



UADY

UNIVERSIDAD
AUTÓNOMA
DE YUCATÁN

Ciberseguridad para los negocios

Introducción a la ciberseguridad

Profesor: Wilberth de Jesús Pérez Segura
Correo: wilberth.perez@alumnos.uady.mx

Introducción

"Cuando no ocurre nada, nos quejamos de lo mucho que gastamos en seguridad. Cuando algo sucede, nos lamentamos de no haber invertido más... Más vale dedicar recursos a la seguridad que convertirse en una estadística."

Introducción

La **red de información electrónica** conectada se ha convertido en una parte integral de nuestra vida cotidiana. Todos los tipos de organizaciones, como instituciones médicas, financieras y educativas, utilizan esta red para **funcionar de manera eficaz**.

Los negocios utilizan la red para **recopilar, procesar, almacenar y compartir** grandes cantidades de información digital.

¿Qué debemos entender por Información?

Datos



A collection of irregularly shaped colored cards (blue, yellow, red) scattered across the page, containing various pieces of data:

- Blue card: María
- Yellow card: Pérez
- Red card: Cimé
- Blue card: Soltera
- Red card: Luis
- Yellow card: 23
- Blue card: 30
- Red card: A+
- Blue card: Soltero
- Red card: 43
- Blue card: Can
- Red card: Soltero
- Yellow card: Juan
- Red card: O+
- Yellow card: años

Información



A structured arrangement of colored cards (red, yellow, blue) in three columns, representing organized information:

Red Column	Yellow Column	Blue Column
	Juan	
	Pérez	
	30	
	años	
	Soltero	
	Sangre	
	A-	

La información

La información es el Activo más importante para las organizaciones después de las personas.



¿Dónde podemos encontrar activos de información?



La información la podemos encontrar en

[Nombre de la empresa]

[Calle]

[Ciudad, provincia y código postal]

Teléfono: (000) 000-0000

FACTURA

[Nombre]

[Nombre de la empresa]

[Calle]

[Ciudad, provincia y código postal]

[Teléfono]

[Dirección de correo electrónico]

DESCRIPCIÓN	CANT.	PRECIO UNITARIO	IMPORTE
-------------	-------	-----------------	---------

Tarifa del servicio 1 200,00 200,00

Mano de obra: 5 horas a 75 € la hora 5 75,00 375,00

Descuento de cliente nuevo - 50,00 - 50,00

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

- - - - -

La información se transmite a través de:



**La red interna
de la empresa**



**La red pública
de Internet**

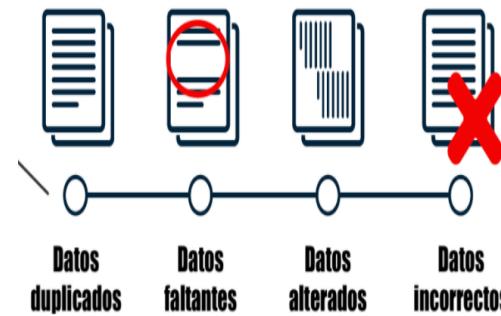
Impacto de ataques hacia la Seguridad de la Información

- Pérdida financiera
- Pérdida en la confidencialidad e integridad
- Pérdida en la reputación
- Pérdida en la relación con los clientes
- Problemas legales
- Impacto en la operación

El manejo de información debe considerar:



Confidencialidad



Integridad



Disponibilidad

Riesgos de la información

Los riesgos de la información pueden estar inherentes al Personal, a las prácticas organizacionales, a aspectos físicos (como edificios, Centros de Datos, etc) a controles de acceso, comunicaciones, administración operativa, computo móvil adquisición HW y/o SW entre otros y del cual se requiere una adecuada administración.



Amenazas

Causa potencial de un incidente no deseado, que pueda resultar en un daño a una organización o sistema.

Es la fuente del riesgo, con posibilidad de atacar.

Tipos

- Daño físico
- Evento natural
- Alteración por radiación
- Fallos en servicios básicos
- Fallos técnicos
- Afectación en la información
- Acciones no autorizadas
- Afectación en las funciones

Orígenes

- Accidental (acción humana no intencionada)
- Deliberado (acción humana intencionada)
- Ambiental (acción no humana)



Vulnerabilidad

- Debilidad de un activo (o control) que puede ser explotado por una amenaza.

Impacto

- Cambio adverso a los objetivos de negocio.
- Consecuencia del riesgo al sistema o organización.
- Expresado en términos de:



Riesgo, vulnerabilidad, amenaza



Panorama de los Riesgos Mundiales en 2020



Fuente: <https://es.weforum.org/reports/the-global-risks-report-2020>

¿Qué es la ciberseguridad?

La ciberseguridad es el **esfuerzo constante por proteger** estos sistemas de red y todos los datos contra el uso no autorizado o los daños.



Actividad Grupal: Ciberataques

Con apoyo de las fuentes de información proporcionadas por el profesor, el alumno realiza una investigación de sobre ciberataques realizados en los últimos 10 años y posteriormente en equipos deberán realizar una presentación en Power Point respondiendo las siguientes preguntas:

- ¿Qué entiendo por el concepto de ciberataque?
- ¿De que trata el ejemplo de ciberataque? ¿Cómo se realizó el ataque?
¿Quiénes son los afectados y cual fue el impacto?
- ¿Antes de la investigación realizada, qué no sabía sobre los conceptos de ciberseguridad y ciberataque?

Ligas de referencia:

<https://www.proceso.com.mx/346707/stuxnet-la-filtracion-de-un-ciberataque>

<https://www.eleconomista.com.mx/tecnologia/5-datos-sobre-el-ataque-a-Dyn-que-colapsó-Internet-20161021-0064.html>

<https://juncotic.com/heartbleed-una-explicacion-y-su-solucion/>

<https://www.20minutos.es/noticia/3035496/0/telefonica-ataque-informatico/>

<https://www.elperiodico.com/es/sociedad/20211011/ataque-informatico-universitat-autonoma-barcelona-12219123>

Niveles de Ciberseguridad

A nivel personal, debe proteger su identidad, sus datos y sus dispositivos informáticos.



A nivel corporativo, es responsabilidad de todos proteger la reputación, los datos y los clientes de la organización.

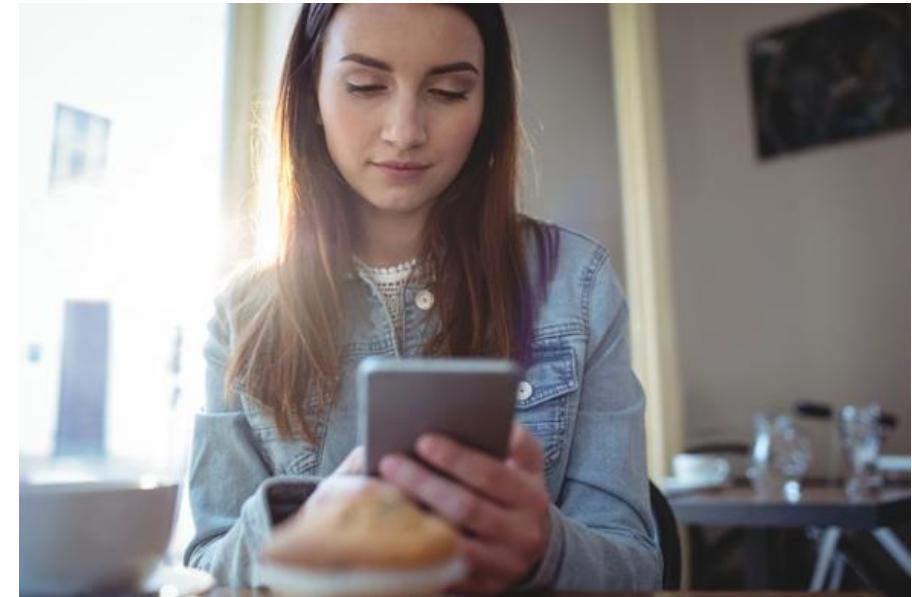


A nivel del estado, la seguridad nacional, y la seguridad y el bienestar de los ciudadanos están en juego.



Personas con secuestro de información

- Un hacker configuró una zona de cobertura inalámbrica abierta y "no autorizada" que se hacía pasar por una red inalámbrica legítima.
- Un cliente inició sesión en el sitio web de su banco.
- El hacker había secuestrado su sesión.
- El hacker obtuvo acceso a sus cuentas bancarias.



Empresas a las que se piden rescates

- Un empleado recibió un correo electrónico de parte de su director ejecutivo con un PDF adjunto.
- Ransomware está instalado en la computadora del empleado.
- Ransomware recopila y cifra datos corporativos.
- Los atacantes conservaron los datos de la empresa para el rescate hasta que se les pagó



Países objetivo

Gusano Stuxnet

- Se infiltró en sistemas operativos de Windows.
- Se destinó al software Step 7 que regula los controladores lógicos programables (PLC) para dañar las centrifugadoras en establecimientos nucleares.
- Se transmitió de las unidades USB infectadas a los PLC y, finalmente, dañó muchas de las centrifugadoras.



Este grupo de delincuentes penetran en las computadoras o redes para obtener acceso por varios motivos. La intención por la que interrumpen determina la clasificación de estos atacantes como delincuentes de sombrero blanco, gris o negro.

Hackers de sombrero blanco



Hackers de sombrero gris



Hackers de sombrero negro



Hackers de sombrero negro

Son delincuentes poco éticos que violan la seguridad de una computadora y una red para beneficio personal o por motivos maliciosos, como ataques a la red. Los hackers de sombrero negro atacan las vulnerabilidades para comprometer la computadora y los sistemas de red.

Hackers de estado

Estos hackers incluyen organizaciones de delincuentes informáticos, hacktivistas, terroristas y hackers patrocinados por el estado. Los delincuentes ciberneticos generalmente son grupos de delincuentes profesionales centrados en el control, la energía y la riqueza. Los delincuentes son muy sofisticados y organizados, e incluso pueden proporcionar el delito cibernetico como un servicio.

Actores maliciosos (Aficionados)

- Se los conoce como script kiddies.
- Tienen poca o ninguna habilidad.
- Utilizan herramientas ya existentes o instrucciones que encuentran en Internet para iniciar ataques.



Actores maliciosos (Hacktivistas)

Protestan frente a organizaciones o gobiernos

- Publican artículos y videos.
- Filtran información.
- Interrumpen los servicios web con ataques DDoS.



HACKER PROFILES:

THE BAD GUYS BEHIND THE LATEST
CYBER SECURITY ATTACKS



¿Qué tipo de perfil tiene este personaje?



My Motives:
Disrupting the status quo, seeking virtual mischief and mayhem to make a point to the government and large corporations, freeing terrorists, vigilante-ism, "Doxing," cyber protest, anarchy, fun

My Boss:
Myself and what I believe

My Comrades:
4chan, Anonymous, LulzSec, AntiSec

HACKTIVIST

My Methods:
I use freely available skript kiddie tools to launch DDoS attacks or web application attacks to try to hijack a legitimate website or steal data

My Hero:
Guy Fawkes, the Face of Anonymous

hackers got a bigger piece of the pie

My Claims to Fame:
Project Chanology, Operation Payback, Arab Spring activities, Operation HBGary, Operation Ouroborus, Operation Sony, Operation Megaupload, just to name a few

¿Qué tipo de perfil tiene este personaje?



My Motives:
Identity theft, credit card information, extortion (via ransomware or DDoS), click-jacking, pirating software, monetizing computer data in any way possible

My Boss:
My financier, a traditional criminal organization that has decided to recruit tech savvy kids

My Comrades:
Other cyber criminals in the underground market, where we swap hacking kits

CYBER CRIMINAL

My Methods:
I prefer web-based drive-by downloads, spamming, click-jacking, installing ransomware and fakeware, and can even use my victims to attack others

My Hero:
Albert Gonzalez, who stole over 170 million credit and debit card numbers in two years

My Claims to Fame:
I recently completed a global bank heist, stealing about \$45 million from ATMs

¿Qué tipo de perfil tiene este personaje?



My Motives:
Obtaining intelligence from my foes, cyber espionage, stealing secrets from my adversaries, disrupting or damaging an enemy's military infrastructure, propaganda, distracting an enemy during a real attack

NATION STATE

My Methods:
Advanced persistent threats, zero day exploits, rootkit technology, strong encryption, and many evasion techniques. — I use malware customized for non-traditional computing systems

In the Aurora attacks of 2009, I introduced the watering hole attack and have targeted over 30 large companies including Google

My Hero:
UglyGorilla (real name: Jack Wang)

My Claims to Fame:
Google Aurora attacks, New York Times hack, and other classified security breaches

Actividad: identificar el color del sobrero

Instrucciones:

Marque con una X para indicar el tipo de hacker que mejor describe cada una de las siguientes características que se presentan en la siguiente tabla:

Actividad: identificar el color del sombrero

Características de un hacker

Sombrero blanco

Sombrero gris

Sombrero negro

Después de hackear las computadoras de ATM en forma remota con una PC portátil, trabajó con los fabricantes de ATM para resolver las vulnerabilidades de seguridad encontradas.

Desde mi PC portátil, transferí \$10 millones a mi cuenta bancaria con los números de cuenta y PIN de la víctima después de ver las grabaciones de las víctimas que ingresaban los números.

Mi trabajo es identificar las debilidades en el sistema informático de mi empresa.

Utilicé el malware para comprometer varios sistemas corporativos para robar la información de tarjetas de crédito y vendí esa información al mejor postor.

Durante mi investigación de ataques a la seguridad, encontré una vulnerabilidad en la seguridad en una red corporativa a la que puedo acceder.

Estoy trabajando con empresas de tecnología para resolver un defecto con DNS.



Instrucciones: ver el siguiente video y posteriormente responder las preguntas.

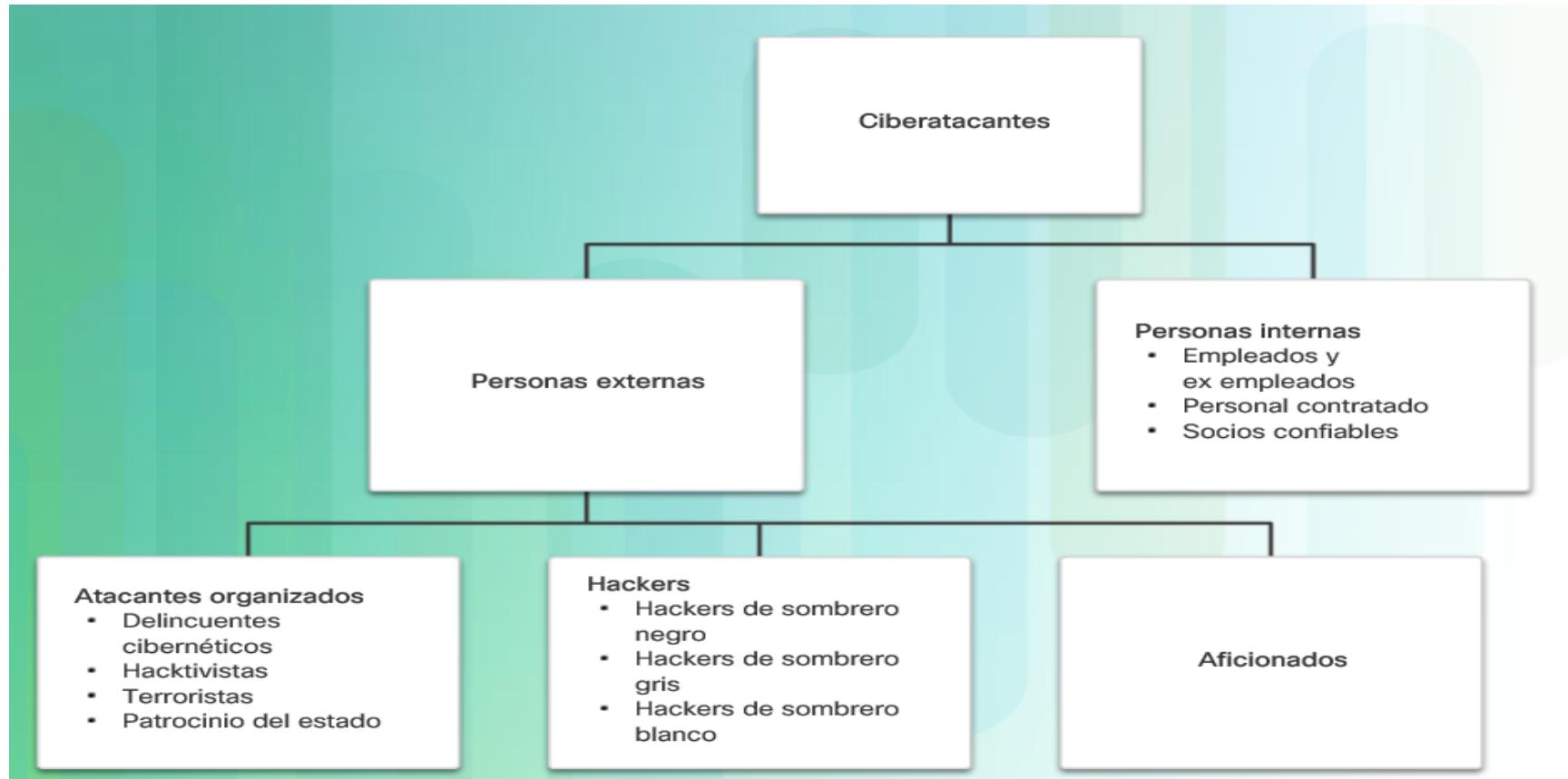
<https://www.youtube.com/watch?v=hqKafI7Amd8>

- a. ¿Cuál es una vulnerabilidad que se está atacando?
- b. ¿Qué datos o información puede obtener un hacker al atacar esta vulnerabilidad?
- c. ¿Cómo se realiza el ataque?
- d. ¿Qué fue lo que les interesó específicamente sobre este ataque?
- e. ¿Cómo creen que podría mitigarse este ataque en particular?

¿Quiénes son los actores maliciosos?



Amenazas internas y externas



Beneficios financieros

Gran parte de la actividad de los hackers es en busca de beneficios financieros.

