

Módulo 8. Seguridad en Bases de Datos

Diplomado Administración de Base de Datos

Francisco Medina López

Dirección General de Cómputo y de Tecnologías de Información y Comunicación
Universidad Nacional Autónoma de México

2019



- 1 Introducción a la Seguridad en Base de Datos
- 2 Identificación y prevención de vulnerabilidades
- 3 Esquemas de acceso a servidores de bases de datos
- 4 Control de acceso y permisos
- 5 Auditoria a bases de datos



- 1 Introducción a la Seguridad en Base de Datos
- 2 Identificación y prevención de vulnerabilidades
- 3 Esquemas de acceso a servidores de bases de datos
- 4 Control de acceso y permisos
- 5 Auditoria a bases de datos



¿Qué es la seguridad en bases de datos?

Definición

Protección de datos almacenados en un sistema manejador de base de datos contra acceso, uso, modificación o destrucción no autorizada.

Componente de la Ciberseguridad



¿Qué es la Ciberseguridad?

De acuerdo a la Comisión de Ciberseguridad de la Unión Europea:

Definición

Controles y acciones que pueden ser utilizadas para proteger el **ciberspacio**, en ámbitos militares y civiles, ante **amenazas** que puedan comprometer la operación de las redes de telecomunicaciones y/o la infraestructura de los sistemas de información¹.

De acuerdo a la Policía Federal:

Definición

Protección de dispositivos, servicios o redes, así como la protección de datos en contra de robo o daño².

¹ *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace.* [► Enlace](#)

² *Glosario de términos en Ciberseguridad de la Policía Federal.* [► Enlace](#)



¿Qué es el Ciberespacio?

Definición

Ámbito virtual creado por medios informáticos³.

- Término popularizado por la novela Neuromante de William Gibson publicada en 1984 [▶ Enlace](#), pero procede del relato del mismo autor Johnny Mnemonic (1981), incluido en el volumen Quemando Cromo [▶ Enlace](#).
- El 8 de febrero de 1996, en Davos, Suiza, John Perry Barlow escribió la Declaración de independencia del ciberespacio en la que exhortaba a los gobiernos a no ejercer soberanía sobre este, definido por él mismo como “El nuevo hogar de la mente” [▶ Enlace](#).
- En la Cumbre de la OTAN en Varsovia de 2016, y en medio de un debate de extraordinaria intensidad, el ciberespacio se reconoció como un nuevo dominio de las operaciones, al lado de los de dominios tierra, mar, aire y espacio [▶ Enlace](#).

³ *Diccionario de la Real Academia Española.* [▶ Enlace](#)



¿Qué es seguridad de la información?

De acuerdo al estándar ISO 27001:

Definición

Es la preservación de la *confidencialidad, integridad y disponibilidad* de la información. ⁴

De acuerdo con el MAAGTIC:

Definición

La capacidad de preservar la *confidencialidad, integridad y disponibilidad* de la información, así como la autenticidad, confiabilidad, trazabilidad y no repudio de la misma⁵.

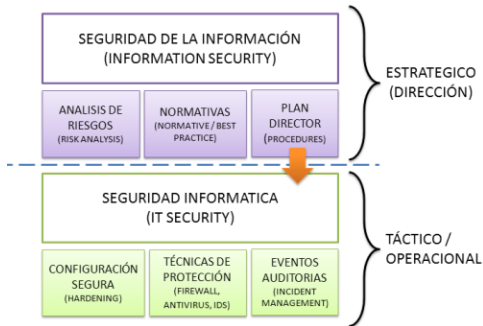
⁴ISO/IEC 27001:2005

⁵Manual Administrativo de Aplicación General en Materia de Tecnologías de la Información y Comunicaciones [▶ Enlace](#)



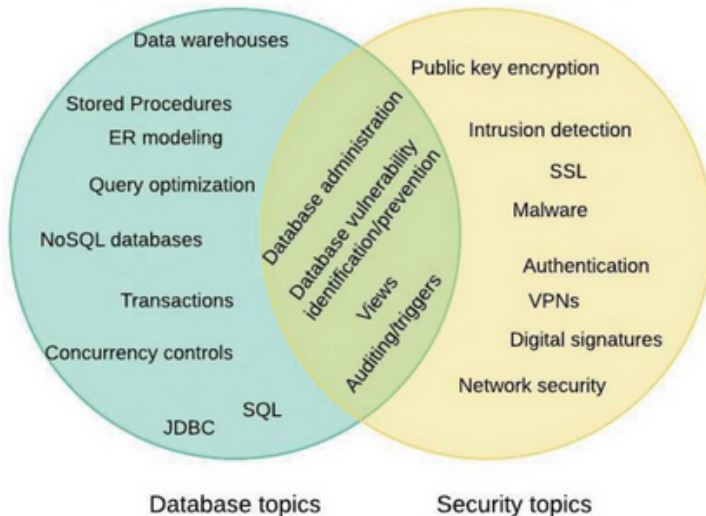
¿Seguridad de la información o informática?

- **La seguridad de la información:** Involucra personas y procesos.
- **La seguridad informática:** Esta enfocado a sistemas de cómputo y redes de datos.



Seguridad en Bases de Datos

The intersection of database and security topics



¿Qué es un ciberataque, cibercrimen y delito?

Ataque informático (Ciberataque)

Intento malicioso de daño, interrupción y acceso no autorizado a sistemas computacionales, redes o dispositivos por medios cibernéticos⁶.

Cibercrimen

El *cibercrimen* es todo delito que implica el uso de medios electrónicos o comunicaciones basadas en Internet.

Delito

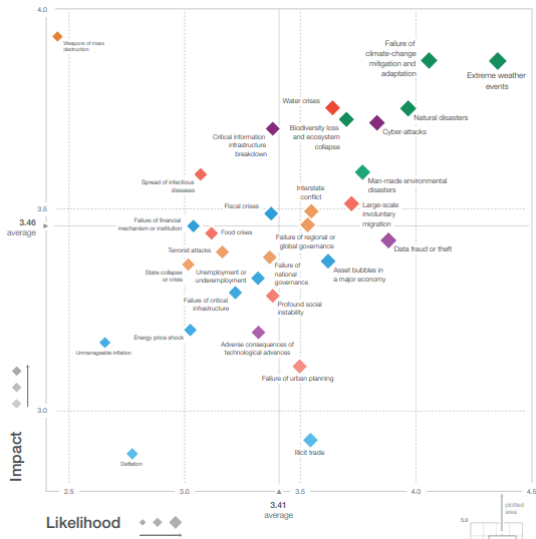
Acto (hacer algo) u omisión (dejar hacer algo) que sancionan las leyes penales. Ejemplos:

- *Pornografía infantil, fraude, extorsión, falsificación, robo de información, alteración de información, espionaje, amenazas, ...*

⁶ Glosario de términos en Ciberseguridad de la Policía Federal. [► Enlace](#)



