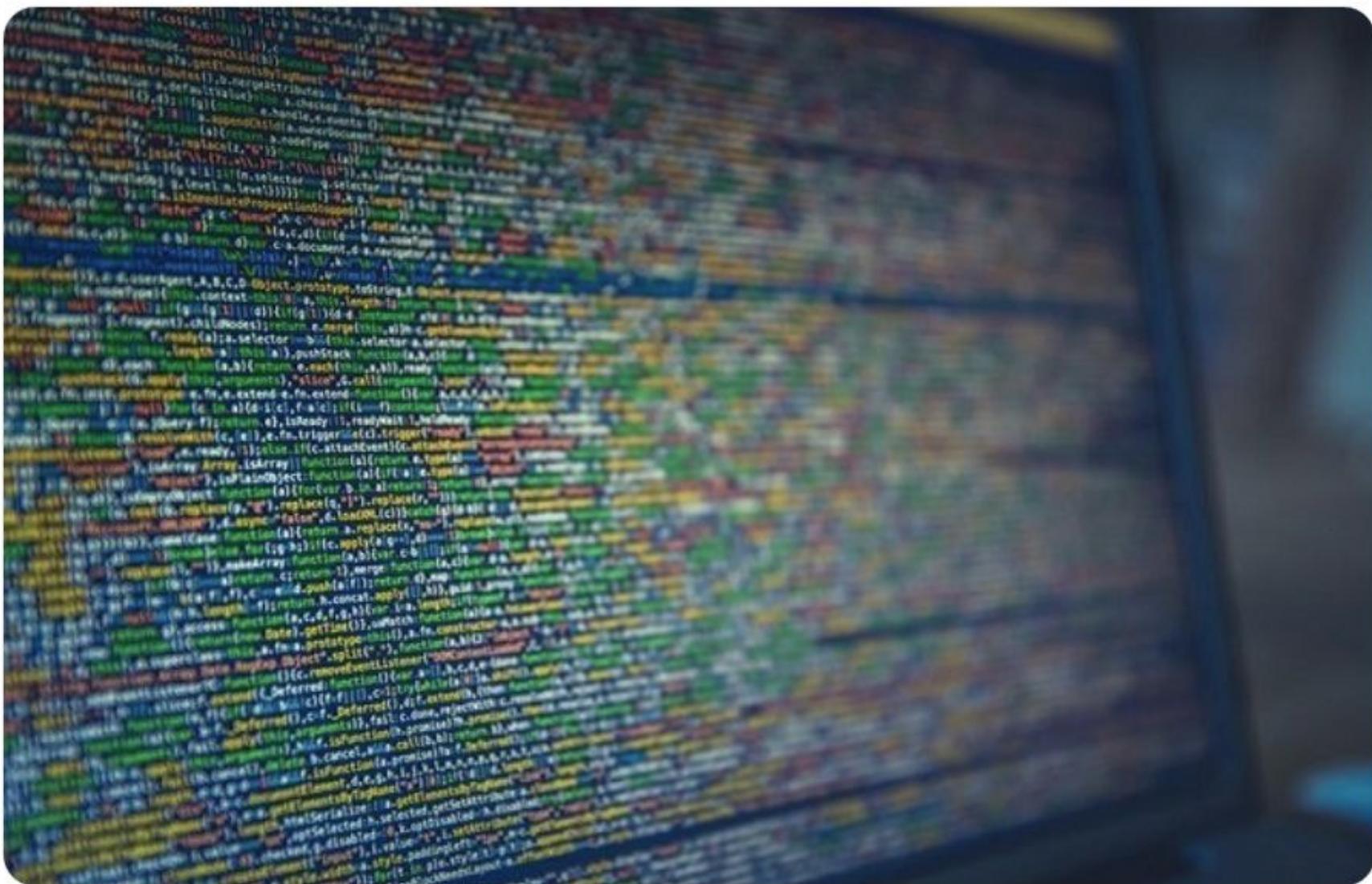
**NVD Last Modified:**

01/19/2019



**UNAM-CERT** @unamcert · 15 mar.

#Vulnerabilidad en #Gearbest expone a millones de compradores [bit.ly/2FePbGn](https://bit.ly/2FePbGn)  
vía @tekcrispy