Los delincuentes ciberneticos desean generar flujo de caja

- Cuentas bancarias
- Datos personales
- Algo más que pueden aprovechar



Secretos comerciales y política global

Los estados de una nación también están interesados en utilizar el ciberespacio.

- Hackeo a otros países
- Interferencia con la política interna
- Espionaje industrial
- Obtención de ventaja importante en el comercio internacional



Laboratorios: Casos de estudio de ciberseguridad y averiguar detalles de los ataques



Internet de las Cosas (IoT)

Con el surgimiento de la Internet de las cosas (IoT), hay muchos más datos para administrar y asegurar. La IoT es una gran red de objetos físicos, como sensores y equipos, que se extiende más allá de la red de computadoras tradicional. Todas estas conexiones, además del hecho de que hemos ampliado la capacidad y los servicios de almacenamiento a través de la nube y la virtualización, llevan al crecimiento exponencial de los datos.

Cuán segura es Internet de las cosas

Internet de las cosas (IdC)

- Cosas conectadas para mejorar la calidad de vida.
- Ejemplo: los rastreadores de actividad física

¿Qué grado de seguridad ofrecen estos dispositivos?

- Firmware
- Errores de seguridad
- Actualizable con parche

Ataque DDoS al proveedor de nombre del dominio, Dyn

- Perjudicó muchos sitios web.
- Las cámaras web, DVR, routers y otros dispositivos de IdC afectados formaron un botnet.
- El hacker controló el botnet que se usó para crear un ataque de DDoS que desactivó servicios esenciales de Internet.

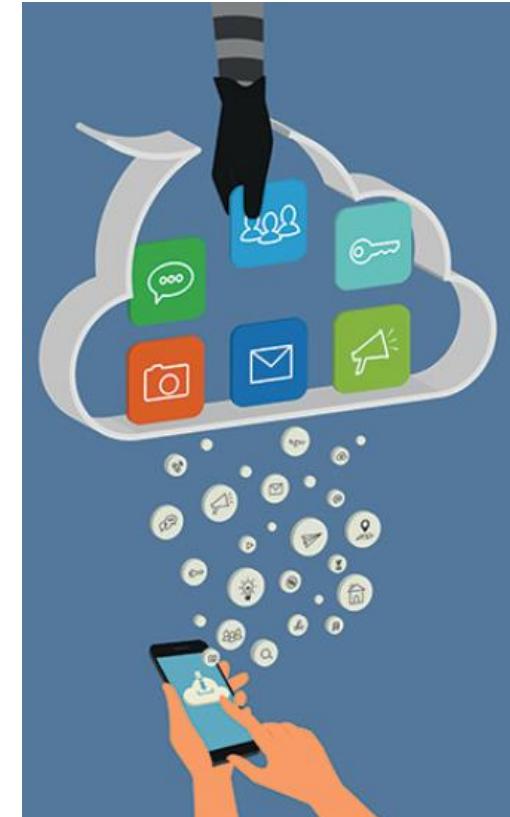


La información que permite identificar personas (Personally Identifiable Information, PII) es cualquier dato que pueda utilizarse para identificar inequívocamente a una persona.

- Ejemplos de PII incluyen: nombre, número de seguro social, fecha de nacimiento, números de tarjetas de crédito, números de cuenta bancaria, identificaciones emitidas por el gobierno, información de la dirección (calle, correo electrónico, números de teléfono).
- Esta información se vende a la Web oscura.
- Se crean cuentas falsas, como tarjetas de crédito y préstamos a corto plazo.

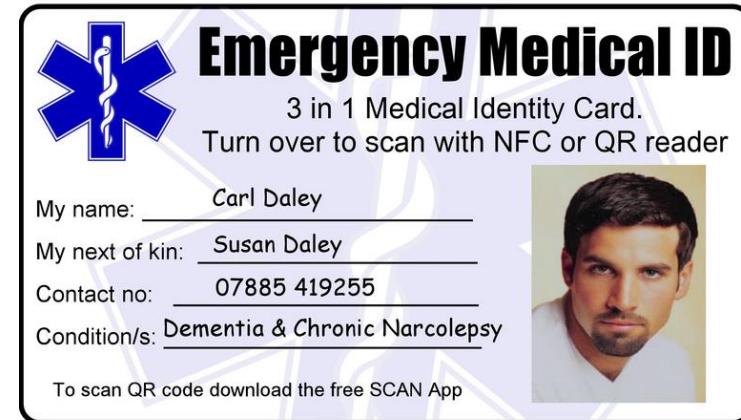
Información confidencial sobre la salud (PHI): un subconjunto de PII:

- crea y mantiene registros médicos electrónicos (EMR)
- Regulada por la Ley de Transferibilidad y Responsabilidad del Seguro Médico (HIPAA)



Identidad Digital (1/2)

A medida que pasa más tiempo en línea, su identidad, en línea y fuera de línea, puede afectar su vida.



Identidad fuera de línea: es la persona con la que sus amigos y familiares interactúan a diario en el hogar, la escuela o el trabajo. Conocen su información personal, como su nombre, edad, o dónde vive.

Identidad en línea: es quién es usted en el ciberespacio. Su identidad en línea es cómo se presenta ante otros en línea. Esta identidad en línea solo debería revelar una cantidad limitada de información sobre usted.

Clasificación de Datos Personales



Impacto: pérdida de la ventaja competitiva

Puede resultar en pérdida de la ventaja competitiva.

- Espionaje corporativo en el ciberespacio.
- Pérdida de confianza que surge cuando una empresa es incapaz de proteger los datos personales de sus clientes.



Impacto: Seguridad nacional y política

En 2016, un hacker publicó PII de 20 000 empleados del FBI y 9000 empleados del Departamento de Seguridad Nacional estadounidense.

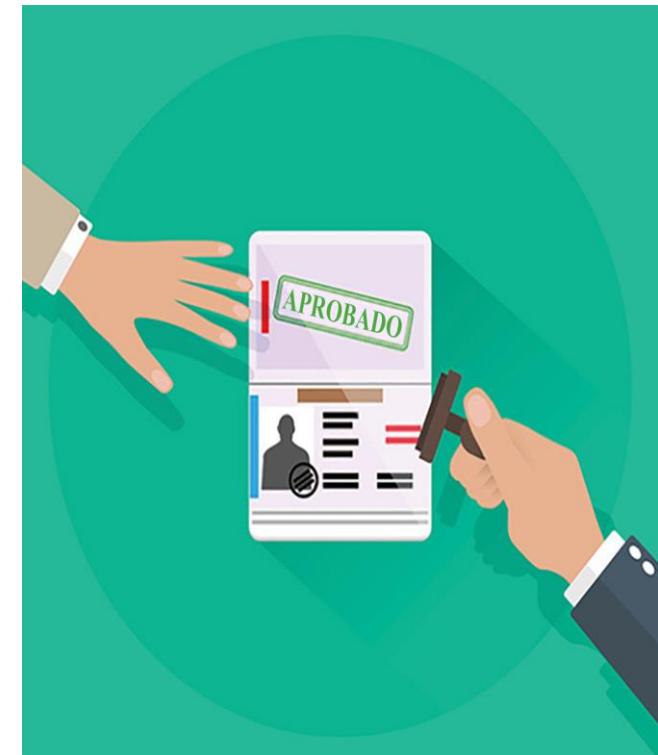
El gusano Stuxnet fue diseñado para impedir el progreso de Irán en el enriquecimiento de uranio.

- Es un ejemplo de un ataque a la red motivado por asuntos de seguridad nacional.

La ciberguerra es una posibilidad concreta.

Internet se ha tornado esencial como medio para actividades comerciales y financieras.

- La interrupción puede acabar con la economía de un país y la seguridad de sus ciudadanos.



¿Dónde están nuestros datos?



Actividad Individual

Laboratorio: Localizar sus datos personales

Contramedidas

Configurar opciones de privacidad de nuestras redes sociales y aplicaciones.

<https://www.welivesecurity.com/la-es/2011/06/29/guia-privacidad-facebook/>

Aplicar cifrado en las unidades de nuestro Disco Duro

<https://www.adslzone.net/2015/12/23/como-cifrar-nuestros-archivos-carpetas-o-unidades-de-disco-en-windows-10/>

Actividad Grupal: ¿Sabes donde están tus datos?

De manera grupal, llevar acabo una discusión sobre su día a día en el hogar , labores o vida personal e identificar cinco situaciones en las cuales se pudieran ver comprometidos sus datos personales.

Posteriormente cada equipo deberá exponer sus resultados y conclusiones en el aula.

Escenario 1: datos médicos

Cuando está en el consultorio médico, la conversación que tiene con el médico se registra en su expediente médico. Para fines de facturación, esta información se puede compartir con la empresa de seguros para garantizar la facturación y la calidad adecuadas. Ahora, una parte de su historial médico de la visita también se encuentra en la empresa de seguros.



Escenario 2: datos personales

Las tarjetas de fidelidad de la tienda pueden ser una manera conveniente de ahorrar dinero en sus compras. Sin embargo, la tienda compila un perfil de sus compras y utiliza esa información para su propio uso. El perfil muestra que un comprador compra cierta marca y sabor de crema dental regularmente. La tienda utiliza esta información para identificar como objetivo al comprador con ofertas especiales del partner de marketing.



Escenario 3: datos personales

Cuando comparte sus imágenes en línea con sus amigos, ¿sabe quién puede tener una copia de las imágenes? Las copias de las imágenes están en sus propios dispositivos. Sus amigos pueden tener copias de dichas imágenes descargadas en sus dispositivos. Si las imágenes se comparten públicamente, es posible que desconocidos tengan copias de ellas también. Podrían descargar dichas imágenes o realizar capturas de pantalla de dichas imágenes. Debido a que las imágenes se publicaron en línea, también se guardan en servidores ubicados en distintas partes del mundo. Ahora las imágenes ya no se encuentran solo en sus dispositivos informáticos.





Controles de acceso, monitoreo de servicios, bitácoras

Profesor: Wilberth de Jesús Pérez Segura
Correo: wilberth.perez@alumnos.uady.mx

¿Qué es un control?

- Representa todas las salvaguardas que se pueden colocar para proteger a un activo y hacerlo menos vulnerable a su entorno.
- Es un mecanismo de seguridad, prevención y corrección utilizado para disminuir la vulnerabilidad sobre un activo.

Algunos ejemplos de controles:

- CCTV
- Extintores
- Gafetes de acceso
- Plantas Eléctricas
- Detectores de humo/calor
- Pararrayos
- Escaleras de Emergencia



¿Qué es un vulnerabilidad?

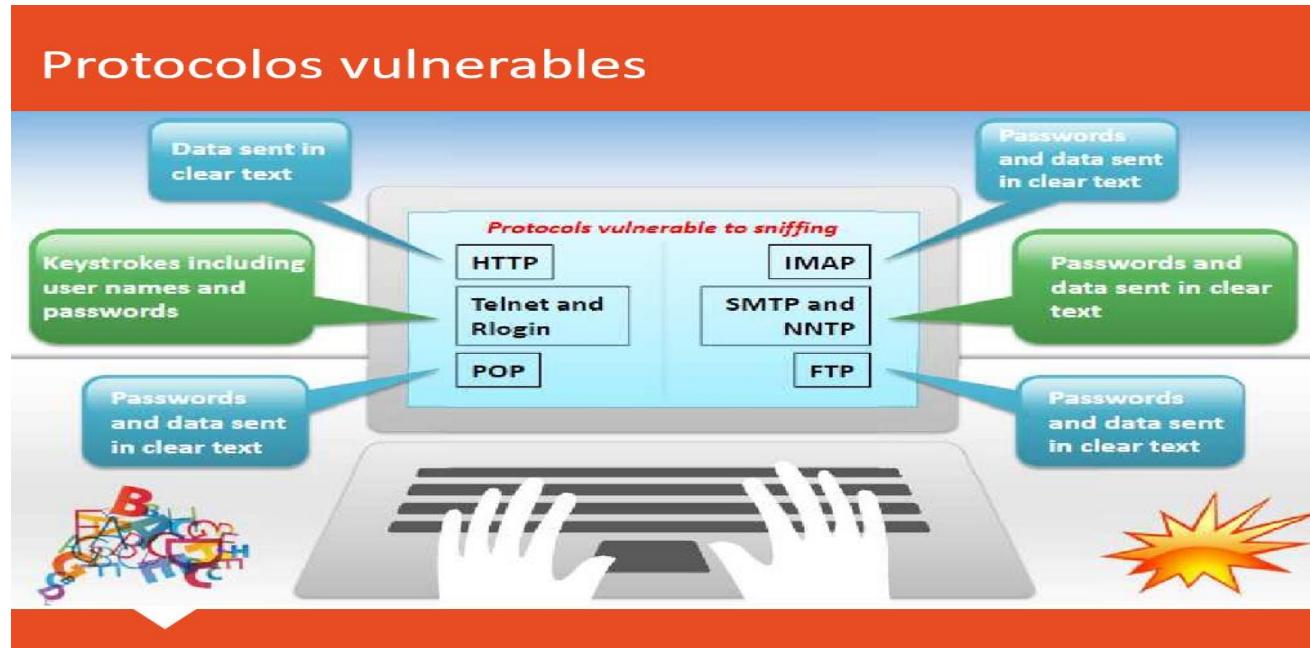
- Ausencia, capacidad insuficiente o carencia de un sistema de protección sobre un activo, a través del cual, una amenaza puede ocurrir más frecuentemente o con una mayor severidad o impacto.
- Son las características y circunstancias propias de un activo que lo hacen susceptible a los efectos dañinos de la materialización de una amenaza.
- Capacidad disminuida de un activo para hacer frente y resistir a los efectos de un peligro natural o causado por la actividad humana.



Identifica la vulnerabilidad



Ejemplos de vulnerabilidades



Referencias para búsqueda de vulnerabilidades

Common Vulnerability Scoring System (CVSS)

<https://nvd.nist.gov>

Common Vulnerability and Exposures (CVE)

<https://cve.mitre.org>

National Vulnerability Database (NVD)

<https://nvd.nist.gov>

Vulnerabilidades más comunes

Misconfiguration

Default Installations

Buffer Overflows

Unpatched Servers

Design Flaws

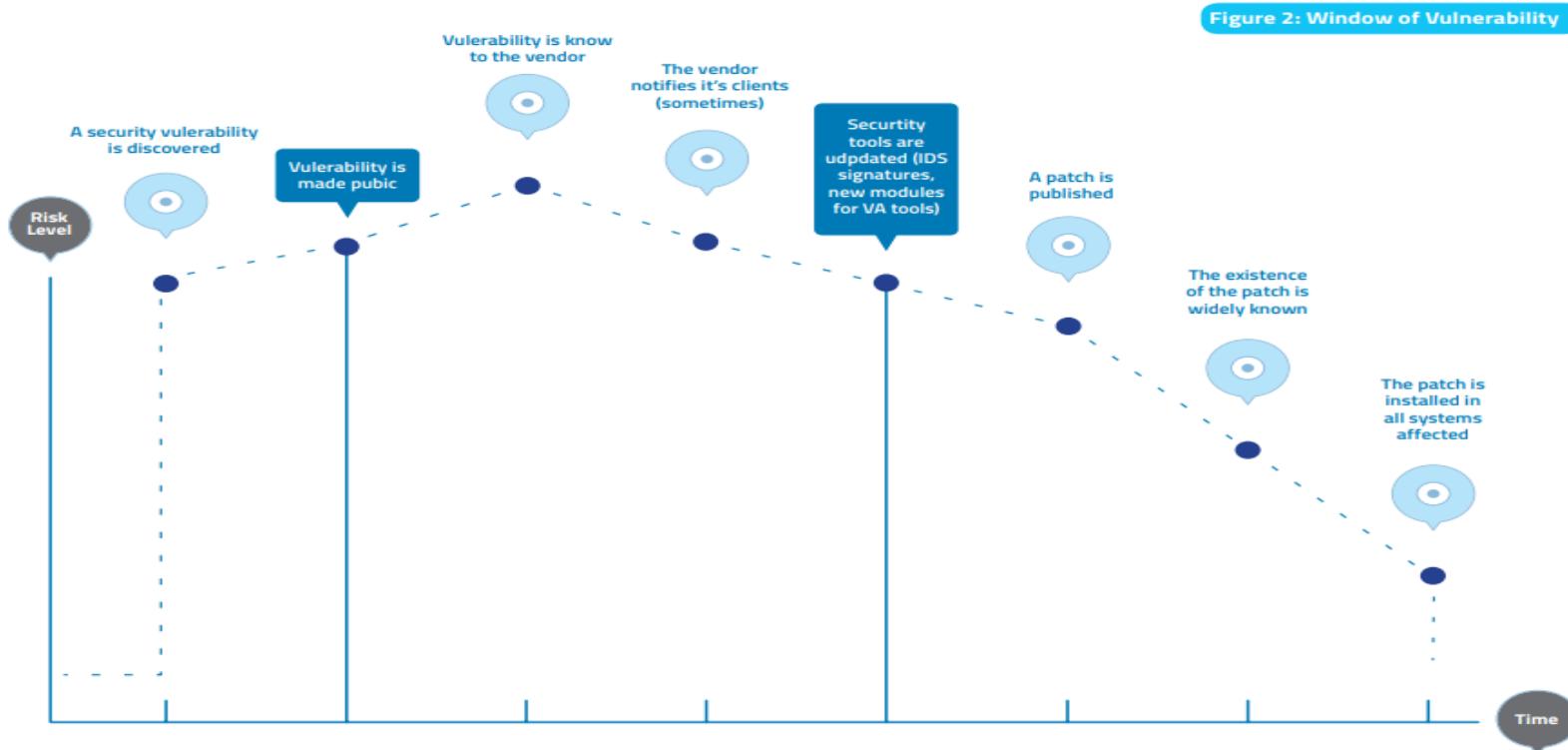
Operating Systems Flaws

Applications Flaws

Open Services

Default Passwords

Ciclo de vida de las vulnerabilidades



Necesidad de controles de seguridad

La información es el Activo más importante para las organizaciones después de las personas.



¿Dónde podemos encontrar la información?



Documentos en papel

Medios electrónicos de la empresa

Dispositivos personales

¿Cómo se transmite la información?