Los ataques informáticos son una amenaza mundial



México, país con más ataques informáticos

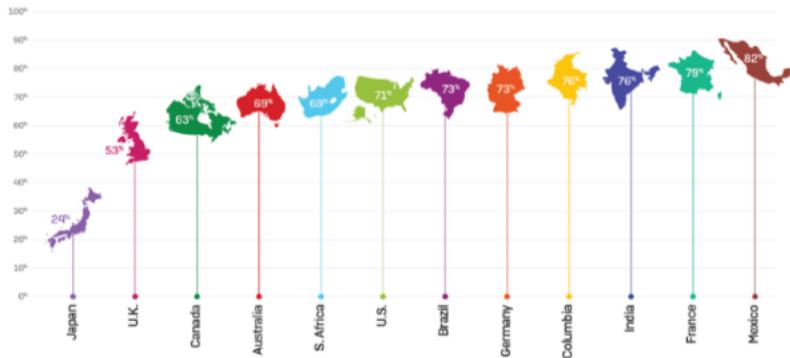


Imagen: Sophos

Figura: “Empresas víctimas de un ciberataque”

(Imagen tomada de: “Economía Hoy”)

► [Enlace](#)



México, país con más ataques informáticos

- Durante 2018 el **82 % de las empresas** fueron blanco de al menos un ataque a los sistemas con los que operan [▶ Enlace](#).
- Todas las **entidades financieras** en México sufrieron ciberataques [▶ Enlace](#).
- **Solo 44 %** de las empresas reporta a autoridades.
- FMI señala la **deficiente** participación de México para intercambiar información sobre ciberataque [▶ Enlace](#).
- Los ataques más representativos tanto en el país como a nivel global sucedieron a través de **phishing**, mientras que uno de cada cuatro episodios se dieron mediante **memorias USB** y dispositivos externos. [▶ Enlace](#).



Ataques informáticos en México I

- **El 30 de julio de 2019**, Librería Porrúa confirma que 1.14 millones de sus clientes fueron afectados por filtración de datos personales. [▶ Enlace](#) [▶ Enlace](#) Después de acceder y borrar la información almacenada en MongoDB, cibercriminales solicitan el pago de bitcoins para recuperar información eliminada. [▶ Enlace](#) .
- **El 15 de julio de 2019**, la Camara Industrial de Nuevo León fue objeto de un ataque que afectó el funcionamiento de sus sistemas [▶ Enlace](#) .
- **El 10 de julio de 2019**, La empresa de seguridad informática Kaspersky informó que descubrió “una nueva muestra de un malware especializado en ataques a cajeros automáticos, cuya actividad ha sido detectada en Colombia y México” [▶ Enlace](#) .
- **El primero de julio de 2019**, el Senado recibió un ciberataque [▶ Enlace](#) .



Ataques informáticos en México II

- **El 19 de junio de 2019**, la española Naturgy fue atacada por un virus del tipo Ransomware [▶ Enlace](#) [▶ Enlace](#) .
- **El 15 de abril de 2019**, hackean y hacen públicos pasaportes, visas y papeles de la embajada de México en Guatemala [▶ Enlace](#) .
- **El 13 de febrero de 2019**, CI Banco restringe operaciones por “virus” [▶ Enlace](#) .
- **El dos de enero de 2019**, la Secretaría de Seguridad Pública del Estado de San Luis Potosí (SSPE) a través de la Policía Cibernética exhortó a la ciudadanía a no abrir el link <http://5ack.com/Mexico/>, el cual ofrece ganar 40 mil pesos de ISS (Instituto de Seguro Social) si has trabajado entre 1980 y 2018 [▶ Enlace](#) ..
- **En enero de 2019**, KPMG México confirma filtración de datos de sus clientes; “lamentamos profundamente este incidente” [▶ Enlace](#) .



Ataques informáticos en México III

- **El 7 de agosto de 2018**, un investigador descubrió una base de datos MongoDB de acceso público en Internet que contenía información personal de más de 2 millones de pacientes de México [▶ Enlace](#).
- **El 17 de julio de 2018**, se detecta una campaña de phishing que suplanta la identidad de Mercado Libre engañando a los usuarios de México con un falso sitio para comprar ropa online [▶ Enlace](#).
- **El 27 de abril de 2018**, se detectan fallas en SPEI [▶ Enlace](#). El hackeo generó fraude en 836 cuentas de 10 bancos [▶ Enlace](#) y permitió el robo de 400 millones de pesos [▶ Enlace](#). Delincuentes ofrecen \$25,000 MX a clientes para retirar dinero robado [▶ Enlace](#).



Ataques informáticos en México IV

- **En febrero de 2018**, el entonces encargado de la Dirección Corporativa de Tecnologías de Información de PEMEX, confió en entrevista con El Universal, que la petrolera es la empresa mexicana con más intentos de penetración ilegal a sus sistemas informáticos

► [Enlace](#)

- **El 9 de enero de 2018**, la Procuraduría General de la República, a través de la Agencia de Investigación Criminal (AIC), en colaboración con el Buró Federal de Investigaciones (FBI, por sus siglas en inglés), logró identificar en la infraestructura del ciberespacio mexicano, un software malicioso de origen norcoreano denominado FALLCHILL, aplicación que probablemente sería un virus informático para la obtención de información y control de los equipos ► [Enlace](#) ..

- **Desde 2017**, el spyware Pegasus para Android e iOS está activo en México y otros 44 países ► [Enlace](#)



Ataques informáticos en México V

- **El 27 de diciembre de 2014**, el grupo Sickillers lanzó un blog (sickillersmx.wordpress.com) donde comenzó a publicar datos del hackeo a la tienda departamental Liverpool [▶ Enlace](#).



Control o contramedida

Definición

Cualquier tipo de **mecanismo** que permita *identificar, proteger, detectar, responder o minimizar* el **riesgo** asociado con la ocurrencia de una **amenaza** específica.

Objetivo:

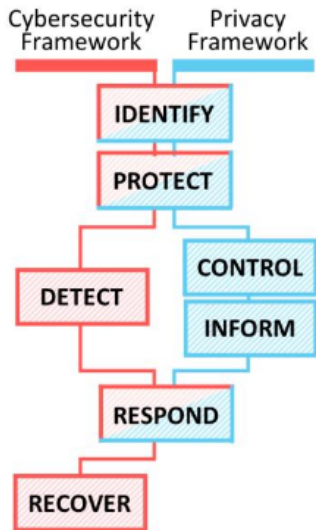
- Reducir los efectos producidos por las amenazas de seguridad (threats) y vulnerabilidades (vulnerabilities) a un nivel tolerable para una organización.

Los controles o contramedidas pueden ser:




- Preventivos / De detección / Correctivos / De respuesta / De recuperación.
- Físicos / Técnicos (Lógicos) / Administrativos



Clasificación de los controles



Primary Functions for Managing Privacy Risk Sources:

-  data security loss
-  data security loss & direct authorized data processing
-  direct authorized data processing



Definición

Cualquier **debilidad** que puede explotarse para causar pérdida o daño a un sistema.

- Condición que podría permitir que una amenaza se materialice con mayor frecuencia, impacto o ambas.
- Una vulnerabilidad puede ser la ausencia o debilidad en los controles administrativos, técnicos o físicos.

El punto más débil de seguridad de un sistema consiste en el punto de mayor vulnerabilidad de ese sistema.



Definición

Posibilidad de ocurrencia de algún evento negativo para las personas y/o empresas .