Introducción al Ethical Hacking

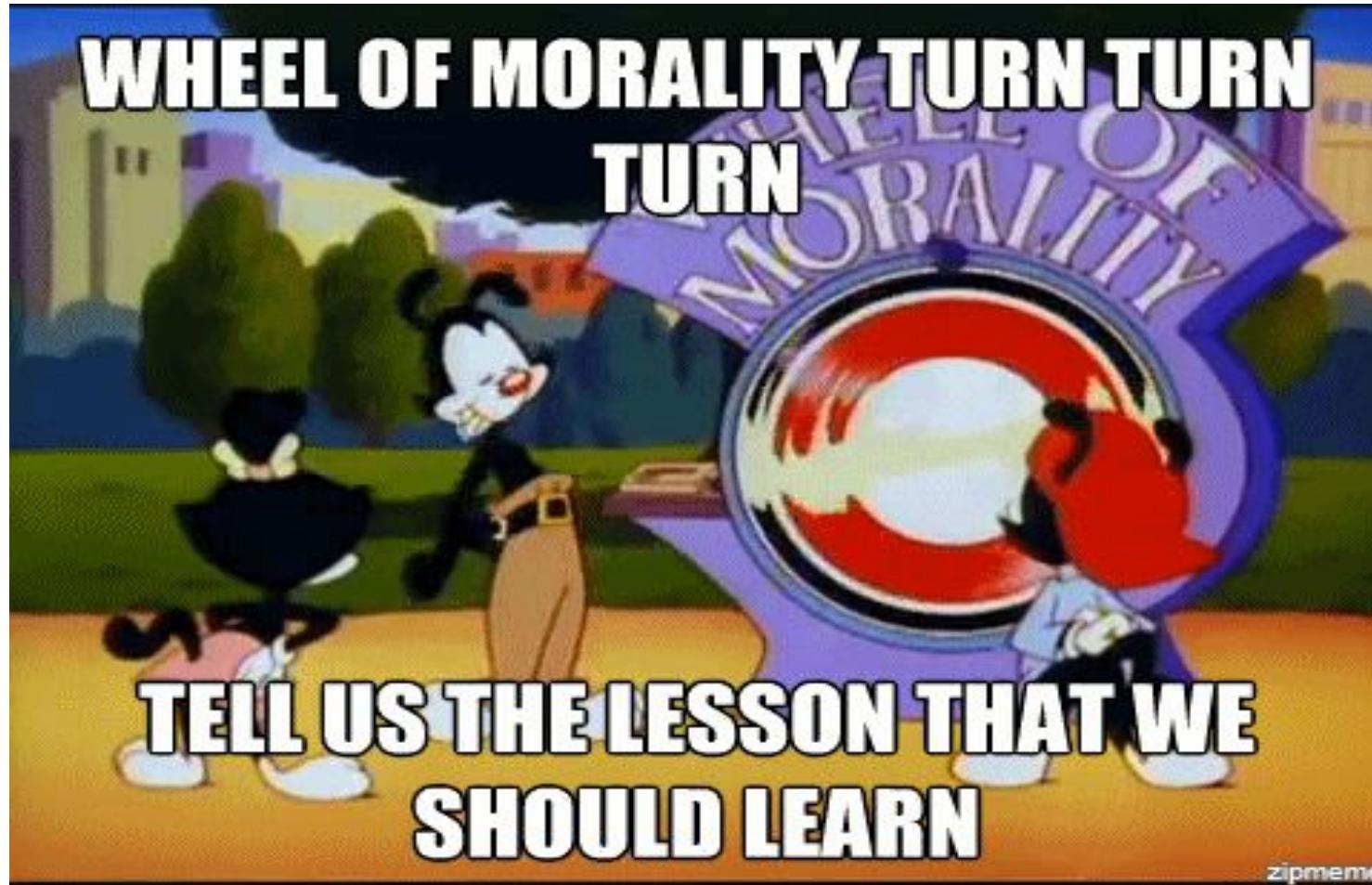
---

¿Qué es hacking y  
hacker?

Black Hat, White Hat, Gray Hat

---

# ¿Qué es la Ética?



# La pregunta del día



¿A quién le das el asiento?

“

En cada comunidad, incluso en la tripulación de un barco pirata, hay acciones obligadas y acciones prohibidas, acciones loables y acciones reprobables

”

*Bertrand Russell*

---

# Código de ética

Conjunto de normas.

---

# ¿Qué es hacking?

Se refiere a la explotación de sistemas vulnerables.

---

---

# Principales motivos

- Robo de información y/o servicios críticos.
- Emoción y desafío intelectual.
- Curiosidad y experimento.
- Ganancia financiera.
- Prestigio y poder.
- Reconocimiento de los compañeros.
- Venganza.

## ¿Cómo es un hacker?

Individuos con excelentes habilidades informáticas.

Capacidad de crear y explorar el software y hardware de un equipo de computo.

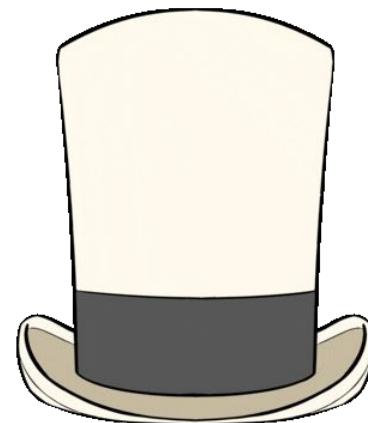
Con conocimientos para descubrir vulnerabilidades en un sistema objetivo.

---

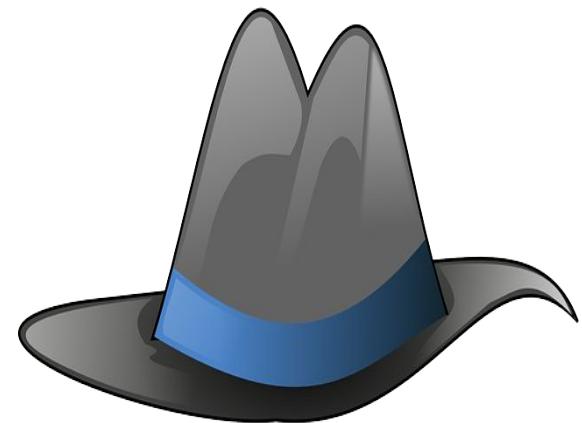
# Tipos de hacker



Black Hat



White Hat



Gray Hat

---

# Tipos de hacker



Script Kiddies



Hacktivist

Introducción al Ethical Hacking

---

# Obteniendo información de fuentes abiertas.

Google Hacking, OSINT  
Framework

---

# Jugando con Google dorks

- Intitle o allintitle.
- inurl o allinurl.
- Intext.
- site.
- filetype.

Introducción al Ethical Hacking

---

¿Es necesario un Hacker  
Ético?

Habilidades, Certificaciones

“

Si utilizas al enemigo para  
derrotar al enemigo, serás  
poderoso en cualquier lugar a  
donde vayas

”

Sun Tzu  
*El arte de la guerra*

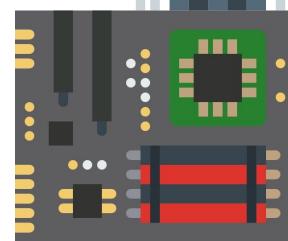
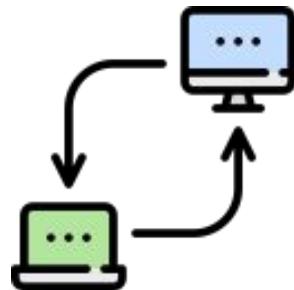
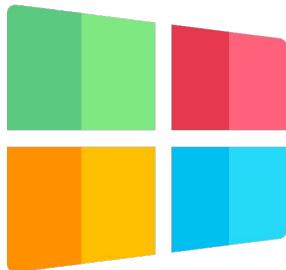
---

# ¿Es necesario un hacker ético?

- Prevenir que un atacante obtenga acceso a los sistemas de información de una organización.
- Descubrir vulnerabilidades en sistemas y explorar su riesgo potencial.
- Para analizar y fortalecer la postura de seguridad de una organización.

---

# Habilidades técnicas



---

# Habilidades no técnicas



## Consultor de Ciber Seguridad jr

CORE ONE IT

Ciudad de México, D. F. [+1 ubicación](#)

**\$13,000 - \$17,000 al mes**

Importante empresa de Seguridad Informática ¡Te esta buscando! Licenciatura o Ingeniería en Informática, Sistemas o carreras a fin. \* Conocimientos en...

**Postúlate rápidamente vía Indeed**

hace 8 días [guardar empleo](#) más...

## Hacker Ético Jr.

Valuglobal Consultoria

Benito Juárez, D. F.

Deseable contar con alguna de las siguientes certificaciones, CEH, GPEN, Security+, ISO/IEC 27001:2013, CISM....