**La red interna
de la empresa**



**La red pública
de Internet**

Impacto al negocio por la falta de controles de seguridad

- Pérdida financiera
- Pérdida en la confidencialidad e integridad
- Pérdida en la reputación
- Pérdida en la relación con los clientes
- Problemas legales
- Impacto en la operación



Mecanismos de seguridad

Mecanismos administrativos

Mecanismos de control

Planes y políticas

Mecanismos administrativos

NAT

DMZ

Segmentación y VLAN

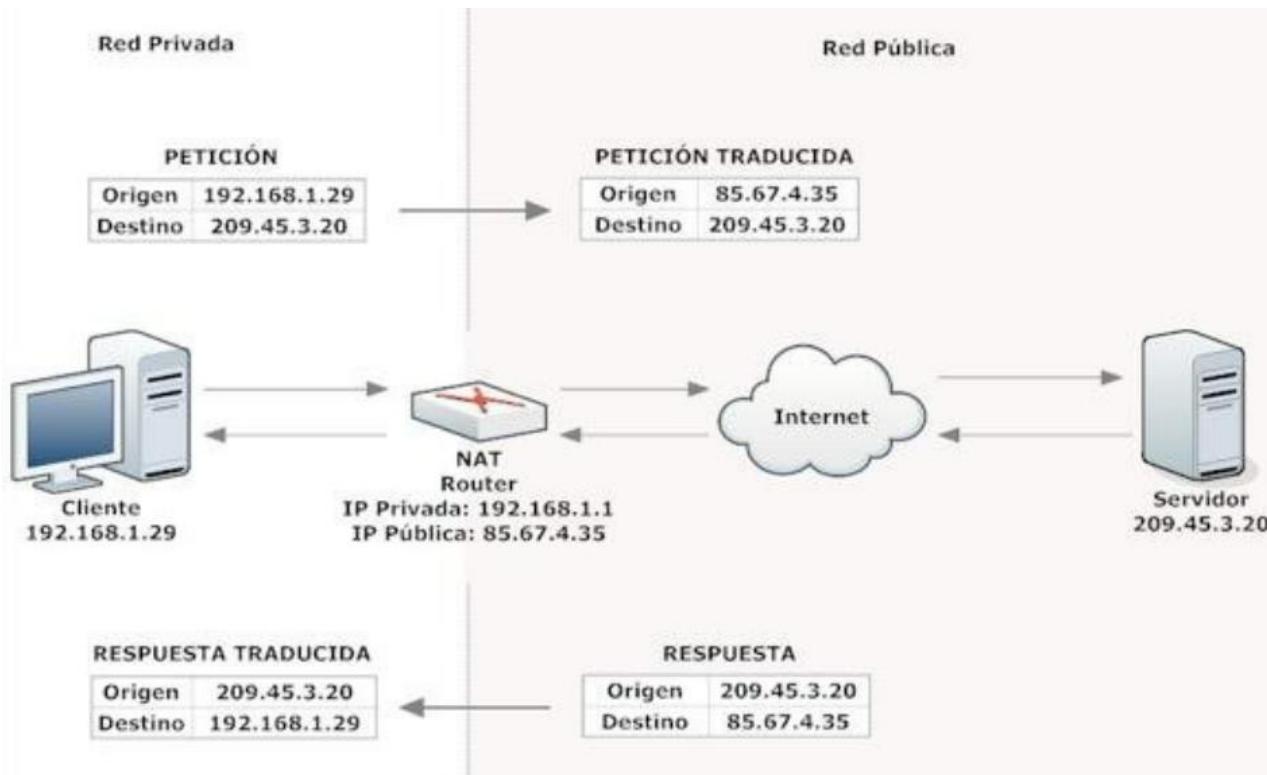
Port Security

Redundancia

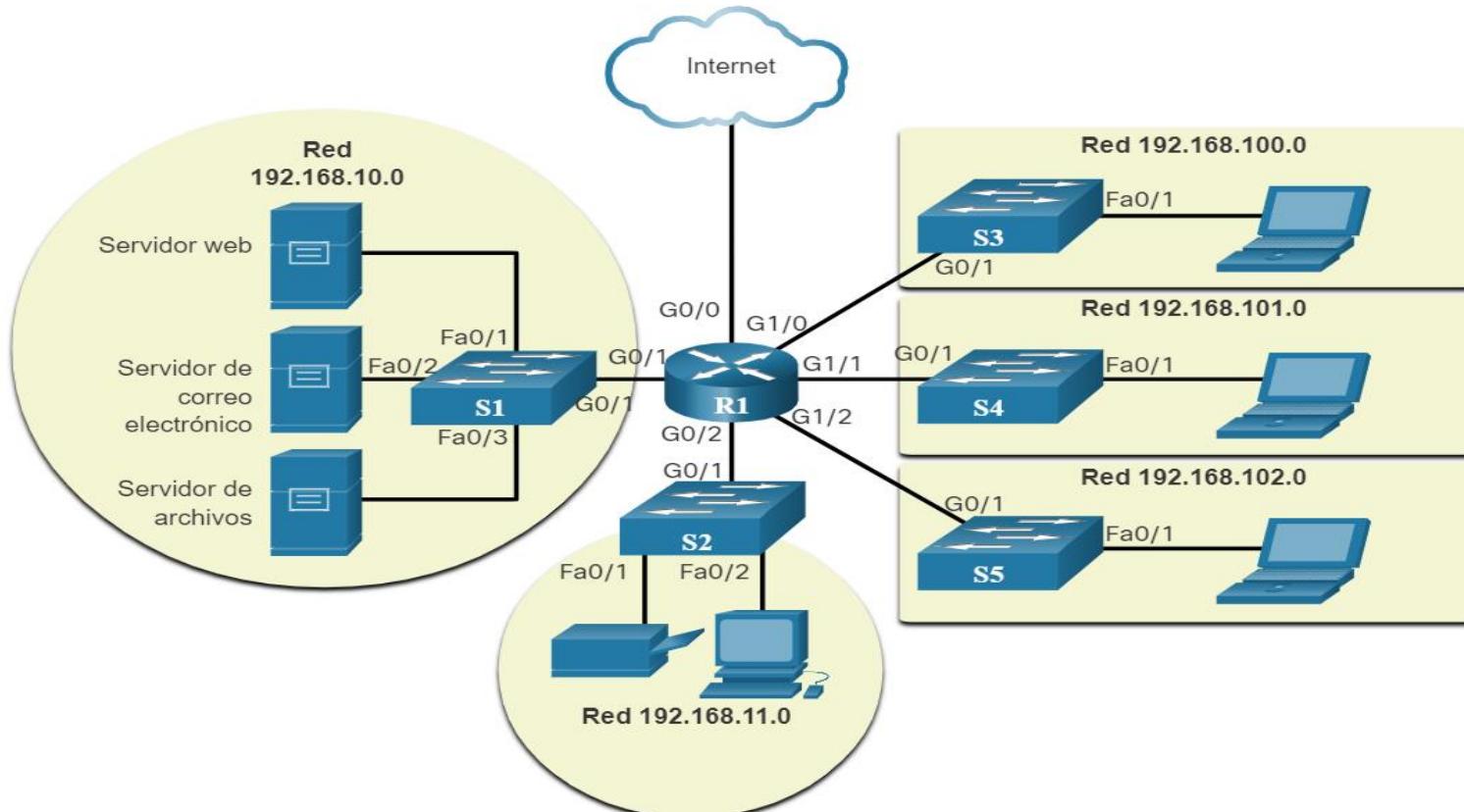
Cifrado

Listas de acceso

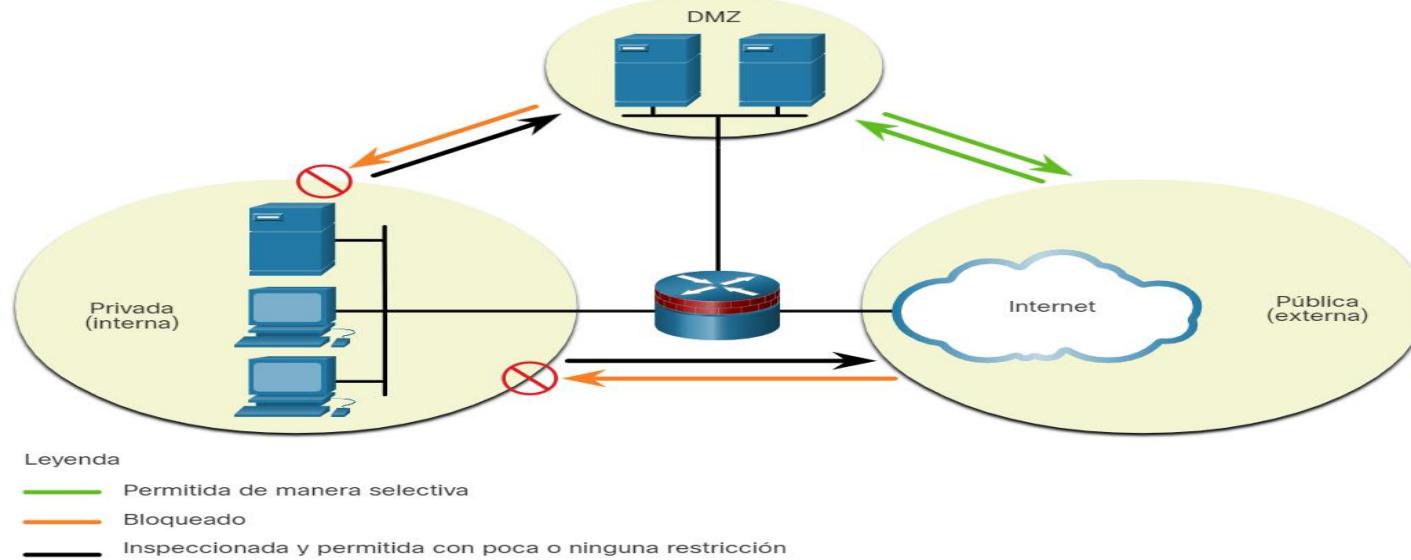
Network Address Translation (NAT)



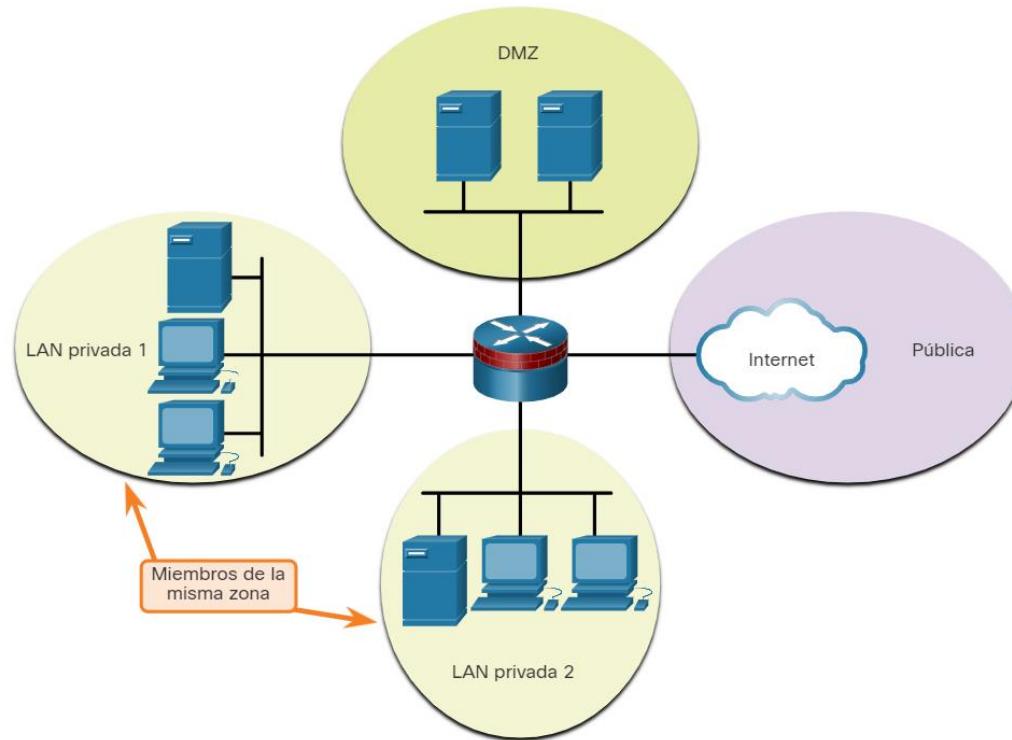
Arquitectura de seguridad DMZ



Una zona perimetral (DMZ, Demilitarized Zone) es un diseño de firewall donde, normalmente, hay una interfaz interna conectada a la red privada, una interfaz externa conectada a la red pública y una interfaz de DMZ.

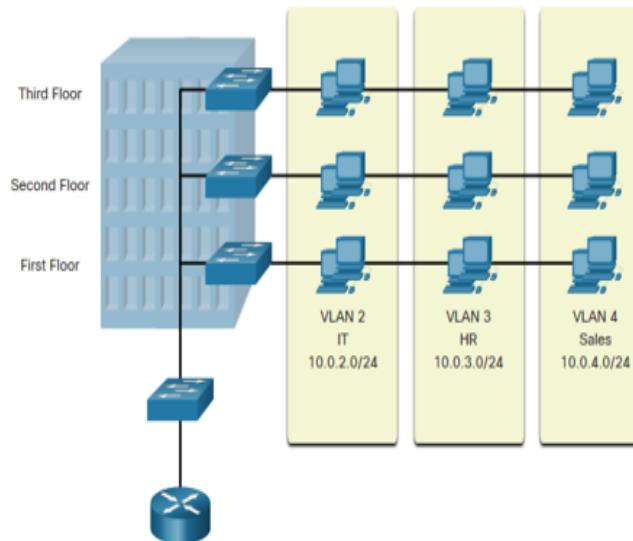


Zonas de seguridad



Segmentación y VLAN

Las VLAN son conexiones lógicas con otros dispositivos similares.



La colocación de dispositivos en varias VLAN tienen las siguientes características:

- Proporciona segmentación de los diversos grupos de dispositivos en los mismos switches
- Proporciona una organización más manejable
 - Difusiones, multidifusión y unidifusión se aíslan en la VLAN individual
 - Cada VLAN tendrá su propia gama única de direcciones IP
 - Dominios de difusión más pequeños

Beneficios de las VLANs

Beneficios	Descripción
Dominios de difusión más pequeños	Dividir la LAN reduce el número de dominios de difusión
Seguridad mejorada	Solo los usuarios de la misma VLAN pueden comunicarse juntos
Eficiencia de TI mejorada	Las VLAN pueden agrupar dispositivos con requisitos similares, por ejemplo, profesores frente a estudiantes
Reducción de costos	Un switch puede admitir varios grupos o VLAN
Mejor rendimiento	Los pequeños dominios de difusión reducen el tráfico y mejoran el ancho de banda
Gestión Simple	Grupos similares necesitarán aplicaciones similares y otros recursos de red

Tipos de VLAN

VLAN predeterminada

La VLAN 1 es la siguiente:

- La VLAN predeterminada
- La VLAN nativa predeterminada
- La VLAN de administración predeterminada
- No se puede eliminar ni cambiar el nombre

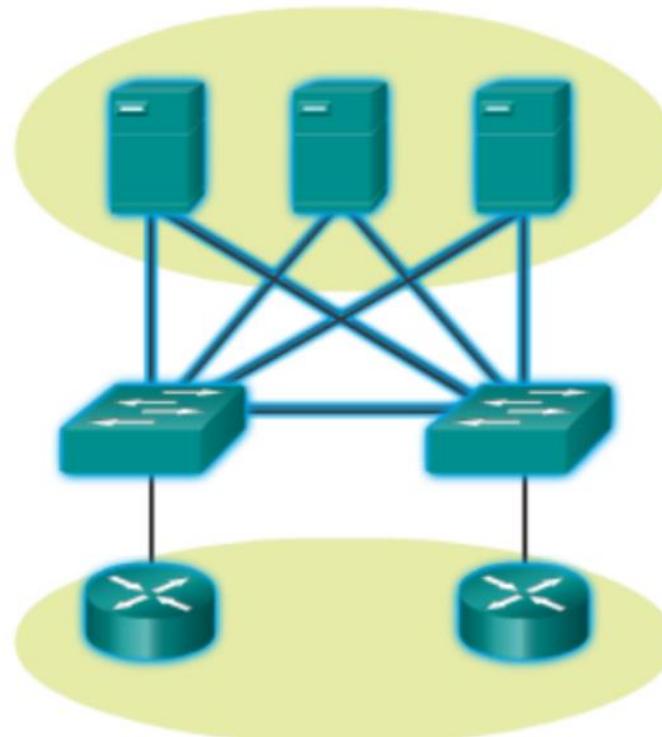
Switch# show vlan brief			
VLAN Name	Status	Ports	
1 default	active	Fa0/1, Fa0/2, Fa0/3, Fa0/4 Fa0/5, Fa0/6, Fa0/7, Fa0/8 Fa0/9, Fa0/10, Fa0/11, Fa0/12 Fa0/13, Fa0/14, Fa0/15, Fa0/16 Fa0/17, Fa0/18, Fa0/19, Fa0/20 Fa0/21, Fa0/22, Fa0/23, Fa0/24 Gi0/1, Gi0/2	
1002 fddi-default		act/unsup	
1003 token-ring-default		act/unsup	
1004 fddinet-default		act/unsup	
1005 trnet-default		act/unsup	

Port Security

El método más simple y eficaz para evitar ataques por saturación de la tabla de direcciones MAC es habilitar el port security.

- La seguridad de puertos limita la cantidad de direcciones MAC válidas permitidas en el puerto. Permite a un administrador configurar manualmente las direcciones MAC para un puerto o permitir que el switch aprenda dinámicamente un número limitado de direcciones MAC.

Redundancia



El cifrado tiene como finalidad ofuscar la información mediante técnicas criptográficas para así evitar que los datos sean legibles para aquellos que no conozcan la clave de descifrado. Este tipo de técnicas son una solución eficaz para el almacenamiento y transmisión de información sensible, especialmente a través de soportes y dispositivos móviles, ya que:

- permiten controlar el acceso a la información;
- limitan la difusión no autorizada en caso de pérdida o robo de dichos soportes.