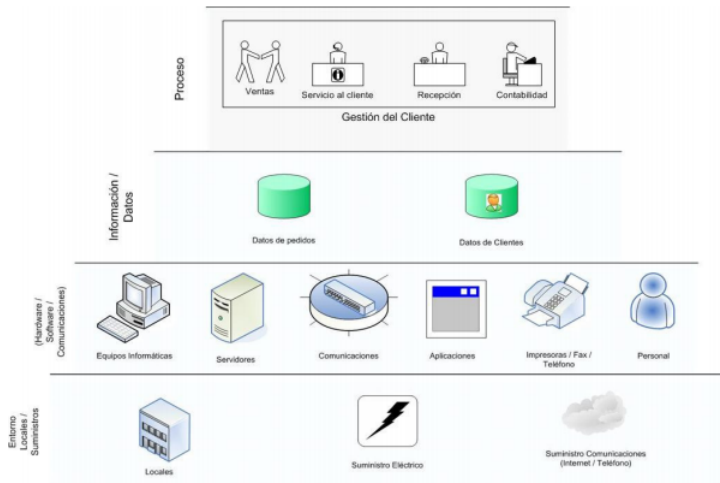
Definición

Recursos que se están tratando de proteger

- Pueden ser datos, sistemas, software, . . .
- El valor o la criticidad del activo determina las medidas de seguridad a implementar.



Activos de un sistema de cómputo



Definición

Evento o **circunstancia** con el potencial suficiente de causar pérdida o daño a una organización o individuo.

- La amenazas explotan, es decir toman ventaja de **vulnerabilidades**.
- La “entidad” que toma ventaja de una vulnerabilidad, suele referirse como “agente de la amenaza” (*Threat Agent*).
- Origen de las amenazas:
 - Naturales (terremotos, inundaciones, ...),
 - Humanas (Cyberdelincuentes, Malware, ...)



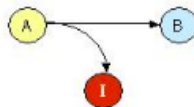
Clasificación de amenazas



Flujo Normal



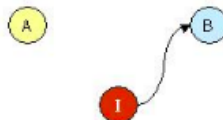
Interrupción



Intercepción



Modificación



Fabricación



Interrupción

Definición

Un activo del sistema se pierde, se hace no disponible o inutilizable.

Ejemplos:

- Destrucción maliciosa de un dispositivo.
- Borrado de un programa o de un archivo de datos.
- Malfuncionamiento del manejador de archivos del sistema operativo que trajera como consecuencia que no se pueda hallar un archivo particular en el disco duro.



Definición

Alguna parte no autorizada logra acceso a un activo del sistema.

Ejemplos:

- Copiado ilícito de programas o archivos de datos.
- La intervención del canal para obtener datos sobre la red.



Definición

Cuando una parte no autorizada logra acceso al activo del sistema y puede manipular ese activo.

Ejemplos:

- Cambiar datos en una base de datos.
- Alterar un programa para que realice alguna computación adicional o distinta a la que realiza
- Modificar datos en una comunicación, entre otras acciones.



Definición

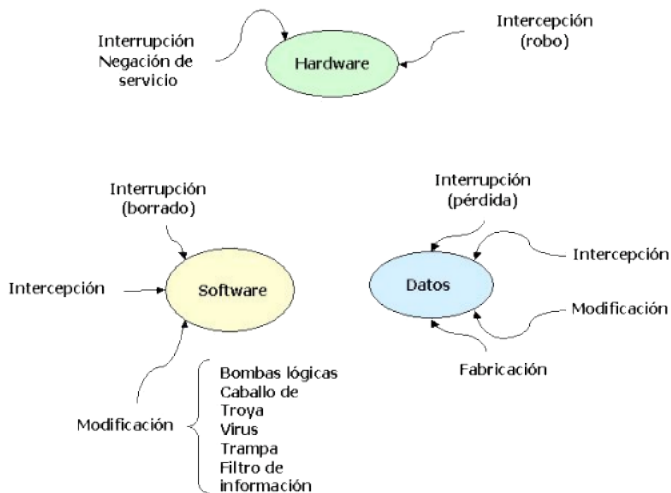
Una parte no autorizada puede crea o fabrica objetos falsos en un sistema.

Ejemplos:

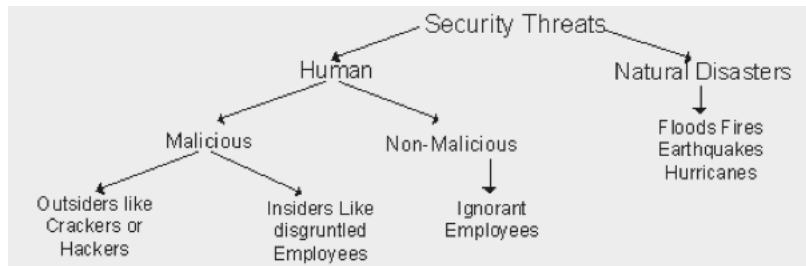
- Inserción de transacciones espurias en un sistema de comunicación en red.
- Agregar registros a una base datos ya existente.



Amenazas a Hardware, Software y Datos



Origen de las amenazas



IT for Decision Makers



Relación conceptos de seguridad informática

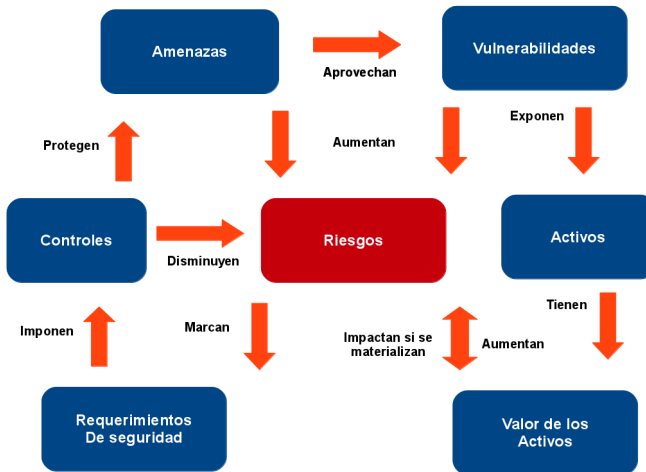


Figura: “Relación conceptos de seguridad informática”

(Elaboración propia.)



Definición

Programas diseñados para infiltrarse en los sistemas y ocasionar afectaciones en los dispositivos electrónicos (computadoras, tabletas, teléfonos móviles inteligentes, etcétera), alterando su funcionamiento y poniendo en riesgo la información almacenada en ellos [▶ Enlace](#).

Ejemplos:

- Malware polimórfico.
- Virus.
- Ransomware.
- Gusano (Worm).
- Troyano (Trojan).
- Rootkit.
- Keylogger.
- Adware.
- Spyware.
- Bots.
- RAT.
- Bomba lógica.
- Backdoor.



Evolución del malware

Cantidad total de malware

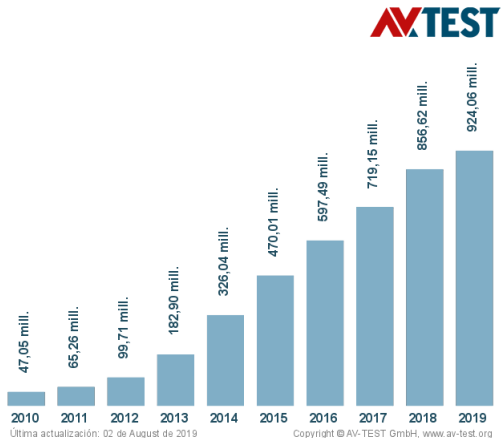


Figura: “Cantidad total de malware”

(Imagen tomada de: <https://www.av-test.org/en/statistics/malware/>)



Definición

Código malicioso que por medio de un motor polimórfico se muta a sí mismo mientras mantiene su algoritmo original intacto, es decir, mantiene su funcionalidad prescrita intacta. Esta técnica es utilizada comúnmente por virus informáticos y gusanos para ocultar su presencia [▶ Enlace](#).