Empleos TI hace 3 días [guardar empleo](#) más...

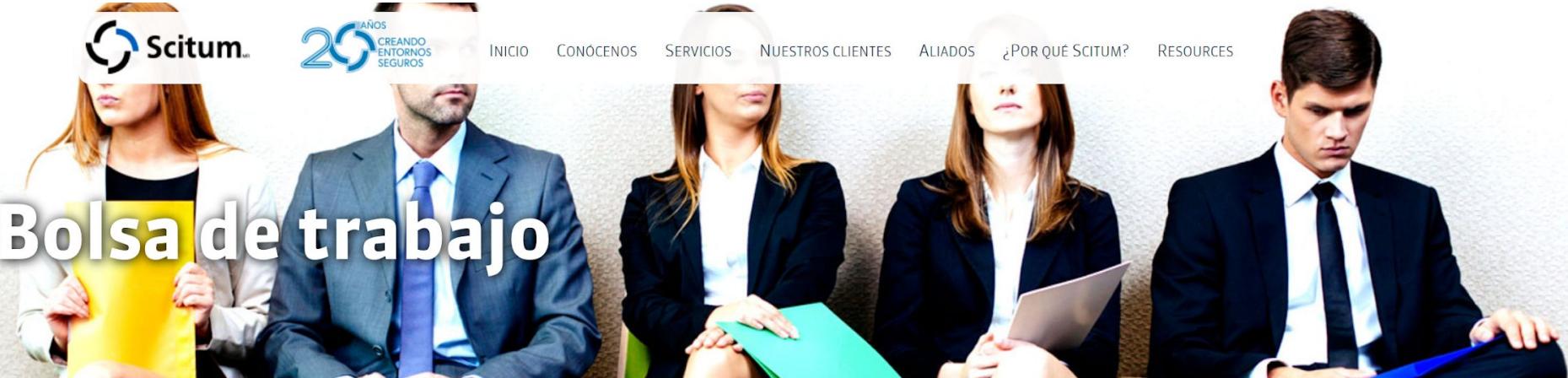
## Ingeniero N3

Kio Networks  41 evaluaciones

Querétaro, Qro.

Certificación en al menos un vendor (Checkpoint, palo alto, fortinet, ect) y/o curso de seguridad (CIH, NSA, CEH)....

hace 16 días [guardar empleo](#) más...



# Bolsa de trabajo

## Vacantes

En Scitum tenemos un compromiso con los altos niveles de servicio para alcanzar la completa satisfacción de nuestros clientes, por eso buscamos la continua capacitación de nuestro personal y su desarrollo constante.

Nos preocupamos por tener siempre un equipo de alto rendimiento y por ello solamente elegimos a los mejor preparados y a los más profesionales ¡Intégrate al equipo Scitum!

Si quieres formar parte de Scitum envíanos un correo con el título de la vacante y tu currículum vítae a [atracciondetalento@scitum.com.mx](mailto:atracciondetalento@scitum.com.mx).

En caso de que cumplas el perfil nos comunicaremos contigo.

 Ing. de operación

 Consultor Tiger Team

- Hackeo Ético
- Pruebas de intrusión
- Análisis de vulnerabilidades
- Fortalecimiento de sistemas.

Una certificación de seguridad y/o metodologías para pruebas de penetración: CEH, OPST, OPSA, GPEN, GWAPT

 Líder técnico

 Gerente de ventas

---

# Hacking ético como profesión.

Un Profesional en Seguridad  
de la Información.

---

# Empresas y asociaciones



**EC-Council**



**CompTIA.**

 **ISACA®**  
*Trust in, and value from, information systems*

**SANS**  
INSTITUTE

**ISECOM**  
INSTITUTE FOR SECURITY AND OPEN METHODOLOGIES

**mile2**  
IT Security Training

# CEH Certified Ethical Hacking.



CORE

ADVANCED

EXPERT



Pentesting

---

# Conceptos

Recomendaciones

---

# Conceptos

**Prueba de penetración:** Es un método para evaluar la seguridad de los sistemas de información y redes.

## ¿Por qué realizar un Pentesting?

Reducir el gasto seguridad de TI y mejorar el RO SI.

Enfocarse en vulnerabilidades de alta severidad y aumentar la conciencia de seguridad.

Adoptar las mejores prácticas en cumplimiento de las normativas legales y del sector.

---

# Recomendaciones

- Establecer los parámetros para la prueba de penetración.
- Documentando el resultado cuidadosamente y haciéndolo comprensible para el cliente.

# Activos a evaluar



Servidores



Estaciones de trabajo



Routers



Firewalls



Dispositivos de red



Base de datos



Aplicaciones



Telecomunicaciones



Seguridad física



Usuarios

# QUÉ NO ES

## Un Pentesting!

---



PENTESTING



AUDITORÍA  
DE SEGURIDAD



EVALUACIÓN DE  
VULNERABILIDADES

Pentesting

---

# Tipos de Pentesting.

Black Box, White Box, Grey Box y  
fases de un pentesting

---

# Diferentes Pentesting

- 1.** Seguridad en la Red
- 2.** Aplicación
- 3.** Seguridad física
- 4.** Ingeniería social