La criptografía viene desde muchos años atrás...



¿Qué es un proceso de cifrado/descifrado?

A pair of algorithms. One for encryption (E) and the other for decryption (D)

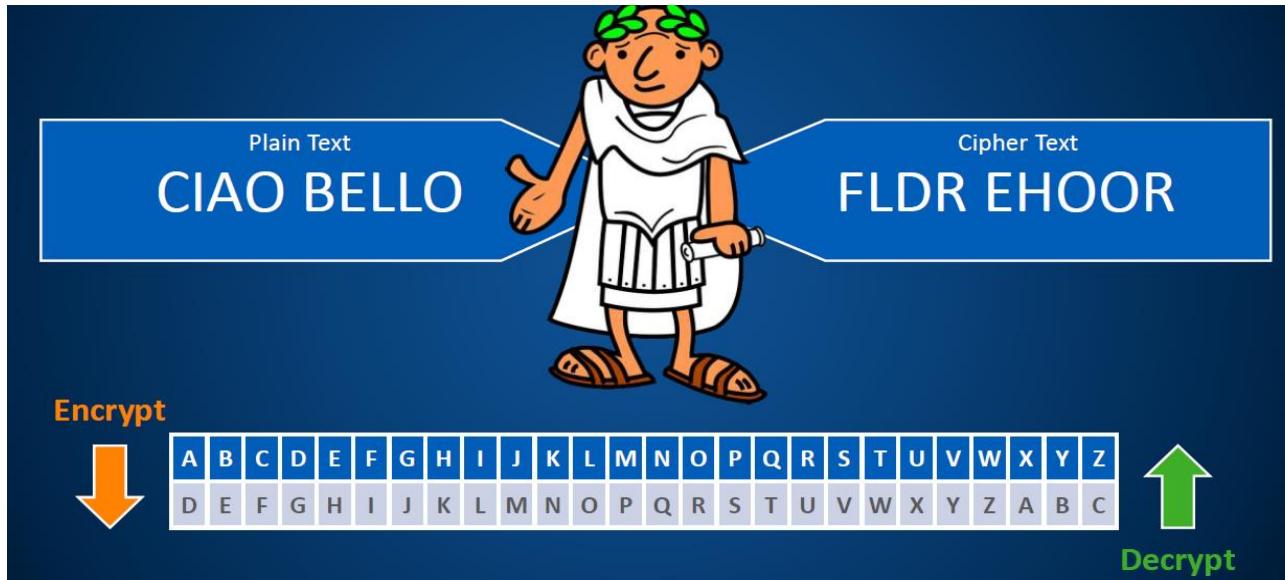
K = the key. M = the message. C = the ciphertext

Encrypting the message M with the key K produces the ciphertext C

Decrypting the ciphertext C with the key K reveals the message M

This can be shown as $E(K,M) = C$ and $D(K,C) = M$

Cifrado El Cesar



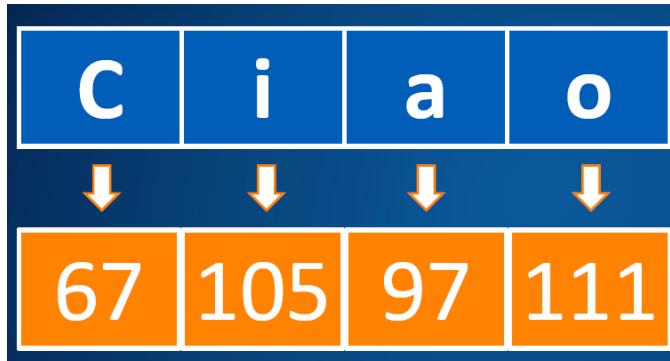
¿Cómo trabaja el cifrado/descifrado?

Substitución: cada carácter mantiene su posición pero cambia su identidad.

Transposición: cada carácter retiene su identidad pero cambia su posición.

Original	a	b	c	d	e	f	g	h	i	j	k	l	m
Cifrado	d	e	f	g	h	i	j	k	l	m	n	o	p
Original	n	o	p	q	r	s	t	u	v	w	x	y	z
Cifrado	q	r	s	t	u	v	w	x	y	z	a	b	c

Las computadoras usan otro lenguaje



ASCII printable characters			
65	A	97	a
66	B	98	b
67	C	99	c
68	D	100	d
69	E	101	e
70	F	102	f
71	G	103	g
72	H	104	h
73	I	105	i
74	J	106	j
75	K	107	k
76	L	108	l
77	M	109	m
78	N	110	n
79	O	111	o
80	P	112	p
81	Q	113	q
82	R	114	r
83	S	115	s
84	T	116	t
85	U	117	u
86	V	118	v
87	W	119	w
88	X	120	x
89	Y	121	y
90	Z	122	z

Lenguaje binario

67 | 105 | 97 | 111

128	64	32	16	8	4	2	1	=
1	1	1	1	1	1	1	1	255
0	1	0	0	0	0	1	1	67
0	1	1	0	1	0	0	1	105
0	1	1	0	0	0	0	1	97
0	1	1	0	1	1	1	1	111



Proceso de Cifrado



Propiedades del cifrado

Confusión: hacer que la relación entre el texto cifrado y la llave secreta sea lo más complejo posible. En otras palabras significa si aún el analista tiene múltiples muestras del textoplano-textocifrado usando una llave en particular, debe ser extremadamente difícil determinar la llave.

Difusión: Cada cambio que afecte a un simple carácter de entrada debería cambiar muchos caracteres de la salida. Esto tendrá el efecto de dispersar cualquier patrón de texto plano en varios textos cifrados haciendo más difícil la tarea del analista.

Accesos seguros SSH

SSH es un tipo de acceso remoto más seguro:

- Requiere un nombre de usuario y una contraseña.
- El nombre de usuario y la contraseña se pueden autenticar localmente.

El método de base de datos local tiene algunas limitaciones:

- Las cuentas de usuario deben configurarse localmente en cada dispositivo que no sea escalable.
- El método no proporciona ningún método de autenticación alternativa.

```
R1(config)# ip domain-name example.com
R1(config)# crypto key generate rsa general-keys modulus 2048
R1(config)# username Admin secret Str0ng3rPa55w0rd
R1(config)# ssh version 2
R1(config)# line vty 0 4
R1(config-line)# transport input ssh
R1(config-line)# login local
```

Lab - Configuración de Seguridad en el Switch

Topología

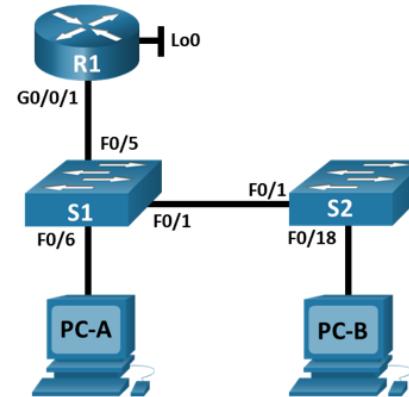


Tabla de Asignación de Direcciones

Dispositivos	Interface / VLAN	Dirección IP	Máscara de Subred
R1	G0/0/1	192.168.10.1	255.255.255.0
	Bucle invertido 0	10.10.1.1	255.255.255.0
S1	VLAN 10	192.168.10.201	255.255.255.0
S2	VLAN 10	192.168.10.202	255.255.255.0
PC – A	NIC	DHCP	255.255.255.0
PC – B	NIC	DHCP	255.255.255.0

Laboratorio - Configurar dispositivos de red con SSH

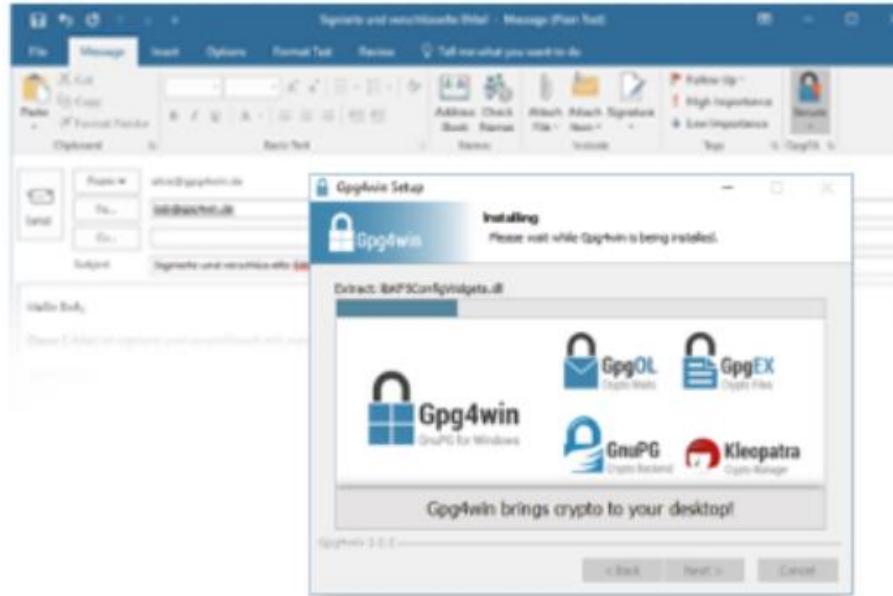
Topología



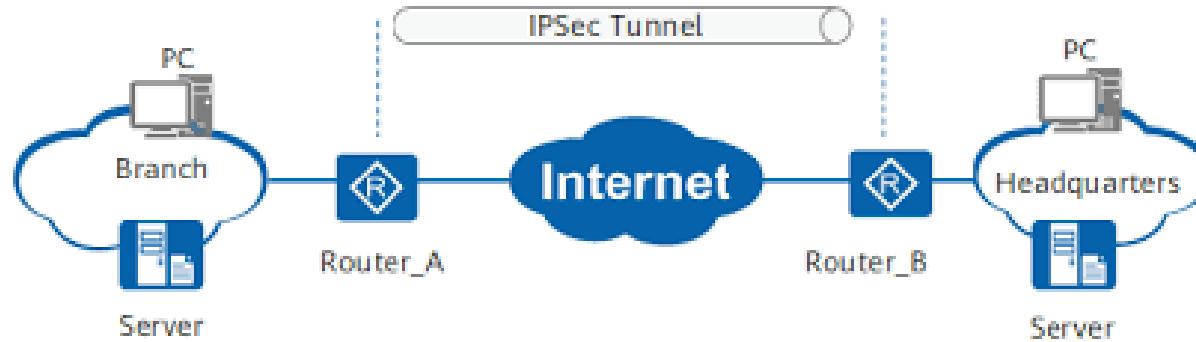
Tabla de asignación de direcciones

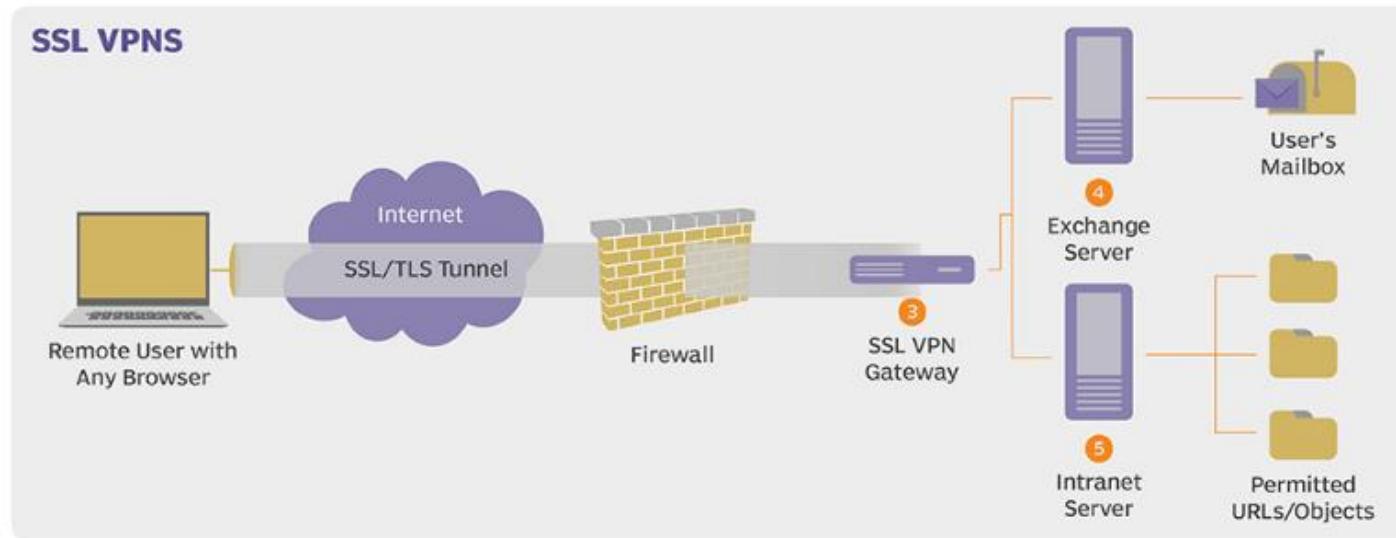
Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminado
R1	G0/0/1	192.168.1.1	255.255.255.0	N/D
S1	VLAN 1	192.168.1.11	255.255.255.0	192.168.1.1
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1

Cifrado de correos con PGP

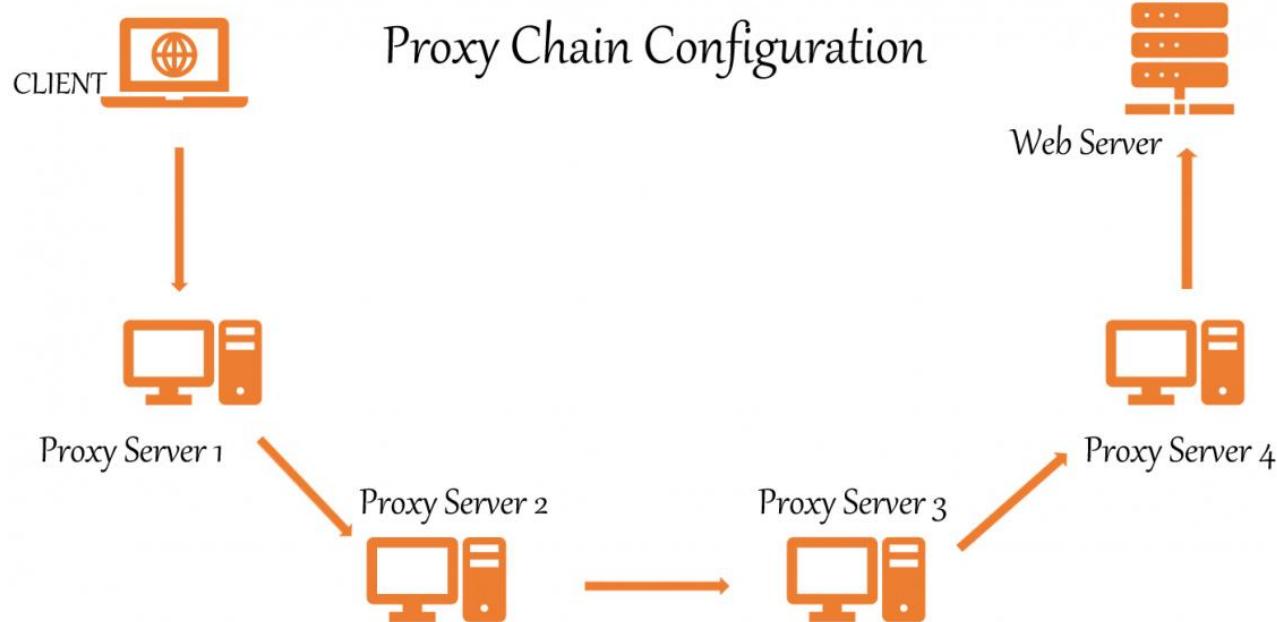


VPN IPSec





PROXY CHAINS

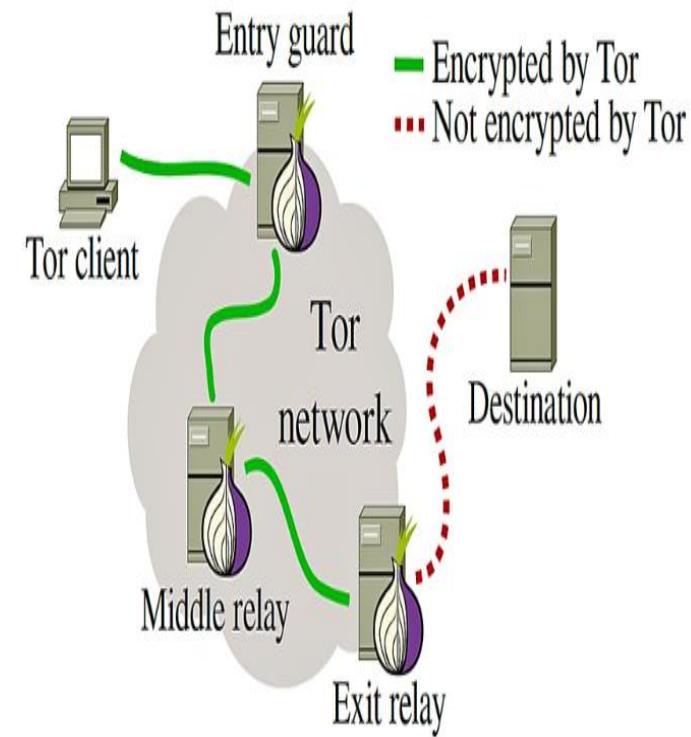


La red Tor

- La red Tor es un sistema popular que consiste en personas de ideas afines que usan software de código abierto para crear una serie de conexiones virtuales entre usuarios. Utilizada correctamente, la red Tor puede frustrar significativamente los esfuerzos para rastrear las comunicaciones que viajan a través de ella.
- La función de Tor esencialmente se reduce a enrutar un mensaje a través de múltiples nodos de tal manera que resista los intentos de análisis de tráfico. Antes de enviar un mensaje, el cliente de origen crea una ruta prácticamente aleatoria, un salto a la vez, a través de otros nodos participantes.