Definición

Código malicioso que se propaga o infecta insertando una copia de sí mismo en otro programa para convertirse en parte de él. Un virus no puede ejecutarse por sí mismo, requiere que el programa que lo aloja sea ejecutado para poder realizar sus operaciones.⁷.

⁷ *Glosario de términos del CERT-UNAM.* [▶ Enlace](#)



Definición

Nombre empleado para referirse al código malicioso que cifra archivos en un sistema y los deja inaccesibles permanentemente al usuario.



Definición

Código malicioso diseñado por ciberdelincuentes para bloquear el acceso a los dispositivos electrónicos o codificar los archivos en ellos, para después solicitar a sus víctimas un pago para el “rescate” de su información⁸.

⁸ *Glosario de términos en Ciberseguridad de la Policía Federal.* [► Enlace](#)



Gusano (Worm)

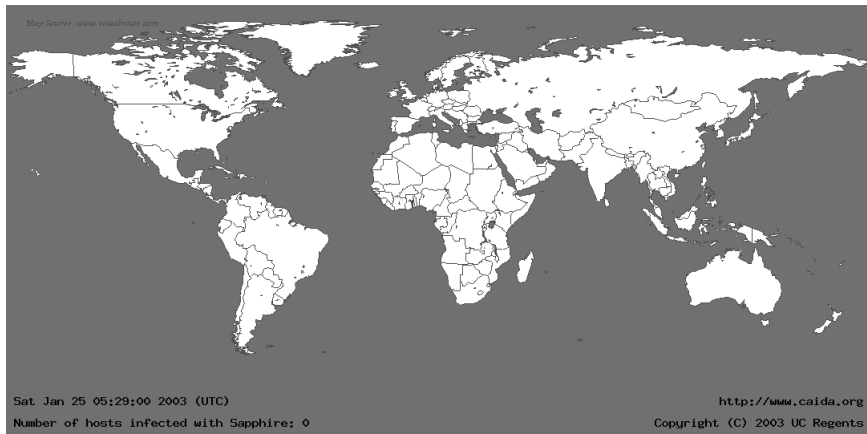
Definición

Agente infeccioso capaz de autoduplicarse de manera autónoma, capaz de buscar nuevos sistemas e infectarlos a través de la red⁹.

⁹ *Glosario de términos en Ciberseguridad de la Policía Federal.* [► Enlace](#)



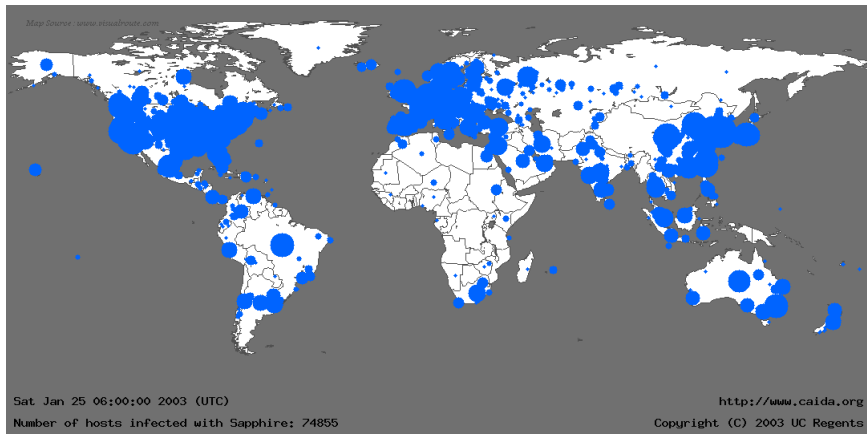
Ejemplo de gusano: Sapphire/Slammer Worm



<http://www.caida.org/publications/papers/2003/sapphire/sapphire.html>



Ejemplo de gusano: Sapphire/Slammer Worm



<http://www.caida.org/publications/papers/2003/sapphire/sapphire.html>



Definición

Código malicioso diseñado para ocultarse en el sistema del equipo infectado bajo la fachada de software legítimo¹⁰.

¹⁰ *Glosario de términos en Ciberseguridad de la Policía Federal.* [► Enlace](#)



Definición

Conjunto de programas que un invasor utiliza para ocultar su intrusión y obtener acceso a nivel de administrador en un equipo de computo o sistema ¹¹.

¹¹ *Glosario de términos del CERT-UNAM.* [▶ Enlace](#)



Definición

Programa que recoge y guarda una lista de todas las teclas pulsadas por un usuario. Dicho programa puede hacer pública la lista, permitiendo que terceras personas conozcan estos datos lo que ha escrito el usuario afectado (información introducida por teclado: contraseñas, texto escrito en documentos, mensajes de correo, combinaciones de teclas ¹².

¹² *Glosario de términos del CERT-UNAM.* [▶ Enlace](#)



Definición

Acrónimo de las palabras “advertisement” (del inglés “anuncio”) y software. Programa que reproduce, muestra o descarga contenido publicitario al equipo de un usuario, usualmente sin su conocimiento, aunque también se instala con autorización en el caso de que se descarguen aplicaciones que lo tienen incluido ¹³.

- Típicamente aparece en forma de ventanas emergentes o cambios en los ajustes de la página de inicio y el motor de búsqueda del navegador. El contenido suele mostrarse de manera inesperada e indeseada para el usuario.

¹³ *Glosario de términos de ESET.* [▶ Enlace](#)



Definición

Código malicioso difícil de detectar que recopila información sobre hábitos e historial de navegación o información personal (como números de tarjetas de crédito) y a menudo utiliza Internet para enviar esta información a terceros sin su conocimiento. Los keyloggers son un tipo de spyware que monitoriza sus pulsaciones en el teclado ¹⁴.



Definición

Viene de “robot”. Es un programa informático cuya función es realizar tareas automatizadas a través de Internet, generalmente funciones simples que requieren de cierta repetición. Los cibercriminales emplean este tipo de software para llevar a cabo acciones maliciosas a través de redes botnet como la distribución de correo basura (spam), descarga de malware u otros ataques desde las computadoras zombis ¹⁵.

¹⁵ *Glosario de términos de ESET.* [▶ Enlace](#)



Remote Acces Tool (RAT)

Definición

Herramienta de acceso remoto (del inglés Remote Access Tool o Remote Access Trojan) que permite obtener privilegios de administrador en un equipo remoto. Si bien son mayormente asociadas a fines maliciosos, e instaladas sin consentimiento del usuario, también pueden ser utilizadas en la administración legítima del sistema ¹⁶.

- El término “RAT” se puede considerar sinónimo de “backdoor”, aunque usualmente implica un paquete completo que incluye una aplicación cliente destinada a la instalación en el sistema objetivo, y un componente de servidor que permite la administración y el control de los bots individuales o sistemas comprometidos.