---

# Tipos de Pentesting



Black-Box



White-Box



Grey-Box

---

# **Formas de realizar un Pentesting**

**Pruebas anunciadas:** Se cuenta con la total cooperación y conocimiento del personal de TI.

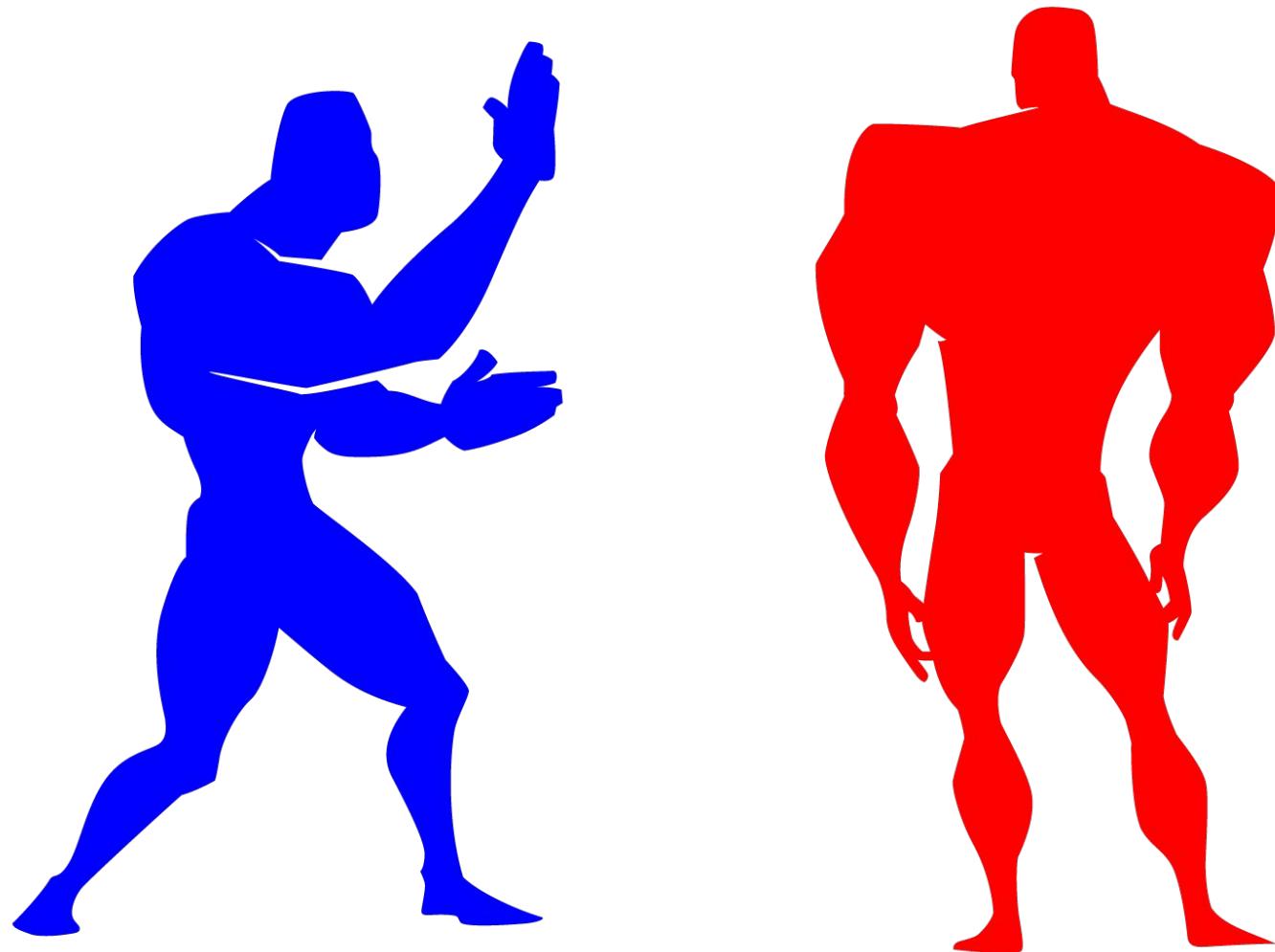
---

# **Formas de realizar un Pentesting**

**Pruebas no anunciadas:** Las pruebas no anunciadas son un intento de comprometer el sistema en la red del cliente sin el conocimiento del personal de seguridad de TI.

---

# Equipo azul y rojo



---

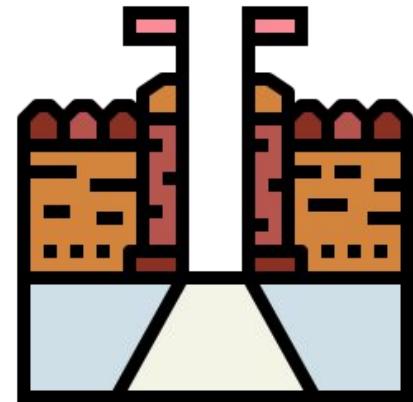
# Fases de un Pentesting



Pre-ataque



Ataque



Post-ataque

Pentesting

---

# Práctica: Escaneo de redes con Nmap.

---

# ICMP Echo Scanning/ Ping Sweep

Se utiliza para detectar equipos activos dentro de la red.

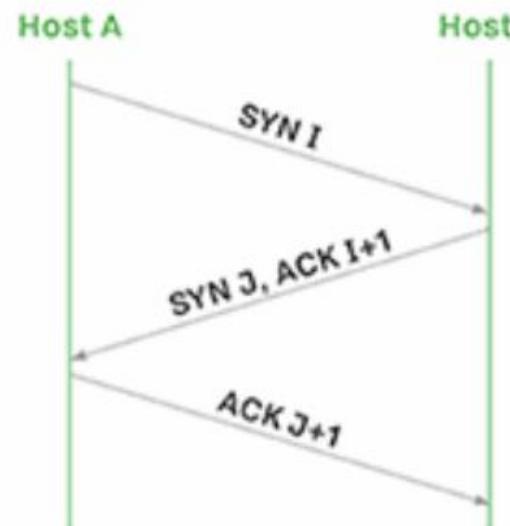
```
nmap -sP 192.168.2.0/24
```

# TCP Connect/ Full Open Scan

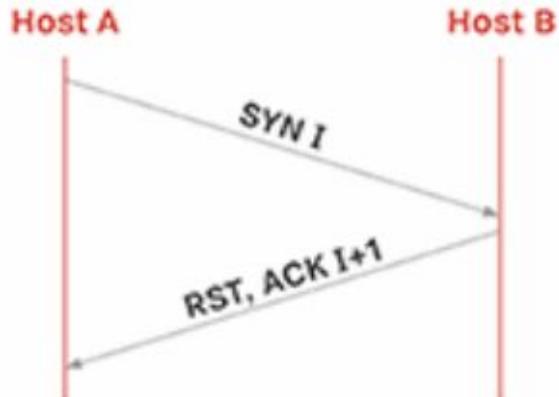
Detecta que puerto se encuentran abiertos

Nmap -sT “IP”