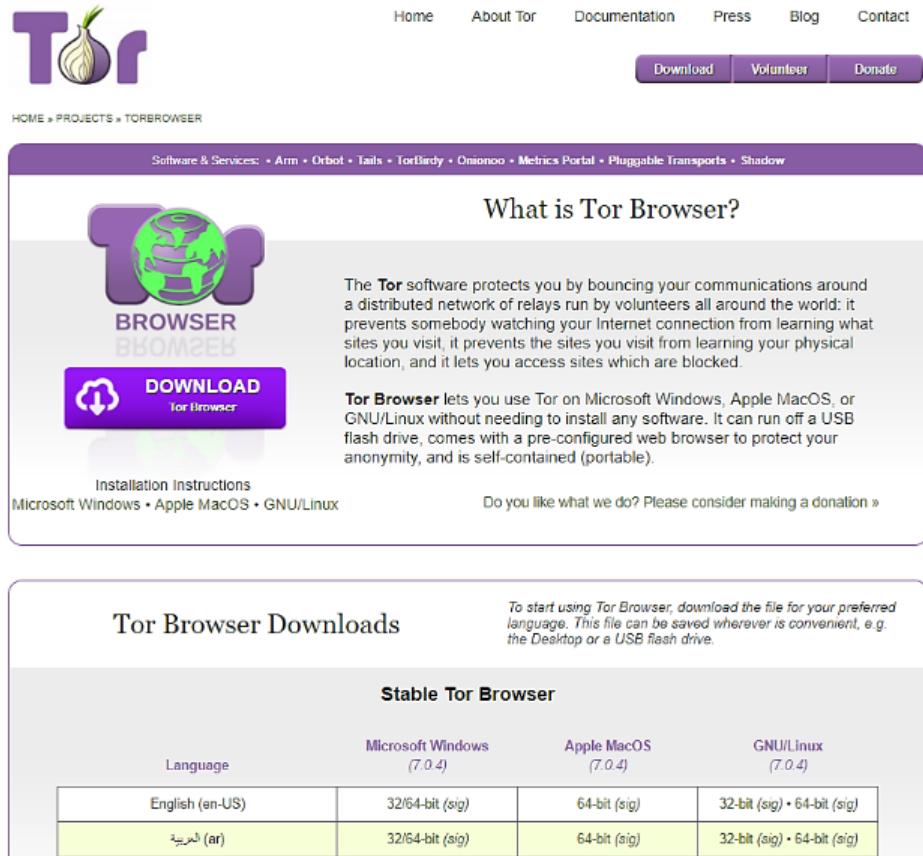
El sistema Tor

- Cada nodo solo conoce la ubicación de los nodos inmediatamente anteriores y posteriores a él porque toda la otra información del encabezado está encriptada con su propia clave. Una vez que se establece una ruta, el tráfico seguro puede comenzar entre el origen y el destino. Sin embargo, para mantener la seguridad, se calcula una nueva ruta cada varios minutos. Los relés a través de los cuales pasan las comunicaciones en Tor son servidores gestionados por voluntarios de todo el mundo.



El navegador Tor

- El método más común para acceder a la red Tor es a través de un navegador Tor. El navegador Tor es una versión modificada del navegador web de código abierto Mozilla Firefox (versión de soporte extendido). El navegador presenta varias extensiones de Firefox junto con el proxy Tor que establece una conexión con el enrutador Onion. También está configurado por defecto para no guardar cookies e historiales de navegación.



The screenshot shows the official Tor Browser website. At the top, there's a purple header with the word "Tor" in white. Below it is a navigation bar with links: Home, About Tor, Documentation, Press, Blog, and Contact. There are also "Download", "Volunteer", and "Donate" buttons. The main content area has a purple background. On the left, there's a large "TOR BROWSER" logo with a green globe icon. In the center, there's a "DOWNLOAD for Browser" button with a white arrow icon. Below the button, there are "Installation Instructions" and links for Microsoft Windows, Apple Mac OS, and GNU/Linux. To the right, there's a section titled "What is Tor Browser?" which explains the software's purpose: protecting user privacy by routing traffic through a network of volunteers' relays. It also mentions that the browser is self-contained and can run from a USB flash drive. At the bottom, there's a "Tor Browser Downloads" section with a "Stable Tor Browser" heading and a table showing download links for different operating systems and languages. The table includes columns for Language, Microsoft Windows, Apple Mac OS, and GNU/Linux, with English and Arabic (ar) listed.

Language	Microsoft Windows (7.0.4)	Apple Mac OS (7.0.4)	GNU/Linux (7.0.4)
English (en-US)	32/64-bit (sig)	64-bit (sig)	32-bit (sig) • 64-bit (sig)
Arabic (ar)	32/64-bit (sig)	64-bit (sig)	32-bit (sig) • 64-bit (sig)

El navegador Tor

- El navegador se puede descargar desde el sitio web principal del Proyecto Tor.

<https://www.torproject.org/projects/torbrowser.html.en>

Archivo Acciones Editar Vista Ayuda

```
root@kali2:/home/analyst/Descargas# sudo -u toruser -H torbrowser-launcher
Tor Browser Launcher
By Micah Lee, licensed under MIT
version 0.3.2
https://github.com/micahflee/torbrowser-launcher
Creating GnuPG homedir /home/toruser/.local/share/torbrowser/gnupg_homedir
QStandardPaths: XDG_RUNTIME_DIR not set, defaulting to '/tmp/runtime-toruse
r'
Downloading Tor Browser for the first time.
Downloading https://aus1.torproject.org/torbrowser/update_3/release/Linux_x
86_64-gcc3/x/en-US
Latest version: 9.5.1
Downloading https://dist.torproject.org/torbrowser/9.5.1/tor-browser-linux6
4-9.5.1_es-ES.tar.xz.asc
Downloading https://dist.torproject.org/torbrowser/9.5.1/tor-browser-linux6
4-9.5.1_es-ES.tar.xz
Verifying Signature
Extracting tor-browser-linux64-9.5.1_es-ES.tar.xz
Running /home/toruser/.local/share/torbrowser/tbb/x86_64/tor-browser_es-ES/
start-tor-browser.desktop
Launching './Browser/start-tor-browser --detach' ...
root@kali2:/home/analyst/Descargas#
root@kali2:/home/analyst/Descargas#
root@kali2:/home/analyst/Descargas#
root@kali2:/home/analyst/Descargas#
root@kali2:/home/analyst/Descargas#
root@kali2:/home/analyst/Descargas#
```



Pincha en "Connect" para conectar con Tor

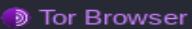
Pulsa "Configurar" para ajustar la configuración de red si estás en un país que censura Tor (como Egipto, China, Turquía) o si estás conectando desde una red privada que requiera un proxy.

Conectar

Configurar

Para asistencia, visita support.torproject.org/#connectingtotor

Salir



¿Nuevo en Tor
Browser?
Comencemos.

Término de búsqueda o dirección



Tor Browser 9.5.1

[Ver registro de modificaciones.](#)

Explora. En privado.

Ahora estás listo/a para experimentar la navegación más privada del mundo.



Buscar con DuckDuckGo



Se puede usar Tor libremente por las donaciones de personas como tu. [Dona ahora. »](#)

¿Preguntas? [Comprobar nuestro Manual del Tor Browser](#)

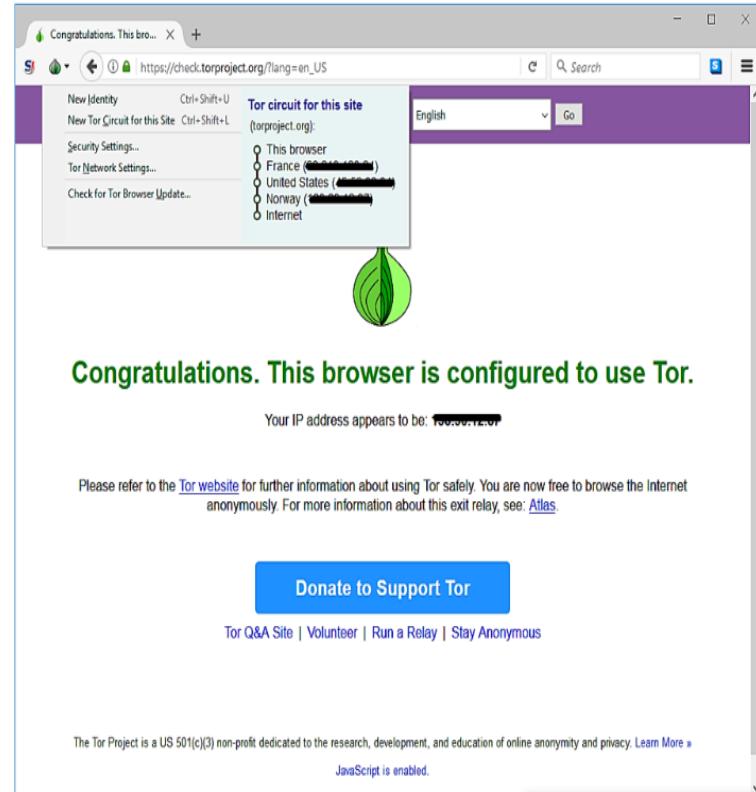


Recibe las últimas noticias de Tor directamente en tu bandeja de entrada. [Inscríbete en Tor News. »](#)

El proyecto Tor es una organización sin fines de lucro definida legalmente en Estados Unidos como 501(c)(3), avanzando libertades y derechos humanos mediante la creación y despliegue de tecnologías de anonimato y privacidad sin costo y de fuente abierta, apoyando su disponibilidad y uso sin restricciones y ampliando su entendimiento científico y popular. [Involúcrate](#)

Iniciando con el navegador Tor

- Al iniciar el Navegador Tor por primera vez, es una buena idea familiarizarse un poco con el sistema antes de saltar directamente a la Dark Web. Es recomendable leer el manual proporcionado en la página de inicio del navegador Tor.
- Además, Tor proporciona un enlace a algunos consejos para usar correctamente el sistema para maximizar el anonimato. Para verificar que el navegador esté conectado correctamente al enrutador Onion, haga clic en "Probar configuración de red Tor" en la página de inicio predeterminada.





DESCARGAR

Cómo descargar el Tor Browser

Instalación

Instalar el Navegador Tor

Corriendo el Navegador Tor por primera vez

Cómo usar el Tor Browser por primera vez

Evitando obstáculos

Qué hacer si la red Tor está bloqueada

PUENTES

La mayoría de los Transportes Conectables, como obfs4, se basan en el uso de repetidores "puente".

Gestionando identidades

Aprende a controlar la información para identificarte en el Navegador Tor

Servicios Onion

Servicios que sólo son accesibles usando Tor

CONEXIONES SEGURAS

Acerca de Tor

+



¿Nuevo en Tor
Browser?
Comencemos.

Explora. En privado.

Ahora estás listo/a para experimentar la navegación más privada.



Buscar con DuckDuckGo

Se puede usar Tor libremente por las donaciones de personas como tú. [Donar](#)

¿Preguntas? [Comprobar nuestro Manual del Tor Browser](#)



Recibe las últimas noticias de Tor directamente en tu bandeja de entrada. [Inscríbete en la newsletter](#)



Nueva ventana

Ctrl+N

Nueva identidad

Ctrl+Mayús.+U

Nuevo circuito Tor para este sitio

Ctrl+Mayús.+L

Tamaño

- 100% + ↗

Editar

x ↕ 🗑

Catálogo

>

Inicios de sesión y contraseñas

Ctrl+Mayús.+A

Complementos

Preferencias

Personalizar...

Abrir archivo...

Ctrl+O

Guardar como...

Ctrl+S

Imprimir...

Buscar en esta página...

Ctrl+F

Más

>

Desarrollador web

>

Ayuda

>

Salir

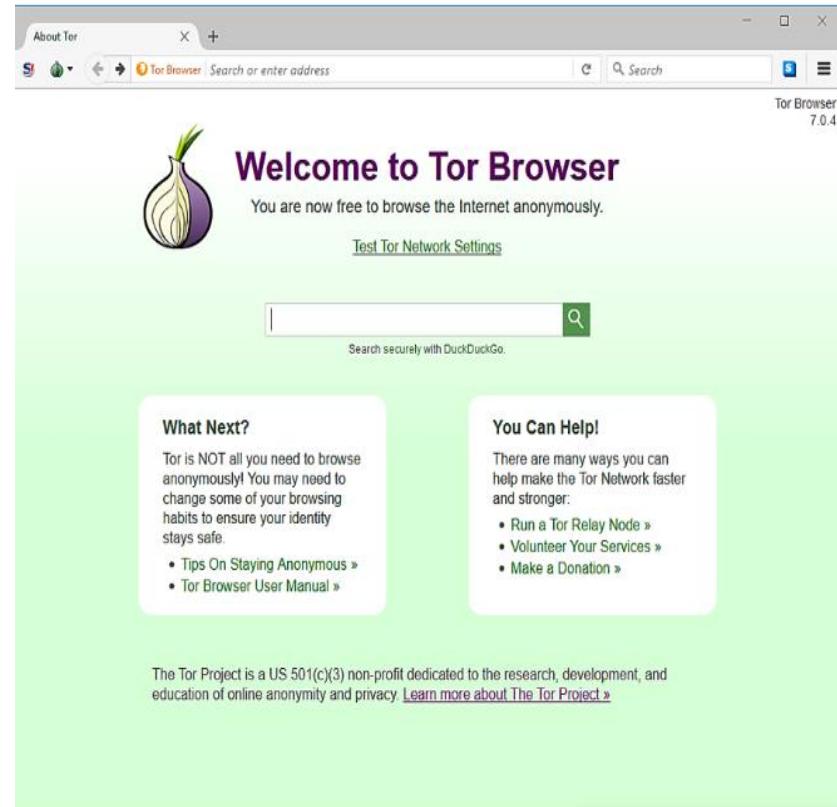
Ctrl+Q

La Web Obscura

- La "Web oscura" es un término que se refiere a los contenidos de Internet a los que solo se puede acceder mediante protocolos de anonimato y enrutamiento como la red Tor (es un error común pensar que la Web oscura y la "Web profunda" son términos intercambiables, pero "Deep Web" simplemente se refiere a los sitios en la World Wide Web que no están indexados por los motores de búsqueda.)

La Web Obscura

- La naturaleza anónima de la comunicación en la Dark Web es fuente de gran controversia en todo el mundo porque tal anonimato eventualmente lleva a proliferación de contenido objetable, y a veces peligroso. Además de servir como un posible canal de comunicación para terroristas, la Deep Web facilita la distribución abierta de narcóticos ilegales, armas, información financiera robada y pornografía ilícita, entre otras cosas.



Acerca del uso de Tor ...

- La dirección IP del nodo de salida que los sitios web ven para su conexión es diferente de la dirección IP pública asignada a su máquina por su ISP. Así es como se logra el anonimato. Puede confirmar esto ingresando a un navegador web estándar (no en Tor) y verificando su dirección IP pública.
- Una cosa a tener en cuenta al usar Tor es que muchos proveedores de servicios de Internet intentan detectar si sus clientes están usando Tor y bloquear el tráfico o informar la actividad a las fuerzas del orden público. Aunque en la mayoría de los casos no pueden rastrear acciones particulares hasta un usuario, el hecho de que se esté utilizando Tor puede atraer atención no deseada.

Acerca del uso de Tor ...

- La detección del tráfico Tor se puede eludir, aunque sea solo temporalmente, utilizando puentes Tor o relés de puente. Debido a la naturaleza de Tor, los nodos de cebolla son conocidos públicamente, por lo que un ISP puede ver si un cliente se está conectando a un punto de entrada de Tor. Los relés de puente son nodos de entrada alternativos que intentan permanecer ofuscados, pero debe tenerse en cuenta que generalmente son menos confiables que los nodos públicos de Tor.

Relays puentes

- Para configurar el navegador Tor para usar relés de puente, haga clic en el ícono del menú desplegable de Cebolla y abra el cuadro de diálogo Marque la casilla junto a "Mi proveedor de servicios de Internet (ISP) bloquea las conexiones a la red Tor" y elija el botón de opción "Conectar con puentes provistos". Elegir el tipo de transporte obs4 promulgará transportes enchufables.

The screenshot shows the 'Tor Browser' preferences window with the URL 'about:preferences#tor'. On the left, there's a sidebar with icons for General, Inicio, Buscar, Privacidad & Seguridad, and Tor. The 'Tor' icon is highlighted with a red box. The main content area has two sections: 'Configuración de Tor' and 'Puentes'. Under 'Configuración de Tor', it says 'El Navegador Tor enruta tu tráfico a través de la Red Tor, mantenida por miles de voluntarios alrededor del mundo.' with a 'Más información' link. Under 'Puentes', it says 'Los puentes te ayudan a acceder a la Red Tor en lugares donde Tor está bloqueado. Dependiendo de dónde te encuentres, un puente puede funcionar mejor que otro.' with another 'Más información' link. A red box highlights the checked checkbox 'Usa un puente'. To its right is a dropdown menu set to 'obs4', also highlighted with a red box. Below the dropdown are three radio button options: 'Seleccionar un puente construido' (selected), 'Solicitar un puente de torproject.org', and 'Proporcionar un puente'. A button 'Solicitar un nuevo puente...' is next to the dropdown. At the bottom, there's a text input field with placeholder text 'escribe dirección:puesto (uno por línea)'.

Relays puentes

- Si tiene su propia lista de relés de puente que prefiere conectar, elija el botón de opción "Introducir puentes personalizados" y pegue las ubicaciones de los puentes en el cuadro de texto, uno por línea. Se puede encontrar una lista de puentes en el sitio web del Proyecto Tor en el siguiente enlace, pero los hackers éticos siempre deben estar atentos a nuevos puentes de fuentes confiables.
 - **Puentes estándar:**

<https://bridges.torproject.org/bridges>

- **Puentes de transporte enchufables:**

<https://bridges.torproject.org/bridges?transport=obfs4>

Tor Network Settings

My Internet Service Provider (ISP) blocks connections to the Tor network

Connect with provided bridges

Transport type: obfs4 (recommended)

Enter custom bridges

Enter one or more bridge relays (one per line).