¹⁶ *Glosario de términos de ESET.* [▶ Enlace](#)



Definición

Del término en inglés Logic Bomb. Es un programa informático que se instala en una computadora y permanece oculto hasta cumplirse una o más condiciones preprogramadas para entonces ejecutar una acción. A diferencia de un virus, una bomba lógica jamás se reproduce por sí sola ¹⁷.

- **Ejemplos de condiciones predeterminadas:** día de la semana, hora, pulsación de una tecla o una secuencia de teclas, levantamiento de un interfaz de red, etc.
- **Ejemplos de acciones:** borrar la información del disco duro, mostrar un mensaje, reproducir una canción, enviar un correo electrónico

¹⁷ *Glosario de términos del CERT-UNAM.* [▶ Enlace](#)



Definición

1. Métodos utilizados por los desarrolladores de software para asegurar que pueden continuar teniendo acceso a las aplicaciones incluso si en un futuro se cambian los métodos normales de acceso.
2. Programas que son instalados por los atacantes después de lograr acceso no autorizado a sistemas para asegurar que pueden continuar teniendo acceso completo a los mismos.



Indicadores de compromiso (IOCs)

Definición

Pistas o signos presentes en un sistema comprometido por actividad no autorizada. [▶ Enlace](#) Es decir, la **evidencia digital** forense de un ataque informático. [▶ Enlace](#)

Herramientas para la búsqueda de indicadores de compromiso:

- Redline de Fireeye. [▶ Enlace](#)



Indicadores de compromiso (IOCs)

- Patrones de tráfico inusual en la red.
- Anomalías en la actividad de la cuenta de usuario con privilegios.
- Irregularidades geográficas en los patrones de acceso.
- Banderas rojas en el acceso a cuentas.
- Incremento del volumen de la base de datos.
- Cambio en el tamaño del HTML de respuesta.
- Un gran número de solicitudes para el mismo archivo.
- Puertos de aplicaciones estándar no coinciden.
- Registro o cambios sospechosos en el sistema de archivos.
- Peticiones DNS inusuales.
- Actualizaciones de sistemas no esperada.
- Cambios en el perfil de dispositivos móviles.
- Datos en lugares incorrectos.
- Tráfico Web con comportamiento no humano.
- Rastros de actividad DDoS incluso por breves lapsos.



Ataques informáticos

Definición

Intento organizado y deliberado de una o más personas para causar daño o problemas a un sistema informático o red. [▶ Enlace](#)

- Consiste en aprovechar alguna debilidad o falla (vulnerabilidad) en el software, hardware e incluso en las personas que forman parte de un ambiente informático, a fin de obtener un beneficio causando un efecto negativo en la seguridad del sistema, que repercute directamente en los activos de la organización [▶ Enlace](#).

Tipos de ataques informáticos:

- Métodos de Ingeniería Social.
- Ataques a aplicaciones/servicios.
- Ataques a redes inalámbricas.
- Ataques a la criptografía.



Ejemplo de ataques informáticos

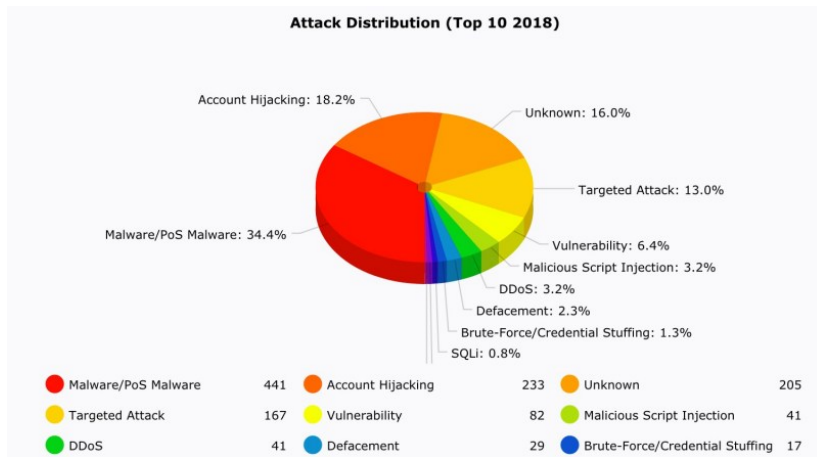
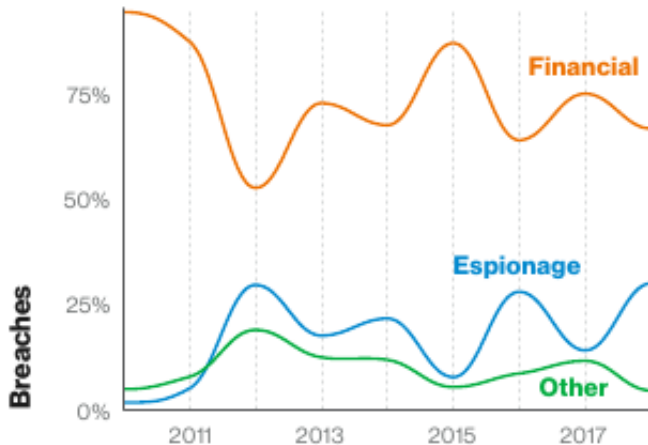


Figura: “Distribución de ciberataques”

(Imagen tomada de: <https://www.hackmageddon.com/2019/01/15/2018-a-year-of-cyber-attacks/>)



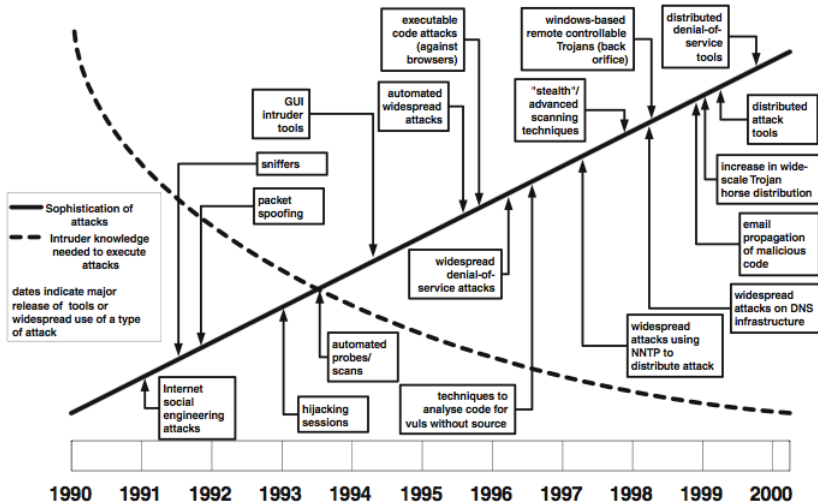
Motivación detrás de los ataques informáticos



2019 Data Breach Investigations Report [▶ Enlace](#)



Evolución de los ataques



Definición

Técnicas utilizadas para **manipular** a la gente a fin de que **realice** acciones específicas o se sume a la **difusión** de información que es útil para un atacante. [▶ Enlace](#)

Métodos Online:

- Phishing, Vishing, Whaling, Spear Phishing
- Spoofing

Métodos Offline / Físicos

- Tailgating
- Impersonation
- Dumpster Diving
- Shoulder Surfing
- Hoax
- Watering Hole Attack



Principios de la Ingeniería Social

- 1 Autoridad.
- 2 Intimidación.
- 3 Consenso.
- 4 Escasez.
- 5 Familiaridad.
- 6 Confianza.
- 7 Urgencia.