Puerto abierto



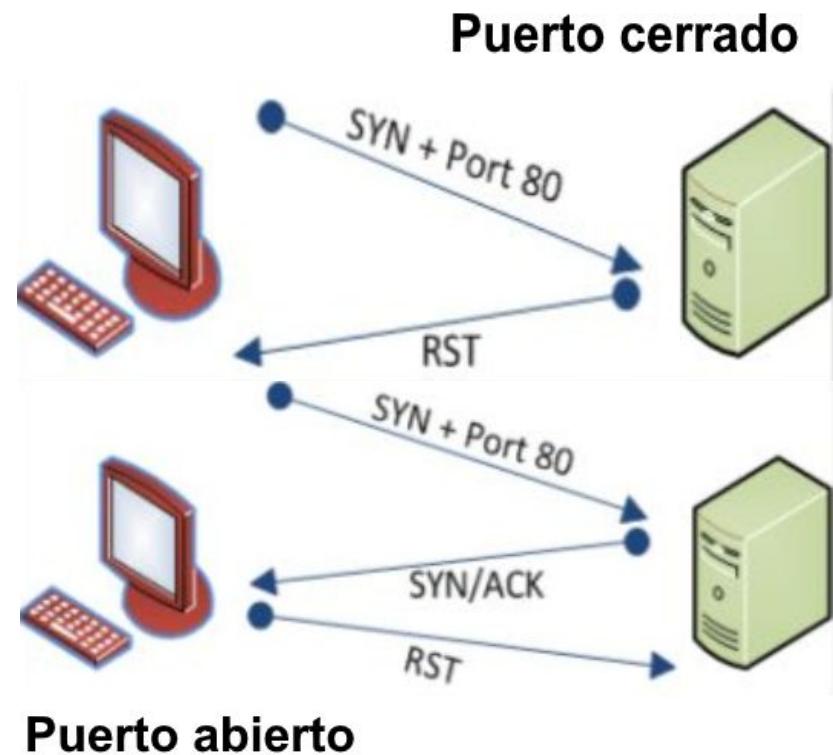
Puerto cerrado



# Stealth Scan (Half-open Scan)

Este escaneo corta el three-way handshake antes de establecer la conexión.

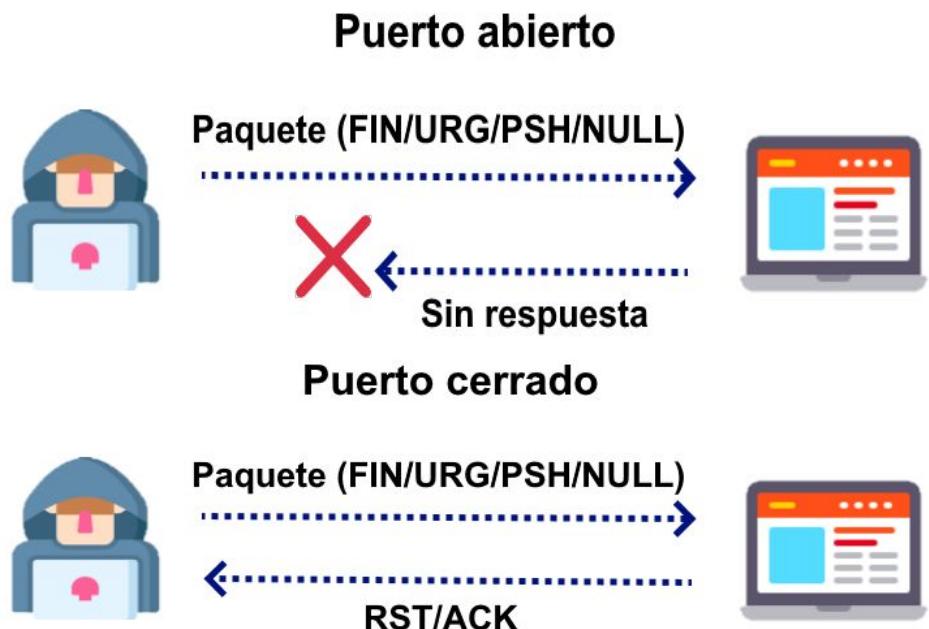
Nmap -sS “IP”



# Inverse TCP Flag Scanning

Envían un conjunto de indicadores (FIN, URG, PSH) o sin indicadores (NULL).

nmap -sX “IP”



# ACK Flag Probe Scanning

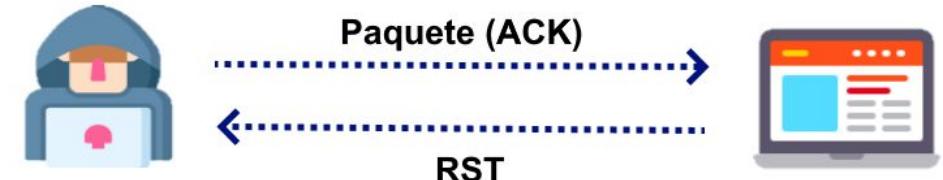
Comprobar si un host destino cuenta con algún mecanismo de filtrado de paquetes.

nmap -sA "IP"

Firewall de Estado presente



Sin Firewall



# IDLE/IPID Header Scan

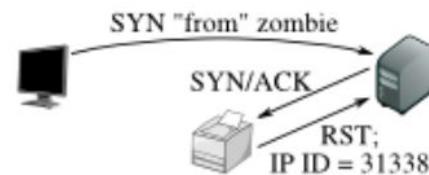
Se utiliza para enviar una dirección de origen falsificada.

Nmap -Pn -p- -sI “IP zombie” “IP víctima”

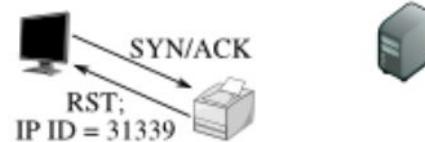
Step 1: Probe the zombie's IP ID.



Step 2: Forge a SYN packet from the zombie.



Step 3: Probe the zombie's IP ID again.



The attacker sends a SYN/ACK to the zombie. The zombie, not expecting the SYN/ACK, sends back a RST, disclosing its IP ID.

The target sends a SYN/ACK in response to the SYN that appears to come from the zombie. The zombie, not expecting it, sends back a RST, incrementing its IP ID in the process.

The zombie's IP ID has increased by 2 since step 1, so the port is open!

---

# Escaneo UDP

Si el sistema no responde con un mensaje entonces el puerto se encuentra abierto.