Help

```
obfs4 52.17.245.227:9443 5F9DC0B2D626B978764AA3EE3D338E384C053683 cer  
obfs4 138.197.104.74:9443 D6B1BC39AE1AD67A09361F2D625CDF8010EA0F27 ce  
obfs4 107.191.58.23:34345 225A895211B179FDE2E8F8E35BE8EE5C8BECC0B0 ce
```

<

>

This computer needs to use a local proxy to access the Internet

This computer goes through a firewall that only allows connections to certain ports

For assistance, visit torproject.org/about/contact.html#support

[Copy Tor Log To Clipboard](#)

OK

Cancel

Mejorando las capacidades de Tor

- Tor es un proceso subyacente que el navegador Tor usa para acceder al enrutador Onion, pero también se puede usar con otras aplicaciones aparte de un navegador. Esto es especialmente importante cuando se ejecutan exploits.
- Para configurar Tor para usar relés de puente de transporte enchufables en Linux sin usar el Navegador Tor, se necesitan algunos comandos de terminal y configuración.

Instalando un proxy

- Suponiendo que Tor ya se haya instalado, ingrese los siguientes comandos para descargar e instalar los servicios de puente obsf (use sudo si es necesario):
- # service tor stop
- # apt-get update
- # apt-get install obsfproxy obsf4proxy

Posteriormente debemos abrir y editar el archivo de configuración "torrc" que se encuentra dentro del directorio /etc/tor/directory

Edición del archivo torrc

```
## Bridges
UseBridges 1
ClientTransportPlugin obfs3 exec /usr/bin/obfsproxy managed
ClientTransportPlugin obfs4 exec /usr/bin/obfs4proxy managed

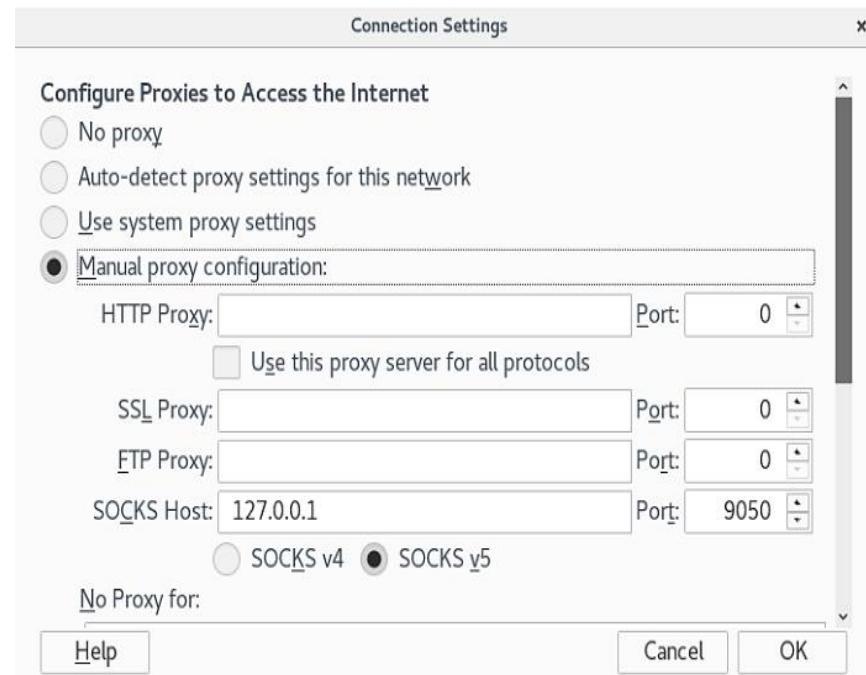
Bridge obfs4 52.213.17.227:443
Bridge obfs4 136.159.101.112:443
Bridge obfs4 100.100.100.100:443
```

Verificación de Proxy

- Iniciar Tor desde una terminal:

```
# service tor start
```

- Para confirmar que tor se está ejecutando, abra un navegador web estándar (no el navegador Tor). En la configuración de red, establezca la configuración manual del proxy en un host SOCKSv5 local de 127.0.0.1:9050



Recomendaciones

1. No utilices aplicaciones de intercambio de archivos torrent sobre Tor
2. No instales complementos en el navegador Tor ni habilites ninguno que esté deshabilitado de forma predeterminada
3. No abras documentos descargador del navegador Tor
4. Usa un relay de puente Tor cuando sea posible.
5. Utiliza preferentemente URLs con HTTPS



https://duckduckgo.com/?ia=web

hidden wiki

All Images Videos News Maps | Meanings Settings ▾

France ▾ Safe Search: Moderate ▾ Any Time ▾

Hidden Wiki | Tor .onion urls directories

▶ <https://thehiddenwiki.org>

The Hidden Wiki is one of the oldest link directories on the dark web. Famous for listing all important .onion links. From drug marketplaces to financial services you can find all the important deep web services listed here. If you can not find the link you are looking for, check the other introduction points. ...

Hidden Wiki - The Original @ HiddenWiki.com • Hidden Wiki

● <https://hiddenwiki.com>

The Hidden Wiki is not illegal to browse, also all sites listed on HiddenWiki.com are legal to browse if you only do it for educational purposes and you do not order any illegal items. Only as mentioned above, some links on the uncensored hidden wiki may not be legal, so it is better to not browse to those urls.

The Hidden Wiki

● <https://thehiddenwiki.com>

The Hidden Wiki - The Hidden Wiki 2020 link. DuckDuckGo - A Hidden Service that searches the clearnet. OnionLinks - .Onion link directory. Hidden Wiki - New Hidden Wiki 2019; Another Hidden Wiki Another hidden wiki like link collection. The Dark Web Pug Pug's Ultimate Dark Web Guide . Financial Services. Currencies, banks, money ...

Hidden Wiki - The Original + https://hiddenwiki.com ... ⚙️

<http://onionlinksanifwu.onion/> Onion Links v3
<http://zqktlwiuvvqqt4ybvgvi7tyo4hjl5xgfuvpdf6otjiycgwqbym2qad.onion>
[/wiki/index.php/Main_Page](http://wiki/index.php/Main_Page) The Original Hidden Wiki
<http://hiddenwikig7vsuh.onion/> The Hidden Wiki 2020
<http://hiddenwikiwks5vm.onion/> Hidden Wiki
<http://darkwebpugm7idof.onion/> Pug's Dark Web Guide
<http://wikikit5zfr2c3rt.onion/> Yet Another Hidden Wiki
<http://darkfaillrhatkn2.onion/> Dark Fail Dark Web Markets

Dark Web Markets

<http://y3sgjf7euifxmibv6wss3mz6j3pj72la5bsn62zyapb3taiszkbi7kyd.onion/> Avaris
<http://cannazon4fb3r4to.onion/> Cannazon
<http://q7g6fqn5uwvgbqtxkcttcqebsk7m4z2fbn7suf6lasyknyvzdb2vcqqd.onion/> Cryptonia
<http://darkbayupf5emqt3.onion/> Darkbay
<http://62qfti22ihjpufqf64fcje4kurxgkup7hsf2ubm4du52fxgsyucslyd.onion/> BitBazaar
<http://apollonzagbibss4.onion/> Apollon
<http://hydrarukvkdeydpv.onion/> Hydra
<http://empiremkt3dhvulo.onion/> Empire
<http://cr46ajob5pksz4gdxypl2tb95ot64pzv3mq5bugrfa6d7vyrgngxid.onion/>
Whitehouse
<http://cannahomeauivztp.onion/> Cannahome
<http://pointgg34zznzsoj.onion/> Tochka
<http://yajak7zicztvgl3nochndqqb4ejjf6i4yh6vlzgajwnsahtryq4xqatid.onion/> Monopoly

Codificar Vs Cifrar

La codificación aplica un proceso de **conversión** de los componentes de un mensaje para que este no sea entendido.

Las reglas de transformación entre un sistema y otro van a estar definidas para poder entender el contenido del mensaje.

La codificación se basa en alterar la semántica del mensaje, lo que está relacionado con el significado del mensaje.

Sistema	Dígitos
Hexadecimal	0 1 2 3 4 5 6 7 8 9 A B C D E F
Octal	0 1 2 3 4 5 6 7
Binario	0 1
Decimal	0 1 2 3 4 5 6 7 8 9

¿Qué nos dice el siguiente mensaje?

MENSAJE:

VVRJNWEyRlhXbkJaTWtaNVNVYzFka2xIVm5wSIIzaDJTVW
N4Y0dNeU1YWkpTRVI4V2xOQ2FtRlhXbmxaV0VrOQ==



Listas de acceso

Todas las listas de control de acceso (ACL) deben planificarse. Al configurar una ACL compleja, se sugiere que:

- Utilice un editor de texto y escriba los detalles de la política que se va a implementar.
- Agregue los comandos de configuración del IOS para realizar esas tareas.
- Incluya comentarios para documentar la ACL.
- Copie y pegue los comandos en el dispositivo.
- Pruebe siempre exhaustivamente una ACL para asegurarse de que aplica correctamente la política deseada.

Sintáxis de una ACL estándar numerada

Para crear una ACL estándar numerada, utilice el comando **access-list** .

```
Router(config)# access-list access-list-number {deny | permit | remark text} source [source-wildcard]  
[log]
```

Parámetro	Descripción
<i>número-acl</i>	El rango de números es de 1 a 99 o de 1300 a 1999
deny	Deniega el acceso si se dan las condiciones.
permit	Permite el acceso si se dan las condiciones.
<i>texto de observación</i>	(Opcional) entrada de texto para fines de documentación
<i>origen</i>	Identifica la red de origen o la dirección de host que se va a filtrar
<i>comodín-origen</i>	(Optativo) Máscara wildcard de 32 bits para aplicar al origen.
registrar	(Opcional) Genera y envía un mensaje informativo cuando el ACE coincide

Sintaxis de una ACL estándar con nombre

Para crear una ACL estándar numerada, utilice el **comando ip access-list standard**

- Los nombres de las ACL son alfanuméricos, distinguen mayúsculas de minúsculas y deben ser únicos.
- No es necesario que los nombres de las ACL comiencen con mayúscula, pero esto los hace destacarse cuando se observa el resultado de show running-config.

```
Router(config)# ip access-list standard access-list-name
R1(config)# ip access-list standard NO-ACCESS
R1(config-std-nacl)# ?
Standard Access List configuration commands:
  <1-2147483647> Sequence Number
  default      Set a command to its defaults
  deny         Specify packets to reject
  exit         Exit from access-list configuration mode
  no           Negate a command or set its defaults
  permit        Specify packets to forward
  remark       Access list entry comment
```

Aplicación de ACL estándar numerada

Después de configurar una ACL IPv4 estándar, debe vincularse a una interfaz o entidad.

- El comando **ip access-group** se utiliza para enlazar una ACL IPv4 estándar numerada o nombrada a una interfaz.
- Para eliminar una ACL de una interfaz, primero introduzca el comando **no ip access-group** interface configuration.

```
Router(config-if) # ip access-group {access-list-number | access-list-name} {in | out}
```

Ejemplo ACL estándar numerada

El ejemplo ACL permite el tráfico desde el host 192.168.10.10 y todos los hosts de la interfaz de salida de red 192.168.20.0/24 serial 0/1/0 en el router R1.

```
R1(config)# access-list 10 remark ACE permits ONLY host 192.168.10.10 to the internet
R1(config)# access-list 10 permit host 192.168.10.10
R1(config)# do show access-lists
Standard IP access list 10
  10 permit 192.168.10.10
R1(config)#
R1(config)# access-list 10 remark ACE permits all host in LAN 2
R1(config)# access-list 10 permit 192.168.20.0 0.0.0.255
R1(config)# do show access-lists
Standard IP access list 10
  10 permit 192.168.10.10
  20 permit 192.168.20.0, wildcard bits 0.0.0.255
R1(config)#
R1(config)# interface Serial 0/1/0
R1(config-if)# ip access-group 10 out
R1(config-if)# end
R1#
```

Ejemplo ACL estándar denominada

El ejemplo ACL permite el tráfico desde el host 192.168.10.10 y todos los hosts de la interfaz de salida de red 192.168.20.0/24 serial 0/1/0 en el router R1.

```
R1(config)# no access-list 10
R1(config)# ip access-list standard PERMIT-ACCESS
R1(config-std-nacl)# remark ACE permits host 192.168.10.10
R1(config-std-nacl)# permit host 192.168.10.10
R1(config-std-nacl)#
R1(config-std-nacl)# remark ACE permits host 192.168.10.10
R1(config-std-nacl)# permit host 192.168.10.10
R1(config-std-nacl)# remark ACE permits all hosts in LAN 2
R1(config-std-nacl)# permit 192.168.20.0 0.0.0.255
R1(config-std-nacl)# exit
R1(config)#
R1(config)# interface Serial 0/1/0
R1(config-if)# ip access-group PERMIT-ACCESS out
R1(config-if)# end
R1#
```

Mecanismos de control

Firewall

IDS/IPS

Proxy

Honeypots

Firewalls

- Algunas propiedades comunes de firewalls:

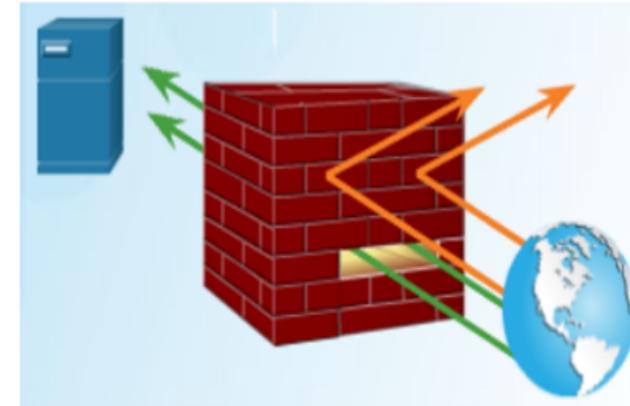
- Los firewalls resisten ataques de red.
- Todo el tráfico fluye a través del firewall.
- Los firewalls aplican la política de control de acceso.

- Algunos beneficios de usar un firewall en una red:

- Previene la exposición de hosts, recursos y aplicaciones confidenciales, y aplicaciones a usuarios no confiables.
- Limpia el flujo del protocolo.
- Bloquea los datos maliciosos de servidores y clientes.
- Reduce la complejidad de la administración de la seguridad.

- Los firewalls también tienen algunas limitaciones:

- Un firewall mal configurado puede tener graves consecuencias para la red.
- Los datos de muchas aplicaciones no se pueden transmitir con seguridad mediante firewalls.
- Los usuarios buscan formas alrededor del firewall para recibir material bloqueado.
- Puede reducirse la velocidad de la red.
- El tráfico no autorizado se puede tunelizar como tráfico legítimo a través del firewall.



Tipos de Firewalls

- **Los firewalls de filtrado de paquetes (sin estado)** suelen formar parte de un firewall de router, que autoriza o rechaza el tráfico a partir de la información de las capas 3 y 4.
- **Firewall con estado:**
 - Permiten o bloquean el tráfico según el estado, el puerto y el protocolo.
 - Monitorea toda la actividad desde la apertura hasta el cierre de una conexión.
- **Firewall de puerta de enlace de la aplicación (proxy de firewall):** filtra la información en las capas 3, 4, 5 y 7 del modelo de referencia OSI.
- **Firewall basado en host (servidor y personal):** una computadora o servidor que ejecuta software de firewall.
- **Firewall transparente:** filtra el tráfico de IP entre un par de interfaces conectadas con puente.
- **Firewall híbrido:** una combinación de los distintos tipos de firewall.

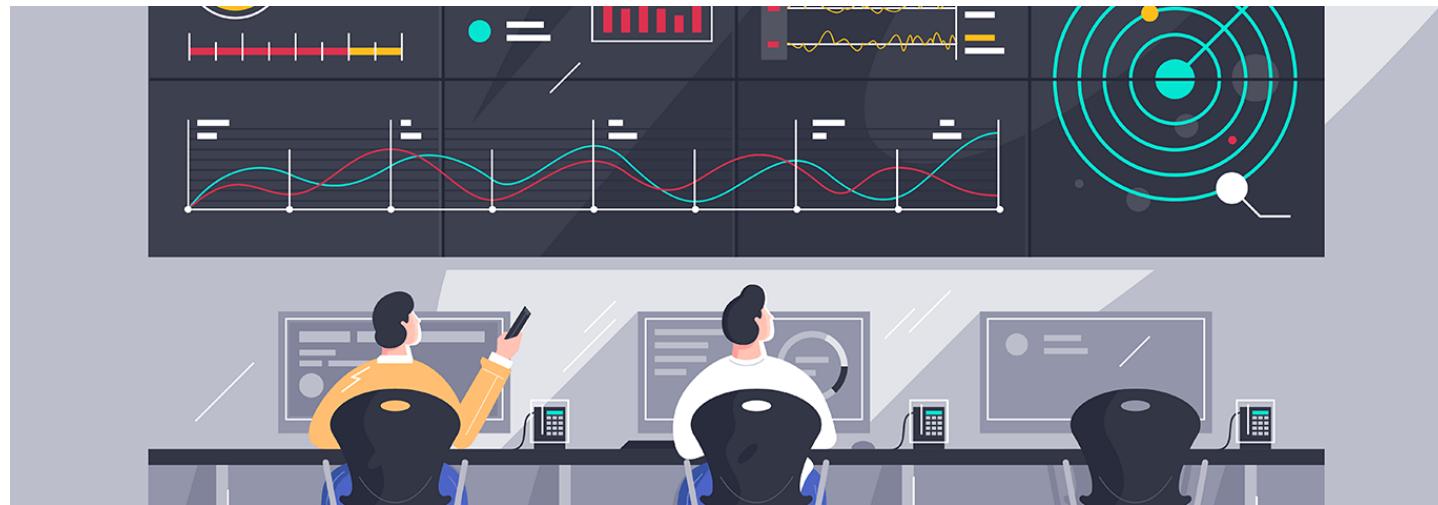
¿Por qué debemos monitorear?

La detección oportuna de fallas y el monitoreo de elementos que conforman una red de cómputo son actividades de gran relevancia para **brindar un buen servicio** a los usuarios.