Ataques a Aplicaciones/Servicios

- DoS
- DDoS
- Man-in-the-Middle
- Buffer Overflow
- Injection
- Cross-Site Request Forgery
- Privilege Escalation
- ARP Poisoning
- Amplification
- DNS Posoning
- Domain Hijacking
- Man-in-the-Browser
- Zero Day
- Replay
- Pass the Hash
- Hijacking y Ataques relacionados
- Driver Manipulation
- Spoofing
- MAC Spoofing
- IP Address Spoofing



Ataques a redes inalámbricas

- Replay
- IV
- Evil Twin
- Rogue AP
- Jamming
- WPS
- Bluejacking
- Bluesnarfing
- RFID
- NFC
- Disassociation



Ataques a la Criptografía

- Cumpleaños
- Texto claro conocido
- Ataques a contraseñas
- Rainbow Tables
- Diccionario
- Fuerza bruta
- Ataques híbridos
- Colisiones
- Downgrade
- Replay
- Implementaciones débiles



Ataques presentes en México durante el 2018

- JS/CoinMiner
- SMB/Exploit.DoublePulsar.B
- HTML/ScrInject.B
- LNK/Agent.DV
- Neurevt
- Win32/Emotet
- FileCoder
- Crysis, TeslaCrypt, CryptoWall, WannaCry y GandCrab.

► Enlace



Tipos de actores I

- **Wannabe lamer:** "I wanna be a hacker but I can't 'hack' it" (9-8 años / Grupo / Usuario Final / Diversión)
- **Script-kiddie:** The script kid (10-18 años / Grupo / Organizaciones con vulnerabilidad bien conocidas / Fama)
- **Hacker:** El hacker "por excelencia" (15-50 años / Solo (rara vez en grupo)/ Organizaciones de gran tamaño / Curiosidad, Aprender, Mejorar habilidades)
- **Cracker:** The destroyer (17-35 años / Solo / Empresas / Fama, Reconocimiento)
- **Hacktivista:** Idealistas (16-35 años / Grupo / Gobierno, Figuras públicas / Desprestigio)
- Crimen organizado.
 - **Black Hat Hacker:** Hackers que buscan beneficio económico a través de actividades ilícitas. (18-45 años / Solo o en Grupo Delitos/ Dinero)



Tipos de actores II

- Naciones / APT.
 - **Agente del gobierno:** Hacker que trabaja para el gobierno(CIA, Mossad, FBI,) (25-45 años / Solo o en Grupo / Terroristas, prófugos, industrias / Actividad profesional)
 - **Hacker militar:** Reclutados para combatir “con una computadora” (25-45 años / Solo o en Grupo (rara vez en grupo)/ Gobiernos e Industria / Actividad profesional y por una causa)
- **Competidores:** El espía industrial (22-50 años / Solo / Empresas multinacionales/ Lucro)
- **Empleados.**



Definición

- 1 *Tradicionalmente*, se dice de quien goza averiguando los detalles de sistemas de cómputo y cómo llevarlos a su límite, en contraposición a la mayoría de los usuarios que prefieren sólo aprender lo necesario.¹⁸
- 2 *En la actualidad*, se dice de quien de forma malintencionada penetra un sistema informático para obtener algún beneficio.
 - También conocidos como *crackers*.
 - Motivados por lucro, protesta, o por el desafío.

Hackers famosos: [▶ Enlace](#)

- Kevin Mitnick, Anonymous, Adrian Lamo, Albert González, Jeanson James Ancheta, Michael Calce, Kevin Poulsen, Jonathan James, ASTRA, Matthew Bevan y Richard Pryce.

¹⁸ <http://searchsecurity.techtarget.com/definition/hacker>



Kevin Mitnick - “Condor” -



<http://www.kevinmitnick.com/>

Se le considera el padre de los hackers y fue el primero en aparecer inmortalizado como hombre más buscado por el FBI. Su historial arranca en los ochenta cuando robaba manuales de hardware y culmina en 1995 cuando es detenido por el FBI gracias al contra-hacker Tsutomu Shimomura.

- **Ataques:**

- 20.000 números de tarjetas de crédito,
- mando central aéreo,
- Centrales telefónicas en California y
- Móviles de Motorola y Qualcomm.



Hackers más buscados por el FBI

Cyber's Most Wanted

Select the images of suspects to display more information.

Search for Filter by

Sort by:

Results: 69 items



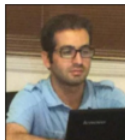
GOZNYM SUBJECTS



FUJIE WANG



IRGC-AFFILIATED CYBER ACTORS



MOJTABA MASOUMPOUR



BEHZAD MESRI



HOSSEIN PARVAR



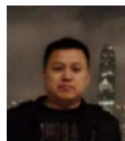
MOHAMAD PARYAR



APT 10 GROUP



ZHANG SHILONG



ZHU HUA

Figura: “Hackers más buscados por el FBI”

(Imagen tomada del Portal del FBI)



Clasificación de los actores

- Internos / Externos.
- Nivel de sofisticación.
- Recursos / Financiamiento.
- Intención y Motivación.












Actores clasificados por Intención y Motivación

- 1 **Black-hats:** Muestran sus habilidades en informática rompiendo sistemas de seguridad de computadoras, colapsando servidores, entrando a zonas restringidas, infectando redes o apoderándose de ellas, entre otras muchas cosas utilizando sus destrezas en métodos hacking.
- 2 **Grey-hats:** Grupo de individuos que en ocasiones penetran sistema sin permiso y otras con permiso.
- 3 **White-hats:** Se dedican a asegurar y proteger los sistemas de Tecnologías de información y comunicación. Suelen trabajar para empresas de seguridad informática.



Convención de nombres de los adversarios

Adversary		Category or Nation-State
	SPIDER	ECRIME
	CHOLLIMA	DEMOCRATIC PEOPLE'S REPUBLIC OF KOREA (NORTH KOREA)
	JACKAL	HACKTIVIST
	TIGER	INDIA
	KITTEN	IRAN

	LEOPARD	PAKISTAN
	PANDA	PEOPLE'S REPUBLIC OF CHINA
	BEAR	RUSSIAN FEDERATION
	CRANE	SOUTH KOREA
	BUFFALO	VIETNAM

<https://crowdstrike.lookbookhq.com/web-global-threat-report-2019/crowdstrike-2019-gtr>



Definición

Del inglés (*Open Source Intelligence* se refiere a procesar datos recopilados en fuentes abiertas o públicas (es decir que sean accesibles por cualquier ciudadano).