Nmap -sU “dirección”

Pentesting

---

# Metodologías

NIST SP 800-115

## Metodologías

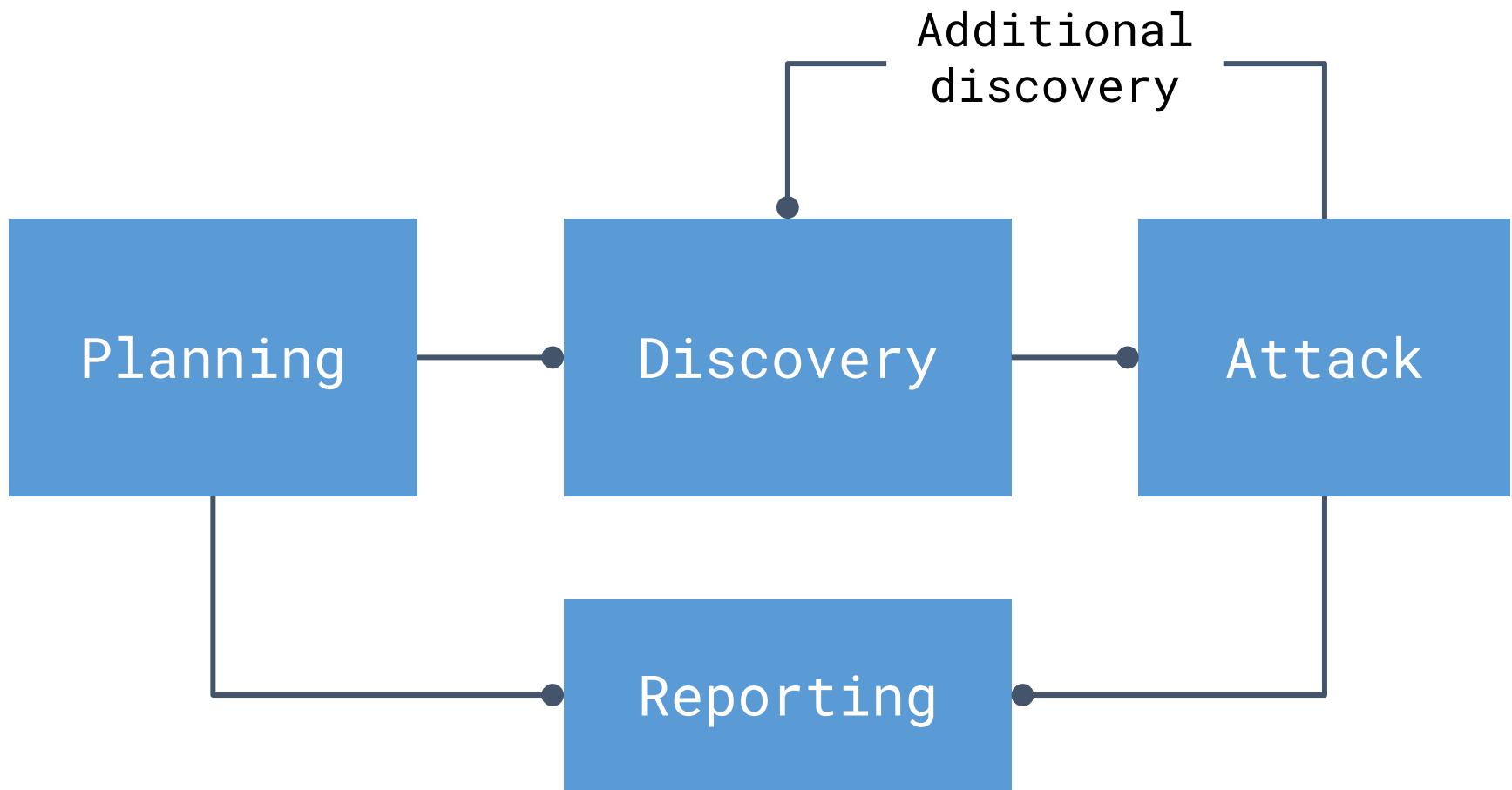
**NIST SP 800-115**  
National Institute of Standards  
and Technologies

**Open Source Security Testing  
Methodology Manual  
(OSSTMM)**

**Information Systems Security  
Assessment Framework (ISAFF).  
OISSG**

---

# NIST SP 800 115



Estándares y aspectos legales

---

# Estándares internacionales.

PCI DSS, HIPAA

---

# Estándar PCI

En el ámbito corporativo es común que se realicen distintos tipos de evaluaciones de seguridad.

---

# PCI DSS

Es un estándar para las organizaciones que manejan información de tarjetas de débito, crédito, prepago, monederos electrónicos, ATM y POS.

---

# Normas de seguridad de datos de la PCI: descripción general de alto nivel

- Desarrolle y mantenga redes y sistemas seguros
- Proteger los datos del titular de la tarjeta
- Mantener un programa de administración de vulnerabilidad
- Implementar medidas sólidas de control de acceso.
- Supervisar y evaluar las redes con seguridad
- Mantener una política de seguridad de información

---

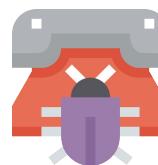
# HIPAA

La HIPAA, también conocida como la Ley de Portabilidad y Responsabilidad de Seguros de Salud (Health Insurance Portability and Accountability Act) de los EE. UU.

# Causas más comunes de Violaciones de HIPAA



- Hackers Profesional
- Divulgación de Socios Comerciales
- Procedimientos de administración incorrectos
- Acceso no autorizado a los registros
- Medidas de seguridad de TI insuficientes



- Acceso no autorizado
- Deshonestidad de los empleados
- Dispositivos perdidos o robados
- Divulgación Accidental del Empleado
- Eliminación inadecuada

# CINCO REGLAS HIPAA



**Regla de privacidad de HIPAA:**  
Reglas de divulgación de PHI



**Regla de seguridad de HIPAA:**  
Normas para salvaguardar ePHI



**Regla omnibus:**  
Fusiona la regla HITECH en HIPAA



**Regla de notificación de incumplimiento:**  
60 días para notificar a HHS



**Regla de cumplimiento:**  
Cómo se llevan a cabo las investigaciones

---

# Digital Millennium Copyright Act (DMCA)

Define la prohibición legal contra la elusión de las medidas de protección tecnológica aplicadas por los propietarios para proteger su trabajo.

## La serie ISO/IEC 27000

La serie 27000 de ISO es un conjunto de normas asociadas a los sistemas de gestión de la seguridad de la información (SGSI).

Incluye requisitos para la evaluación y el tratamiento del riesgo de seguridad de la información adaptados a las necesidades de la organización.

---

# **Ley Sarbanes-OXLEY**

También conocida como SoX, es una ley de los Estados Unidos.

Estándares y aspectos legales

---

# Ciberdelitos

Cibercriminalidad, Convenio de  
Budapest.

---

# Introducción.

La **criminalidad** es uno de los aspectos constantes en la sociedad, la cual data sus orígenes desde el siglo XVIII A.C.

---

# Cibercriminalidad

El desarrollo y la necesidad de la sociedad por la utilización de tecnologías de la información.

---

# Características de la Cibercriminalidad



Fácil Comisión



Situarse  
distintos países



Indicios

---

# **Convenio de Budapest.**

Es el convenio sobre la  
ciberdelincuencia del  
Consejo de Europa.