De esto se deriva la importancia de contar con un esquema capaz de notificarnos de las fallas en la red y de mostrarnos su comportamiento mediante el análisis y recolección de tráfico.

Enfoques de monitoreo

Existen al menos , dos puntos de vista para abordar el proceso de monitorear una red: el **enfoque activo** y el **enfoque pasivo**. Aunque son diferentes ambos se complementan.



Monitoreo Activo

Este tipo de monitoreo se realiza inyectando paquetes de prueba en la red, o enviando paquetes a determinadas aplicaciones midiendo sus tiempos de respuesta. Este enfoque tiene la característica de agregar tráfico en la red. Es utilizado para medir el **rendimiento en una red**.



Vector de ataque

Cuando se quiere comprometer una máquina lo primero que es necesario hacer es prepararse. Aquí hacemos la puntuación de máquina y no de alguien que esté detrás de la misma, porque independientemente de lo que nos parezca, vamos a luchar primero con el equipo (computadora con sus medidas de seguridad) y después con la inteligencia detrás del mismo.



Vector de ataque



Metodología de Footprinting

Un hacker inicialmente aplicaría una metodología de footprinting, la cual es una manera procedimental de recolectar información acerca de una organización objetivo desde todos los recursos disponibles.



¿Qué es Footprinting?

Footprinting, es el primer paso en el Ethical Hacking, se refiere al proceso de recolectar información acerca de la red objetivo y todo su ambiente. Con el uso de Footprinting el Hacker puede encontrar varias maneras de introducirse dentro de los sistemas que se encuentran en red de la organización.

Inicia con el seguimiento de un objetivo basado en:

- Nombre del dominio
- Direcciones IP
- Servicios disponibles TCP/UDP

Ejemplo

Supongamos que un intruso malicioso planea lanzar un ataque sobre una empresa llamada "AndesTrades". Lo primero que hará para descubrir en qué dominio se encuentra puede ser buscar el nombre de la organización en un motor de búsquedas desde Internet.



Motores de búsquedas

Google andestrades X 

[Todo](#) [Maps](#) [Imágenes](#) [Videos](#) [Noticias](#) [Más](#) [Preferencias](#) [Herramientas](#)

Cerca de 4,550 resultados (0.59 segundos)

Quizás quisiste decir: [andes trades](#)

www.andestrades.com ▾
Andes Trades - Productos Organicos para Dieta - Salud ...
AndesTrades te trae los mejores precios y la mejor selección en productos de belleza y salud.
Ven y descubre nuestro catalogo, llenos de instrumentos para su ...
Visitaste esta página el 26/06/20.

www.andestrades.com > [acerca-de-nuestra-tienda-andes...](#) ▾
Productos Organicos para Dieta - Salud ... - Andes Trades
Nuestra compañía, **Andes Trades**, se especializa in importar y exportar los mejores productos para el bienestar y cuidado personal que se encuentren en el ...

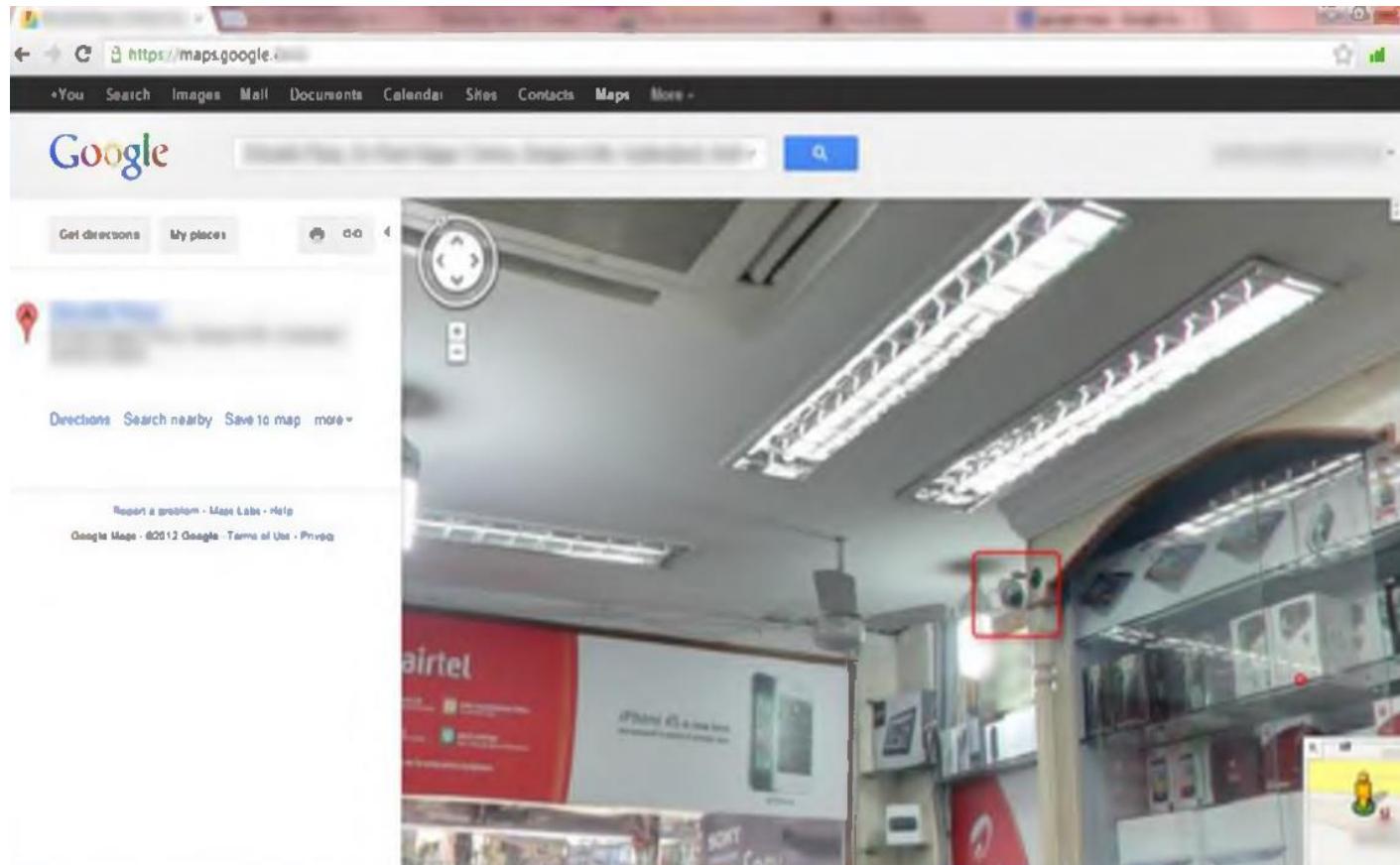


[Ver fotos](#)

Andes Trades
[Sitio Web](#) [Guardar](#)
1.0 ★★★★ [comentario de Google](#)

Teléfono: +56 2 3206 0853

Mapas de Geolocalización



Herramientas online

	Zaba Search http://www.zabasearch.com
	123 People Search http://www.123people.com
	ZoomInfo http://www.zoominfo.com
	PeekYou http://www.peekyou.com
	Wink People Search http://wink.com
	Intelius http://www.intelius.com
	AnyWho http://www.anywho.com
	PeopleSmart http://www.peoplesmart.com
	People Lookup https://www.peoplelookup.com
	WhitePages http://www.whitepages.com

ZABA[®] SEARCH

People Search. Honestly Free! Search by Name.
Find People in the USA. Free People Finder.

White Pages	Reverse Phone Lookup	Advanced People Search	Free Search Menu
<input type="text" value="mariah"/> <input type="text" value="carey"/> <input type="button" value="All 50 States"/> <input type="button" value="Search"/>			
POWERED BY  INTELIUS BEING INFORMED MATTERS			

Filter your results by: [Clear filters](#)

Found 93 Results for Mariah Carey

Mariah Carey
11 Long Ridge Rd, Plainview, NY 11803-1816

[View full profile »](#)

More information for Mariah Carey
[Other Phone Lookup](#)
[Background Check](#)
[Public Records](#)
[Property Records](#)
[Maps & Driving Directions](#)



Mariah Carey

Mariah's Complete Summary: 24% Finished

Key Information

Social Media Summary

Social Media Found

Social Media Found



SOCIAL MEDIA ACCOUNTS FOUND

Our data sources have **uncovered social media accounts** associated with the name Mariah Carey. These may include popular social media platforms and **even dating sites**. Click continue to see these profiles in Mariah Carey's report.

Attention: We search millions of records to find results for you.

CONTINUE

Please do not Refresh, Close, or Press the Back button on this page or your information may be lost



beenverified.com/lp/9a28e2/2/building-report#.



TRIED BY MILLIONS

Databases

23%

Jon Snow

Fayetteville, NC

Searching

Home Address

Phone Numbers

Social Media Scan

Criminal Records

Photos

Social Media Scan

Our search on **Jon Snow** may reveal interesting information such as user profiles, videos, family, friends, professional connections and more

Facebook



Flickr



Twitter



Google+



LinkedIn



Youtube



Picasa



Pinterest



Reddit



Ancestry



Klout



Instagram



Amazon



Vimeo



"BeenVerified is easy to use. I have used BeenVerified over 600 times in the past 2 years."

LINDA. VIA CONSUMERAFFAIRS.COM

Actividad

Con ayuda de un navegador de Internet como Mozilla Firefox o Google Chrome, llevar a cabo una visita en algunas de herramientas para la búsqueda de datos personales de personas que habiten en los estados unidos (actores, comediantes, artistas, dueños de empresas, etc..) y posteriormente comentar tus resultados.

NOTA: Utilizar una cuenta de correo electrónico diferente a la personal para registrarse a las plataformas que solicitan información de formulario.

Actividad

Posteriormente responde las siguientes preguntas

¿Que herramienta considero pudiera ser de mayor utilidad para búsqueda de datos personales sobre gente que resida en los estados unidos?

¿Puedo utilizar la mismas herramientas para buscar información para gente de México? Si/No. Justifica tu respuesta

¿Cuales son alguna herramientas en Internet que pudiera utilizar para hacer búsquedas para habitantes de México?



Zaba Search
<http://www.zabasearch.com>



123 People Search
<http://www.123people.com>



ZoomInfo
<http://www.zoominfo.com>



PeekYou
<http://www.peekyou.com>



Wink People Search
<http://wink.com>



Intelius
<http://www.intelius.com>



AnyWho
<http://www.anywho.com>



PeopleSmart
<http://www.peoplesmart.com>



People Lookup
<https://www.peoplelookup.com>



WhitePages
<http://www.whitepages.com>

Footprinting Web



<https://sitereport.netcraft.com/>

What's that site running?

Find out the infrastructure and technologies used by
any site using results from our **internet data mining**



Example: <https://www.netcraft.com>



Site title	Netcraft Internet Research, Cybercrime Disruption and PCI Security Services	Date first seen	December 2013
Site rank	2338	Netcraft Risk Rating 	0/10 
Description	Internet Research, Cybercrime Disruption and PCI Security Services	Primary language	English

Network

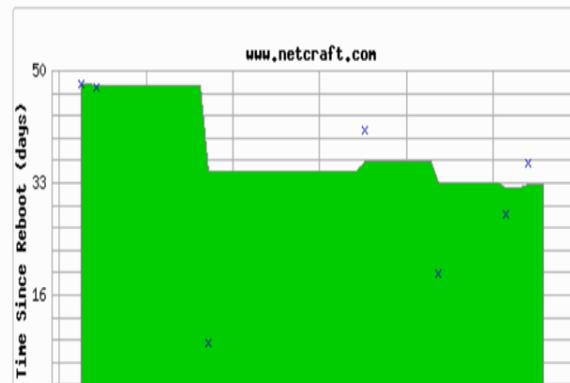
Site	https://www.netcraft.com 	Domain registrar	namecheap.com
Netblock Owner	Amazon.com, Inc.	Nameserver organisation	whois.namecheap.com
Domain	netcraft.com	Organisation	WhoisGuard, Inc., P.O. Box 0823-03411, Panama, Panama
Nameserver	ns1.netcraft.com	Hosting company	Amazon
IP address	13.224.67.81 	Top Level Domain	Commercial entities (.com)
DNS admin	hostmaster@netcraft.com	DNS Security Extensions	unknown
IPv6 address	Not Present	Hosting country	 US 
Reverse DNS	server-13-224-67-81.dub2.r.cloudfront.net	Latest Performance	 Performance Graph 

IP delegation

IPv4 address (13.224.67.81)

IP range	Country	Name	Description
0.0.0.0-255.255.255.255	N/A	IANA-BLK	The whole IPv4 address space
↳ 13.0.0.0-13.255.255.255	🇺🇸 United States	NET13	American Registry for Internet Numbers
↳ 13.224.0.0-13.227.255.255	🇺🇸 United States	AMAZO-CF	Amazon.com, Inc.
↳ 13.224.67.81	🇺🇸 United States	AMAZO-CF	Amazon.com, Inc.

 **Last Reboot** (32 days ago)



Hosting History

Netblock owner	IP address	OS	Web server	Last seen
Amazon.com, Inc. 1918 8th Ave SEATTLE WA US 98101-1244	52.85.104.94	Linux	Apache	10-Jul-2020
Amazon.com, Inc. 1918 8th Ave SEATTLE WA US 98101-1244	13.227.222.91	Linux	Apache	1-Jul-2020
Amazon.com, Inc. 1918 8th Ave SEATTLE WA US 98101-1244	13.224.226.85	Linux	Apache	23-Jun-2020
Amazon.com, Inc. 1918 8th Ave SEATTLE WA US 98101-1244	54.192.137.127	Linux	Apache	15-Jun-2020
Amazon.com, Inc. 1918 8th Ave SEATTLE WA US 98101-1244	143.204.169.42	Linux	Apache	5-Jun-2020
Amazon.com, Inc. 1918 8th Ave SEATTLE WA US 98101-1244	13.224.78.112	Linux	Apache	29-May-2020
Amazon.com, Inc. 1918 8th Ave SEATTLE WA US 98101-1244	13.224.78.3	Linux	Apache	20-May-2020
Amazon.com, Inc. 1918 8th Ave SEATTLE WA US 98101-1244	13.224.130.86	Linux	Apache	12-May-2020
Amazon.com, Inc. 1918 8th Ave SEATTLE WA US 98101-1244	13.224.223.32	Linux	Apache	5-May-2020
Amazon.com, Inc. 1918 8th Ave SEATTLE WA US 98101-1244	13.224.73.124	Linux	Apache	28-Apr-2020

Herramientas online

Domain Dossier

<https://centralops.net/co/DomainDossier.aspx>

Domain Dossier

 Investigate domains and IP addresses

domain or IP address

centralops.net

 domain whois record DNS records traceroute network whois record service scan

user: anonymous [177.236.88.116]

balance: 48 units

[log in](#) | [account info](#)

Do you see Whois records that are missing contact information?

[Read about reduced Whois data due to the GDPR.](#)

Address lookup

canonical name [centralops.net](#).

aliases

addresses **75.126.243.167**

Domain Whois record

Queried **whois.internic.net** with "dom **centralops.net**"...

```
Domain Name: CENTRALOPS.NET
Registry Domain ID: 23425156_DOMAIN_NET-VRSN
Registrar WHOIS Server: whois.namesilo.com
Registrar URL: http://www.namesilo.com
Updated Date: 2019-12-25T00:57:14Z
Creation Date: 2000-03-27T13:18:25Z
Registry Expiry Date: 2021-03-27T12:18:25Z
Registrar: NameSilo, LLC
Registrar IANA ID: 1479
Registrar Abuse Contact Email: abuse@namesilo.com
Registrar Abuse Contact Phone: +1.4805240066
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Name Server: NS1.HEXILLION.COM
Name Server: NS2.HEXILLION.COM
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2020-07-15T18:18:14Z <<<
```

Queried **whois.namesilo.com** with "**centralops.net**"...

```
Domain Name: centralops.net
Registry Domain ID: 23425156_DOMAIN_NET-VRSN
Registrar WHOIS Server: whois.namesilo.com
Registrar URL: https://www.namesilo.com/
Updated Date: 2020-07-08T07:00:00Z
Creation Date: 2000-03-27T07:00:00Z
Registrar Registration Expiration Date: 2021-03-27T07:00:00Z
Registrar: NameSilo, LLC
Registrar IANA ID: 1479
Registrar Abuse Contact Email: abuse@namesilo.com
Registrar Abuse Contact Phone: +1.4805240066
Domain Status: clientTransferProhibited https://www.icann.org/epp#clientTransferProhibited
Registry Registrant ID:
Registrant Name: Domain Administrator
Registrant Organization: Hexillion Technologies
Registrant Street: 6860 North Dallas Parkway, Suite 200
```

DNS records

name	class	type	data		time to live
centralops.net	IN	SOA	server:	ns1.hexillion.com	3600s (01:00:00)
			email:	info@hexillion.com	
			serial:	2019110701	
			refresh:	86400	
			retry:	600	
			expire:	1209600	
			minimum ttl:	3600	
centralops.net	IN	A	75.126.243.167		3600s (01:00:00)
centralops.net	IN	NS	ns2.hexillion.com		3600s (01:00:00)
centralops.net	IN	NS	ns1.hexillion.com		3600s (01:00:00)
centralops.net	IN	TXT	v=spf1 -all		3600s (01:00:00)
167.243.126.75.in-addr.arpa	IN	PTR	hexillion.com		86400s (1.00:00:00)
243.126.75.in-addr.arpa	IN	SOA	server:	ns1.arpa.networklayer.com	3600s (01:00:00)
			email:	root@softlayer.com	
			serial:	2019102300	
			refresh:	10800	
			retry:	3600	
			expire:	604800	
			minimum ttl:	3600	
243.126.75.in-addr.arpa	IN	NS	ns1.arpa.networklayer.com		3600s (01:00:00)
243.126.75.in-addr.arpa	IN	NS	ns2.arpa.networklayer.com		3600s (01:00:00)

Traceroute

Tracing route to [centralops.net \[75.126.243.167\]](http://centralops.net)...

hop	rtt	rtt	rtt	ip address	fully qualified domain name
1	0	0	0	75.126.243.167	hexillion.com

Trace complete

Service scan

FTP - 21 Error: ConnectionRefused

SMTP - 25 Error: ConnectionRefused

HTTP - 80 HTTP/1.1 301 Moved Permanently
Cache-Control: private
Content-Length: 644
Content-Type: text/html; charset=utf-8
Location: http://centralops.net/co
Server: Microsoft-IIS/8.5
Date: Thu, 16 Jul 2020 03:40:20 GMT
Connection: close

POP3 - 110 Error: ConnectionRefused

IMAP - 143 Error: ConnectionRefused

HTTPS - 443 Certificate validation errors: None
Signature algorithm: sha256RSA
Public key size: 2048 bits
Issuer: CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US
Subject: CN=hexillion.com, O=Hexillion Technologies, L=Plano, S=Texas, C=US
Subject Alternative Name: DNS Name=hexillion.com, DNS Name=www.hexillion.com, DNS Name=centralops.net, DNS Name=www.centralops.net
Serial number: 0FCC88C15422BE7BD690B9721997C778
Not valid before: 2017-09-15 00:00:00Z
Not valid after: 2020-11-19 12:00:00Z
SHA1 fingerprint: D4E6BE64C0485E75478FA23D142A152726B08EF0

Network Tools

<https://network-tools.com/>

Express

- Ping
- Traceroute
- Whois Search
- IDN (Native to Punycode) Conversion
- IDN (Punycode to Native) Conversion
- DNS
- Network Lookup
- Spam Blacklist
- URL Encode
- URL Decode
- HTTP Headers
- Email Test

Shar

0
SHARES



Tool

Express



Convert Base-10 to IP

Google Hacking

- Los operadores avanzados de Google ayudan a refinar las búsquedas
- Estos operadores están incluidos como parte de las consultas estándar de Google
- La sintaxis que se utiliza con los operadores avanzados es la siguiente

operador:termino_de_busqueda

Advanced Operators at a Glance

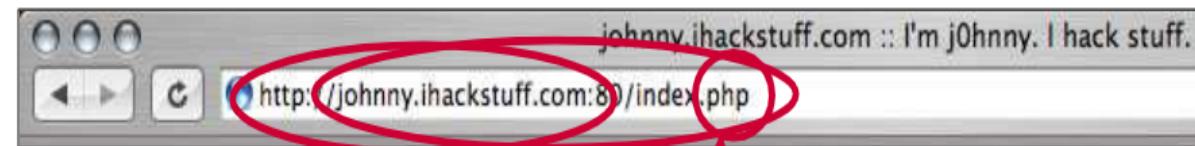
Advanced operators can be combined in some cases.