- **Medios de comunicacion:** periodicos, televisiones, radios, medios formales o informales.
- **Sitios Web:** contenido generado por usuarios, comunidades, foros, redes sociales.
- **Documentos Oficiales:** informes, estadisticas y datos oficiales, comunicados, presupuestos, boletines oficiales, contratos.
- **Profesional y academica:** conferencias, tesis, articulos y trabajos de expertos.
- **Otros recursos:** mapas, proyectos abiertos como Google Earth,



Algunas fuentes abiertas

- 1 Web archive:
 - <https://archive.org/>
- 2 Google dorks:
 - `site:twitter.com OR site:facebook.com`
`‘‘instagram.com/p/’’ ‘‘Nombre’’`
- 3 Twitter:
 - <https://twitterfall.com/>
 - <https://www.pscp.tv/>
- 4 Instagram
 - <https://www.instagram.com/explore/locations/>
- 5 Mapas:
 - <http://wikimapia.org>
- 6 Buscadores:
 - <https://www.shodan.io/>
 - <https://censys.io/>
- 7 Creación de identidades falsas para investigación:
 - <https://es.fakenamegenerator.com/advanced.php>
- 8 Herramientas: Maltego, Recon-ng, The Harvester, FOCA



- 1 Introducción a la Seguridad en Base de Datos
- 2 Identificación y prevención de vulnerabilidades**
- 3 Esquemas de acceso a servidores de bases de datos
- 4 Control de acceso y permisos
- 5 Auditoria a bases de datos



Vulnerabilidad

Definición

Errores, fallas, **debilidades** o exposiciones interna de una aplicación, dispositivo del sistema o servicio que podría conducir a un error de confidencialidad, integridad o disponibilidad[2].

Algunos ejemplos:

- Zero day.
- Condición de competencia.
- Vulnerabilidades en los sistemas.
- Manejo inadecuado de cadenas de entrada.
- Manejo inadecuado de mensajes de error.
- Inadecuada o mala configuración.
- Configuración por defecto.
- Consumo de recursos (Resource Exhaustion)
- Usuario no capacitados.
- Cuentas de usuario mal configuradas.
- Procesos de negocio vulnerables.
- Implementación o algoritmos criptográficos débiles.
- Vulnerabilidades en Memoria/Buffer.



Zero day (Día cero)

Definición

Vulnerabilidades que son **nuevas** y por lo tanto desconocidas por la gente y el fabricante del producto y en consecuencia no hay disponible una actualización para corregir el problema.

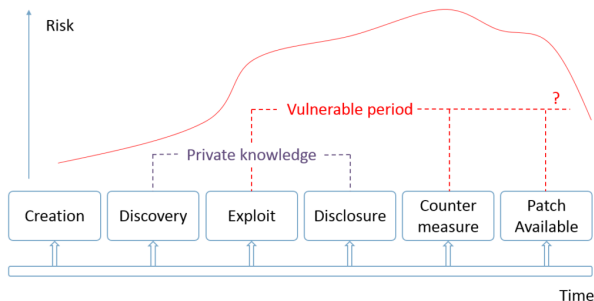


Figura: Ciclo de vida de una vulnerabilidad.

(Imagen tomada de: https://avleonov.com/wp-content/uploads/2018/11/vulnerability_life_cycle-1024x556.png)



Condición de competencia (Race condition)

Definición

Se produce en situaciones de concurrencia cuando varios procesos compiten por los recursos que proporciona el sistema operativo. Por ejemplo las variables, cambiando su estado y obteniendo de esta forma un valor no esperado de la misma.

Servicing stack update for Windows 10, Version 1903: July 9, 2019

Applies to: Windows 10, version 1903

Summary

This update makes quality improvements to the servicing stack, which is the component that installs Windows updates. Key changes include:

- Addresses an issue with a Secure Boot feature update that may cause BitLocker to go into recovery mode because of a race condition.



Vulnerabilidades en los sistemas

Las vulnerabilidades que afectan a los sistemas pueden ocurrir por alguno de los siguientes factores:

- Fin de vida de los sistemas (End of Life).
- Sistemas embebidos.
- Falta de soporte del fabricante.



Configuración por defecto (Default configuracion)

Definición

Configuración **base o inicial** de algún componete de un sistema informático.

Impacto:

- Hackean los datos de más de **100 millones de clientes** del banco Capital One. [▶ Enlace](#) [▶ Enlace](#) [▶ Enlace](#)

Dear Mr. Bezos:

I write to better understand how default configuration settings for Amazon's cloud computing products may have contributed to recent data breaches of servers used by Capital One Financial Corporation ("Capital One") and several other large organizations.

On July 29, Capital One revealed that its systems had been breached, and that personal data on 100 million Americans had been stolen. A criminal complaint filed by the Federal Bureau of Investigation (FBI) alleged that, due to a firewall misconfiguration, a hacker was able to access sensitive data stored on servers rented by Capital One from a cloud computing company. While



Pruebas de seguridad

Definición

Conjunto de pruebas destinadas a evidenciar las deficiencias existentes en materia de seguridad informática.[2]

Una prueba de seguridad únicamente valida la existencia de vulnerabilidades, pero nunca garantiza su inexistencia.

¿Qué es lo que se prueba?

- 1 **Servicio:** Defectos o insuficiencias en su codificación que permitan a un usuario malintencionado afectar a alguna dimensión de la seguridad.
- 2 **Configuración:** Defectos o insuficiencias en la configuración de la infraestructura de IT que sustenta el servicio que puedan ser utilizadas para afectar a alguna dimensión de la seguridad.
- 3 **Medidas de seguridad:** Eficacia y madurez de las medidas de seguridad desplegadas para garantizar la seguridad de un servicio de IT.



Tipos de prueba de seguridad

Escaneo de vulnerabilidades

Tipo de prueba destinada a elaborar una lista lo más amplia y completa que sea posible de las vulnerabilidades existentes en un sistema, priorizadas por nivel de impacto y con recomendaciones para su corrección.

Prueba de penetración

Tipo de prueba que tiene como finalidad la consecución de un objetivo prefijado con anterioridad, como conseguir privilegios de superusuario en una base de datos, acceso a una red interna, ...



Diferencia entre pruebas de seguridad

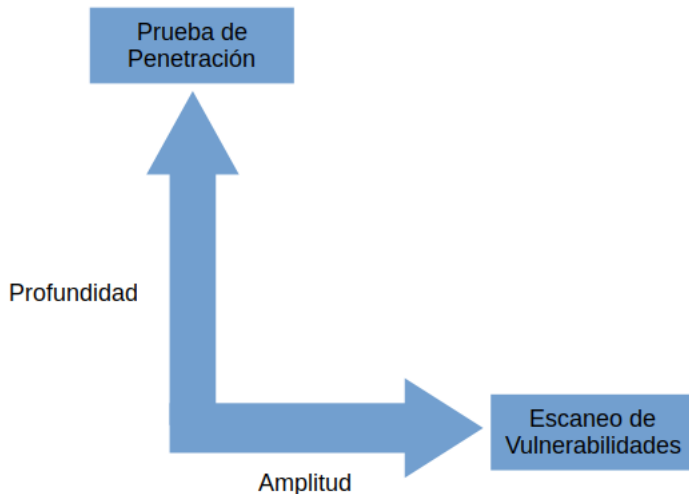


Figura: “Diferencia entre las pruebas de seguridad.”

(Elaboración propia.)



Clasificación Escaneo de vulnerabilidades

Por **nivel de automatización**:

- Automatizadas (Nessus, OpenVAS, OWASP ZAP).
- Semiautomatizadas (nmap, BrupSuite).

Por **Conocimiento y privilegios en el sistema de información**.

- Caja negra (Black box testing).
- Caja gris (Grey box testing).
- Caja blanca (White box testing).