Compuesto  
por 48  
artículos

**Terminología**

**Medidas que se deberán adoptar  
a nivel nacional**

**Cooperación internacional**

**Cláusulas finales**



Firmó en el momento de su apertura (23 de noviembre de 2011).

---

# ¿Cómo vamos en América latina?

Desde 2004, la OEA en particular la Reunión de Ministros de Justicia o de Fiscales Generales de las Américas (REMJA/OEA) y su Grupo de Trabajo en Delito Cibernético.



En 2013, República Dominicana se convirtió en el primer país de América Latina que se adhirió al Convenio de Budapest.



En 2008, Argentina, por medio de la Ley 26.388, reformó la ley sustantiva penal en consonancia con el Convenio de Budapest.



Colombia realizó una enmienda en el Código Penal en 2009 mediante la Ley 1273 y el Código de Procedimiento Penal en 2011 mediante la Ley 1453.



En México las enmiendas a las leyes sustantivas y procesales están a punto de concluir, lo cual permitirá a este país completar el acceso al Convenio de Budapest sobre el Delito Cibernético

---

# Salvaguarda de evidencias digitales

El objetivo de la salvaguarda es disponer de las pruebas o indicios de una actividad criminal.

Casos típicos de ataques

---

# Análisis estático de malware.

Análisis estático y dinámico de malware

## Tipos de análisis

**Análisis estático de malware:**  
También conocido como análisis de código, con el propósito de revisar el código binario sin ejecutarlo.

**Análisis dinámico de malware:**  
Implica ejecutar el malware para conocer la manera en que interactúa con el sistema.

---

# Herramientas necesarias

- Máquina virtual con Windows XP.



Casos típicos de ataques

---

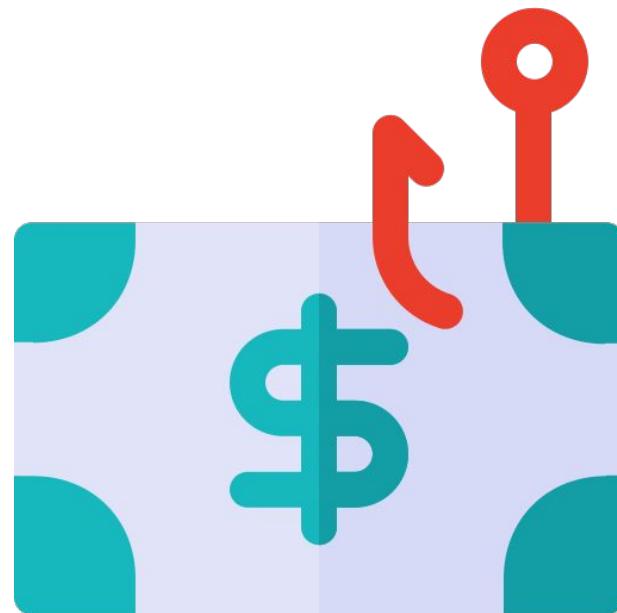
# Ingeniería social

Phishing

---

# Ingeniería social.

Consiste en manipular a una persona.



---

# Phishing

El phishing es una técnica de ingeniería social.

# HARD LESSONS 1 IN HACKING



## #5 TEXTBOOK PHISHING

- ▶ Inbox
  - ▶ Drafts
  - ▶ Sent Items
  - ▶ Deleted Items
- |   |   |         |
|---|---|---------|
| • | ! | Subject |
|---|---|---------|



**CITRIX®**

Security common sense goes a long way and missteps can leave your organization vulnerable. Citrix secures apps and data, reduces complexity and helps manage cloud transition. Visit [Citrix.com/secure](http://Citrix.com/secure) for more.

## Tipos de ataques

**Phishing**

**Dumpster Diving**

**Baiting**

**Shoulder Surfing**

# Casos reales

La web pedia tu ID de Apple y tu contraseña.

Mensaje de texto  
anteayer, 19:09

Alberto Su iPhone 7 128GB  
Black ha sido encontrado a las  
7:09 PM. Ver ubicacion: <https://icluod-find.com/?e=dqx%C>  
iSupport.

---

# ¿Cómo podemos evitarlo?

- Entrenamiento y concientización a los usuarios.
- Realizar campañas de phishing dentro de la institución.
- Analizar detenidamente las URL.
- Verificar los enlaces en páginas como virustotal y phishcheck.me.

Controles y mecanismos de seguridad.

---

# Políticas de seguridad.

Seguridad física, controles de  
acceso

---

# Aseguramiento de información

Se refiere a la garantía de integridad, disponibilidad, confidencialidad y autenticidad de la información.

---

# Políticas de seguridad

Según el IETF se define como: «Una serie de sentencias formales (normas) que deben cumplir todas las personas que tengan acceso a cualquier información y tecnología de una organización»

---

# Aspectos a considerar

- Deben de poder ser implementadas.
- Deben de ser claras y entendibles.
- Deben de hacerse cumplir.
- Deben de definir responsabilidades.
- Deben permitir el flujo normal de trabajo.
- Debe de cumplir con la legislación vigente en cada país.

## Ejemplos de políticas de seguridad.

**Política de contraseñas.**

**Política de acceso remoto.**

**Política de protección antivirus.**

**Política de protección de  
información.**

---

# Seguridad física.

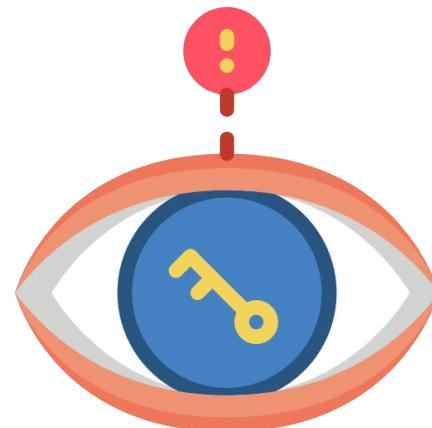
Debemos de considerar que la Seguridad Física consiste en la aplicación de barreras físicas y procedimientos de control.

---

# Dispositivos de control de acceso y vigilancia.



Cámaras



Biometricos



RFID

---

# Controles de acceso.

Protege a una entidad  
contra el uso no autorizado  
de sus recursos.

## Diseño de un mecanismo de control de acceso:

Determinar la información que será accesible por cada usuario.

Determinar el nivel de acceso de cada usuario a la información.

Especificar un mecanismo para otorgar y revocar permisos a los usuarios.

Controles y mecanismos de seguridad.