Pruebas de penetración (PenTest)

Definición

Prueba de seguridad en la cual, los evaluadores simulan ataques reales en un intento de identificar modos de evadir los controles de seguridad de una aplicación, sistema o red de datos. Las pruebas de penetración requieren la simulación de ataques y datos reales en sistemas, empleando las mismas técnicas y herramientas utilizadas por los atacantes, buscando lograr el objetivo previamente establecido. [▶ Enlace](#)

Metodologías:

- **ISSAF**
- **NIST SP 800-115**
- **OSSTMM**
- **PTES**
- **OWASP**



Metodología de un PenTest

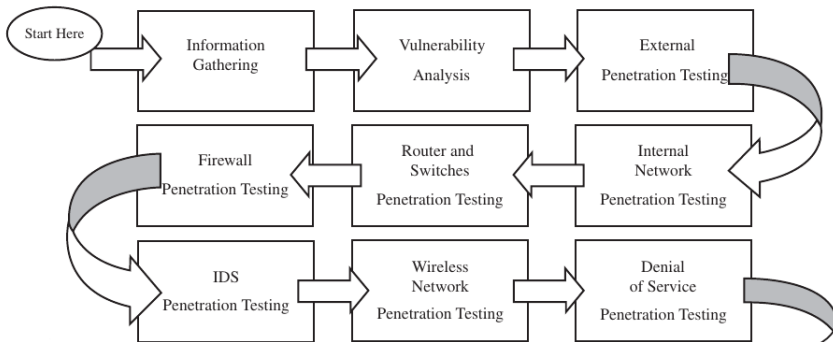


Figura: "Metodología típica de una prueba de penetración"

(EC-Council)



Metodología para una prueba de penetración(cont.

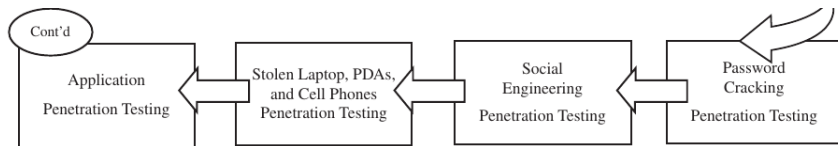


Figura: “Metodología típica de una prueba de pentración”

(EC-Council)



Metodología de un PenTest (cont.)

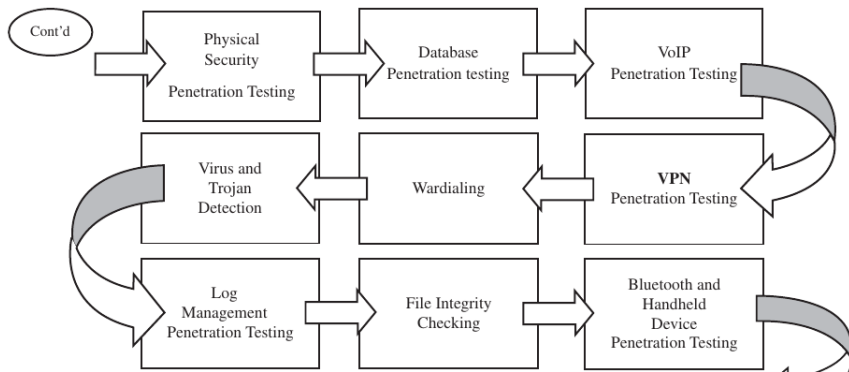


Figura: “Metodología típica de una prueba de penetración”

(EC-Council)



Metodología de un PenTest (cont.)

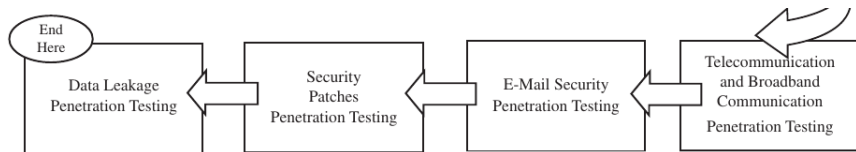


Figura: “Metodología típica de una prueba de penetración”

(EC-Council)



Distribuciones GNU/Linux para PenTest

- 1 Kali Linux
- 2 Parrot Security OS
- 3 BackBox
- 4 Samurai Web Testing Framework
- 5 Pentoo Linux
- 6 DEFT Linux
- 7 Caine
- 8 Network Security Toolkit (NST)
- 9 BlackArch Linux
- 10 Bugtraq



Temario

- 1 Introducción a la Seguridad en Base de Datos
- 2 Identificación y prevención de vulnerabilidades
- 3 Esquemas de acceso a servidores de bases de datos**
- 4 Control de acceso y permisos
- 5 Auditoria a bases de datos

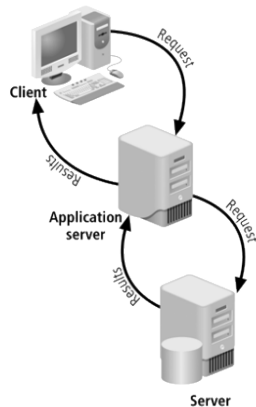
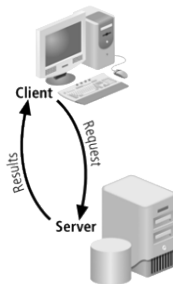


Arquitectura de Sistemas de Información

- Cliente-Servidor
 - Basado en un modelo de negocio
 - Puede ser implementado por niveles: un nivel; dos niveles; n niveles
 - Formado por tres capas (*layer*)
- *Capa*: Plataforma física o lógica
- Sistema manejador de bases de datos (DBMS): Conjunto de programas que administran bases de datos



Ejemplos de arquitectura cliente-servidor

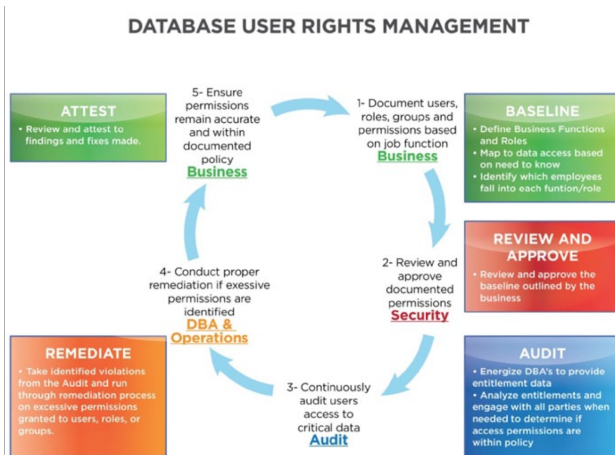


Temario

- 1 Introducción a la Seguridad en Base de Datos
- 2 Identificación y prevención de vulnerabilidades
- 3 Esquemas de acceso a servidores de bases de datos
- 4 Control de acceso y permisos**
- 5 Auditoria a bases de datos



Ciclo de vida en la administración de usuarios



Fuente: Pentest Magazine, p. 82, Septiembre 2012






Temario

- 1 Introducción a la Seguridad en Base de Datos
- 2 Identificación y prevención de vulnerabilidades
- 3 Esquemas de acceso a servidores de bases de datos
- 4 Control de acceso y permisos
- 5 Auditoria a bases de datos



Referencias bibliográficas

-  Comptia Security+ All-In-One Exam Guide, Fifth Edition (Exam Sy0-501)
-  FRANKLIN, J., C. WERGIN AND H. BOOTH CVSS implementation guidance. National Institute of Standards and Technology, NISTIR-7946, 2014.
-  MEDINA, J., Evaluación de Vulnerabilidades TIC. Guía práctica para el desarrollo de procesos básicos de evaluación y control de vulnerabilidades., 2014.