---

# Bypass autenticación QR

Reto #6 SANS Holiday Hack  
Challenge

# Herramientas Necesarias

**PostMan**  
<https://www.getpostman.com/downloads/>

**Python 3.7.3**  
<https://www.python.org/downloads/>

**Qrcode (pip install qrcode)**  
<https://pypi.org/project/qrcode/>

**Requests (pip install requests)**  
<http://docs.python-requests.org/es/latest/user/install.html>

Controles y mecanismos de seguridad.

---

# Gestión de riesgos y modelado de amenazas.

Complemento

---

# Gestión de riesgos

**Riesgo:** Potencial de que cierta amenaza pueda explotar las vulnerabilidades de un activo o grupo de activos y causar daño a la organización.

**Risk = Threat × Vulnerability × Impact**

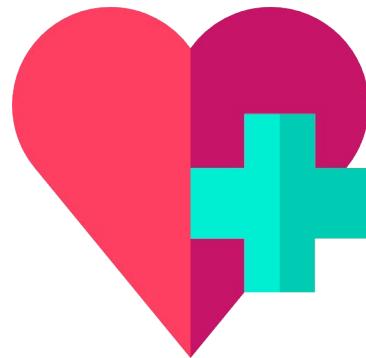
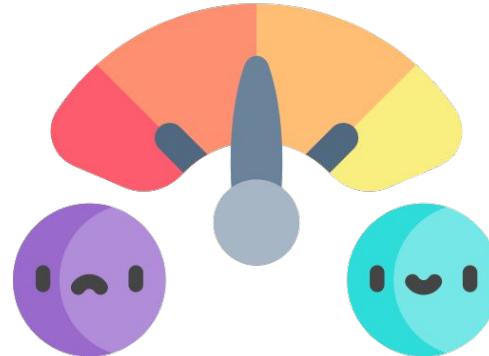
---

# Gestión de riesgos

Es el proceso de identificar, evaluar, responder e implementar actividades que permiten a una organización gestionar riesgos potenciales.

---

# Fases de la gestión de riesgos



---

# Modelado de amenazas

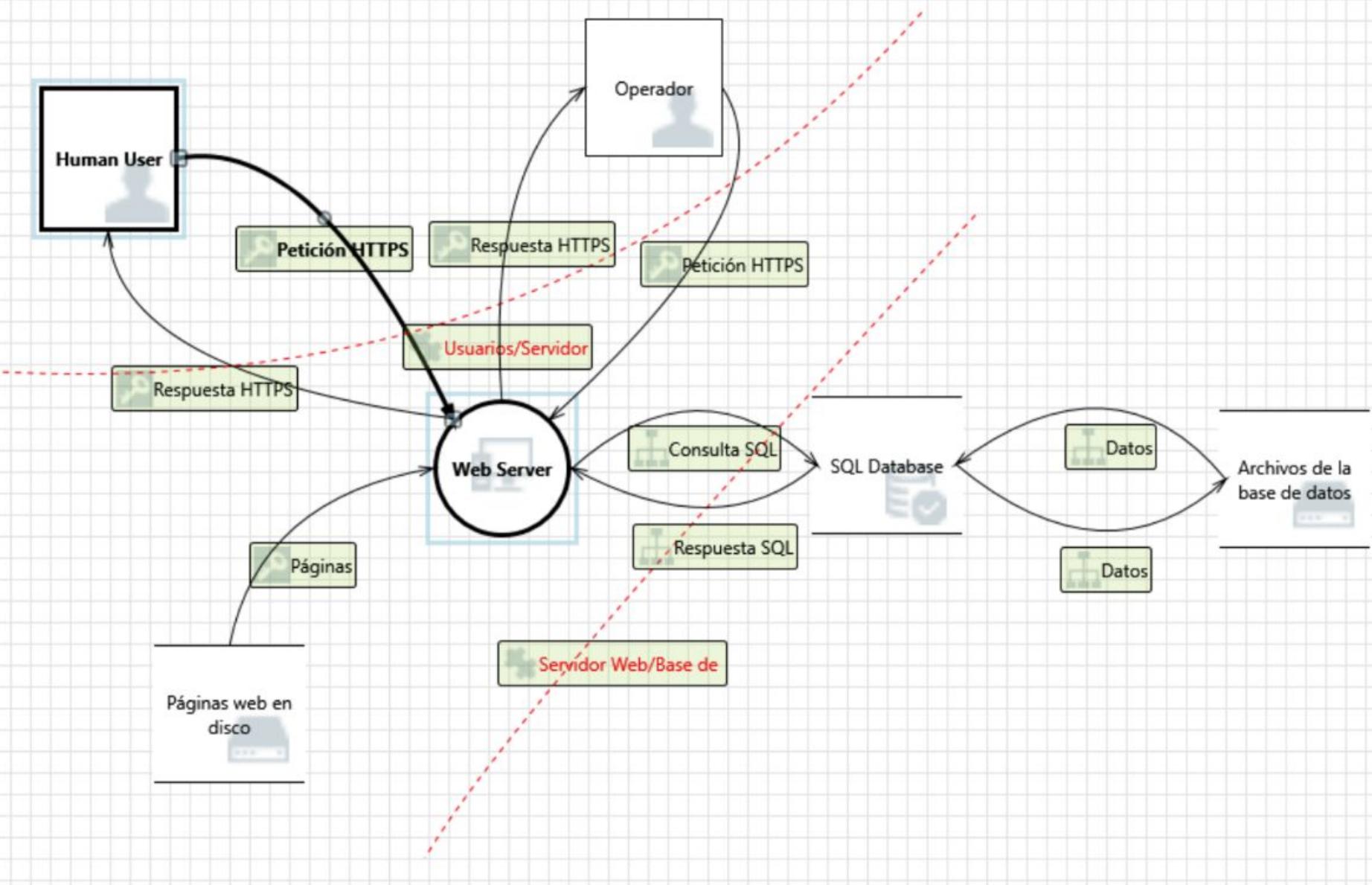
Es un procedimiento para optimizar la seguridad de la red/aplicaciones/Internet.

---

# Fases del modelado de amenazas

- Identificación de la aplicación.
- Definir el uso común.
- Roles de usuarios.
- Identificar dependencias externas.
- Enumerar los supuestos de seguridad.

Diagram: Diagram 1



Controles y mecanismos de seguridad.

---

# Práctica: Instalación del IDS snort.

---

# Instalación del IDS snort.

Es un programa que permite detectar accesos no autorizados a un equipo informático a una red.

## Tipos de IDS

**Sistemas de detección de intrusos basados en equipo (HIDS).**

**Sistemas de detección de intrusos basados en red (NIDS).**