In other cases, mixing should be avoided.

Operator	Purpose	Mixes with other operators?	Can be used alone?	Does search work in			
				Web	Images	Groups	News
intitle	Search page title	yes	yes	yes	yes	yes	yes
allintitle	Search page title	no	yes	yes	yes	yes	yes
inurl	Search URL	yes	yes	yes	yes	not really	like intitle
allinurl	Search URL	no	yes	yes	yes	yes	like intitle
filetype	Search specific files	yes	no	yes	yes	no	not really
allintext	Search text of page only	not really	yes	yes	yes	yes	yes
site	Search specific site	yes	yes	yes	yes	no	not really
link	Search for links to pages	no	yes	yes	no	no	not really
inanchor	Search link anchor text	yes	yes	yes	yes	not really	yes
numrange	Locate number	yes	yes	yes	no	no	not really
daterange	Search in date range	yes	no	yes	not really	not really	not really
author	Group author search	yes	yes	no	no	yes	not really
group	Group name search	not really	yes	no	no	yes	not really
insubject	Group subject search	yes	yes	like intitle	like intitle	yes	like intitle
msgid	Group msgid search	no	yes	not really	not really	yes	not really

Some operators can only be used to search specific areas of Google, as these columns show.

Some operators search overlapping areas. Consider site, inurl and filetype.



SITE:

INURL:

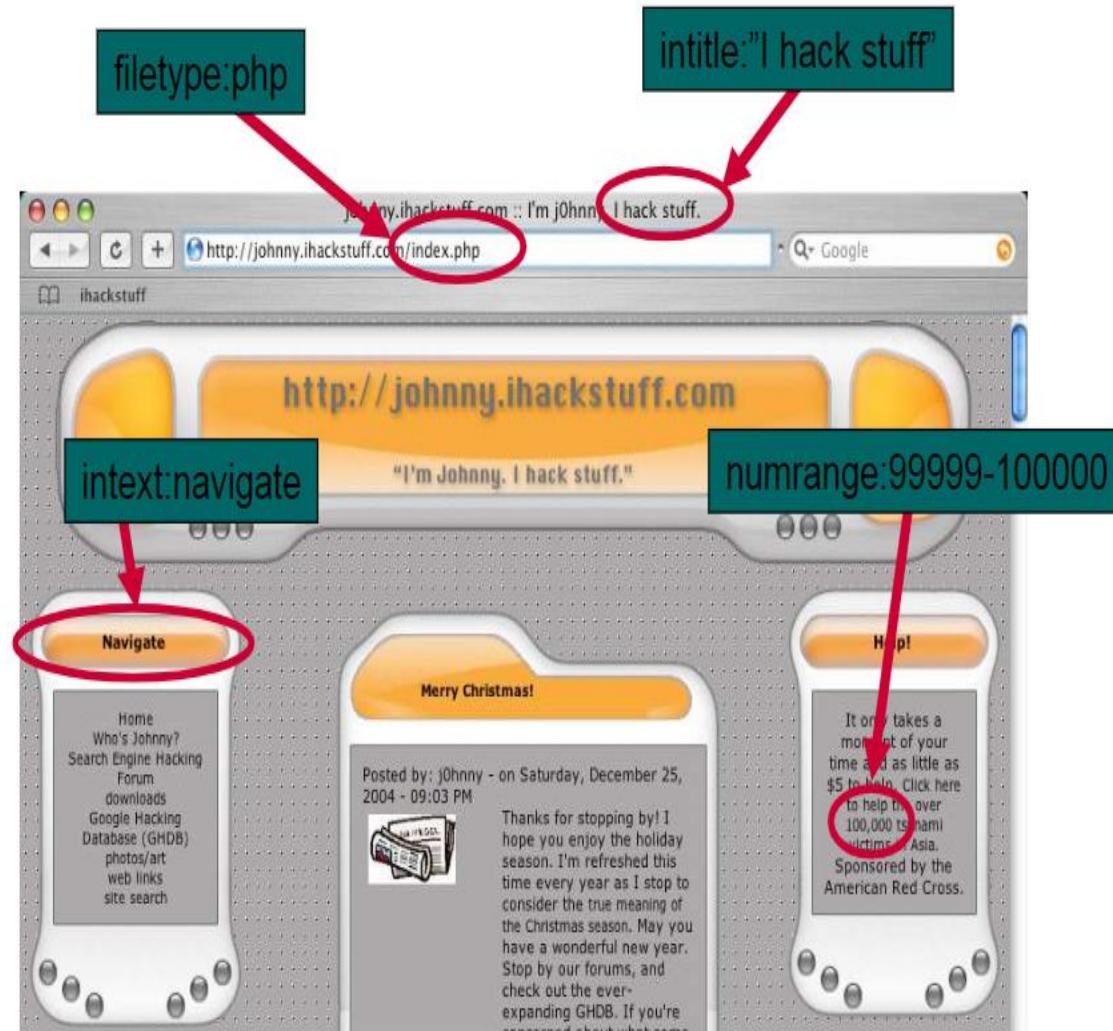
FILETYPE:

Site can not search port.

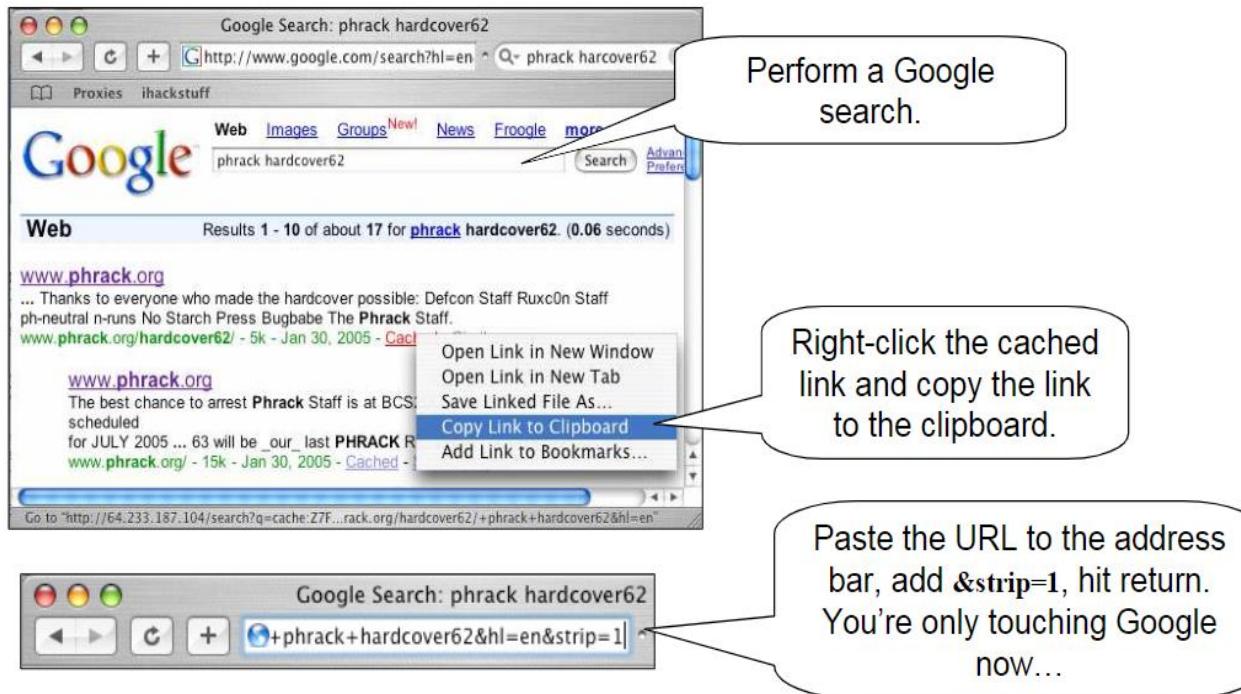
Inurl can search the whole URL, including port and filetype.

Filetype can only search file extension, which may be hard to distinguish in long URLs.

There are many ways to find the same page. These individual queries could all help find the same page.



Google Hacking Anónimo



Actividad

Instrucciones:

Con apoyo de los operadores avanzados de Google llevar a cabo las consultas que se te piden a continuación:

1. Consultar algunas instituciones de educación superior en México que se han visto comprometidas en los últimos años.
2. Consultar posibles sistemas públicos y abiertos de monitoreos de redes (Zabbix , Cacti, OpenNMS, etc..) de algunas empresas
3. Consultar información sensible pública en internet relacionada a bases de datos MySQL



Operator	Purpose	Mixes with other operators?	Can be used alone?
intitle	Search page title	yes	yes
allintitle	Search page title	no	yes
inurl	Search URL	yes	yes
allinurl	Search URL	no	yes
filetype	Search specific files	yes	no
allintext	Search text of page only	not really	yes
site	Search specific site	yes	yes
link	Search for links to pages	no	yes
inanchor	Search link anchor text	yes	yes
numrange	Locate number	yes	yes
daterange	Search in date range	yes	no
author	Group author search	yes	yes
group	Group name search	not really	yes
insubject	Group subject search	yes	yes
msgid	Group msgid search	no	yes

Ejemplo 1



site:edu.mx intitle:"hacked by"

X



www.iesgm.edu.mx > sh-html

Hacked By Shade – UGMEX CAMPUS OAXACA

12 mar. 2020 - Hacked By Shade. GreetZ : Prosox & Sxtz. Hacked By Shade <3. Sitios de Interes. Directorio · Recorrido Virtual · Titulación · Horarios ...

www.csfj.edu.mx > 2013 > junio > Hacked by TobaSec

Hacked by TobaSec – Colegio San Francisco Javier

Hacked by TobaSec. Home · 2013 · junio; Hacked by TobaSec. junio 11, 2013 /Blog/Colegio San Francisco Javier. Hacked by TobaSec ...

xxaniversario.uthh.edu.mx ▾ Traducir esta página

| >Hacked By: #AnonAlb<

[Hacked By # The Zeyth] |

cesigue.edu.mx ▾ Traducir esta página

Hacked by 70P-H4CK3R

Owned By 70P-H4CK3R [Libyana Hacker]. Zone-H : ToP-TeaM. I testify that there is no God but Allah and that Mohammad is His Messenger. Spical GR33Z ...

Ejemplo 2



intitle:"Cacti" AND inurl:"/monitor/monitor.php"



Todos

Imágenes

Shopping

Videos

Noticias

Más

Herramientas

7 resultados (0.33 segundos)

<http://cacti.tyrc.edu.tw> › monitor [Traducir esta página](#)

Cacti

Graphs monitor ; Monitoring ; Last Refresh : 9:28:13 pm. 172.20.11.4. Status: Up. IP Address:
172.20.11.4. Ping: 2.41 ms. Last Fail: Never. Availability: 99.96% ...

<http://mrtg.ffclrp.usp.br> › monitor [Traducir esta página](#)

Cacti

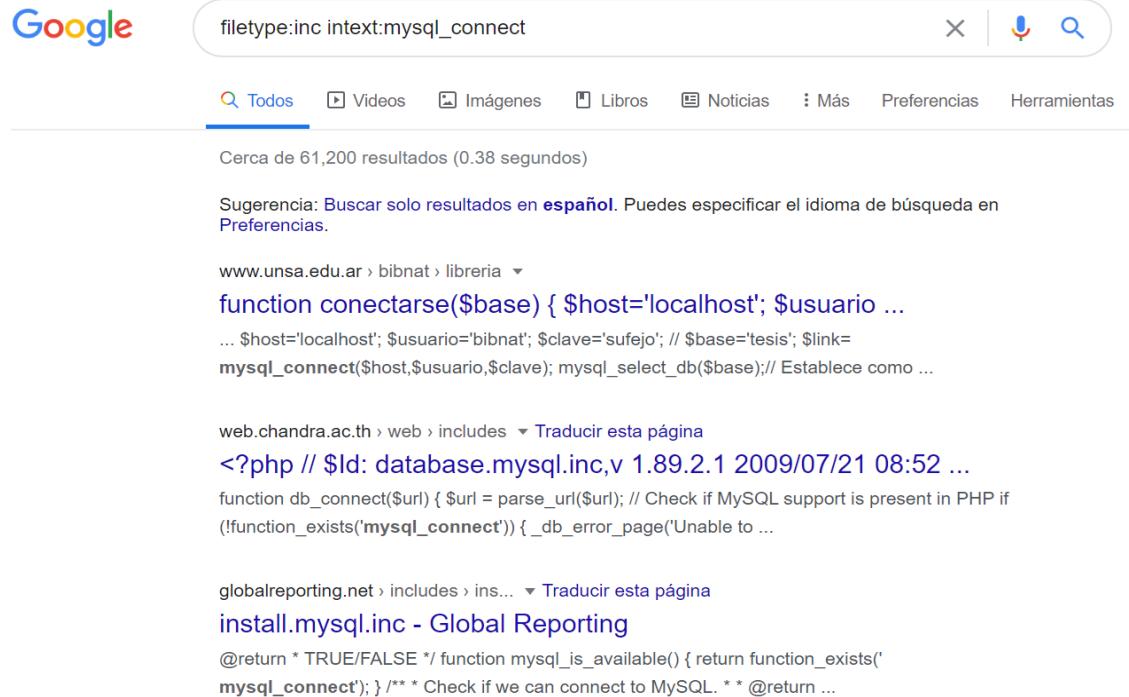
Graphs monitor weathermap ; Monitoring ; Last Refresh : 2:46:07 am. Legend. Normal,
Recovering, Down.

<http://monitor.vnu.edu.vn> › monitor [Traducir esta página](#)

Down Host Messages

143d 3h 33m 50s. Switch_interTTTV. Status: Up. IP Address: 10.150.0.3. Ping: 1.64 ms. Last
Fail: 2022-04-24 21:45:00. Availability: 98.9% ...

Ejemplo 3



Google

filetype:inc intext:mysql_connect

X |

[Todos](#) [Videos](#) [Imágenes](#) [Libros](#) [Noticias](#) [Más](#) Preferencias Herramientas

Cerca de 61,200 resultados (0.38 segundos)

Sugerencia: Buscar solo resultados en [español](#). Puedes especificar el idioma de búsqueda en [Preferencias](#).

www.unsa.edu.ar › bibnat › libreria ▾
`function conectarse($base) { $host='localhost'; $usuario ...
... $host='localhost'; $usuario='bibnat'; $clave='sufejo'; // $base='tesis'; $link=
mysql_connect($host,$usuario,$clave); mysql_select_db($base); // Establece como ...`

web.chandra.ac.th › web › includes ▾ [Traducir esta página](#)
`<?php // $Id: database.mysql.inc,v 1.89.2.1 2009/07/21 08:52 ...
function db_connect($url) { $url = parse_url($url); // Check if MySQL support is present in PHP if
(!function_exists('mysql_connect')) { _db_error_page('Unable to ...`

globalreporting.net › includes › ins... ▾ [Traducir esta página](#)
install.mysql.inc - Global Reporting
`@return * TRUE/FALSE */ function mysql_is_available() { return function_exists('mysql_connect'); } /** * Check if we can connect to MySQL. ** @return ...`

Open-Source Intelligence

Hay varios puntos de partida cuando se trata de adquirir inteligencia de código abierto sobre tu objetivo. La primera es mirar a la empresa en general. Como hacker querrás recopilar información sobre las ubicaciones que tiene la empresa.

Hay casos en los que esto puede resultar sencillo. Sin embargo, cada vez más, puede resultar más difícil. La razón por la que puede ser más difícil es que las empresas reconocen que cuanta más información proporcionen, más información se podrá utilizar en su contra.

Colección y análisis de información sobre amenazas

Identificación y mitigación de varios riesgos de negocio, convirtiendo las amenazas desconocidas en amenazas conocidas.

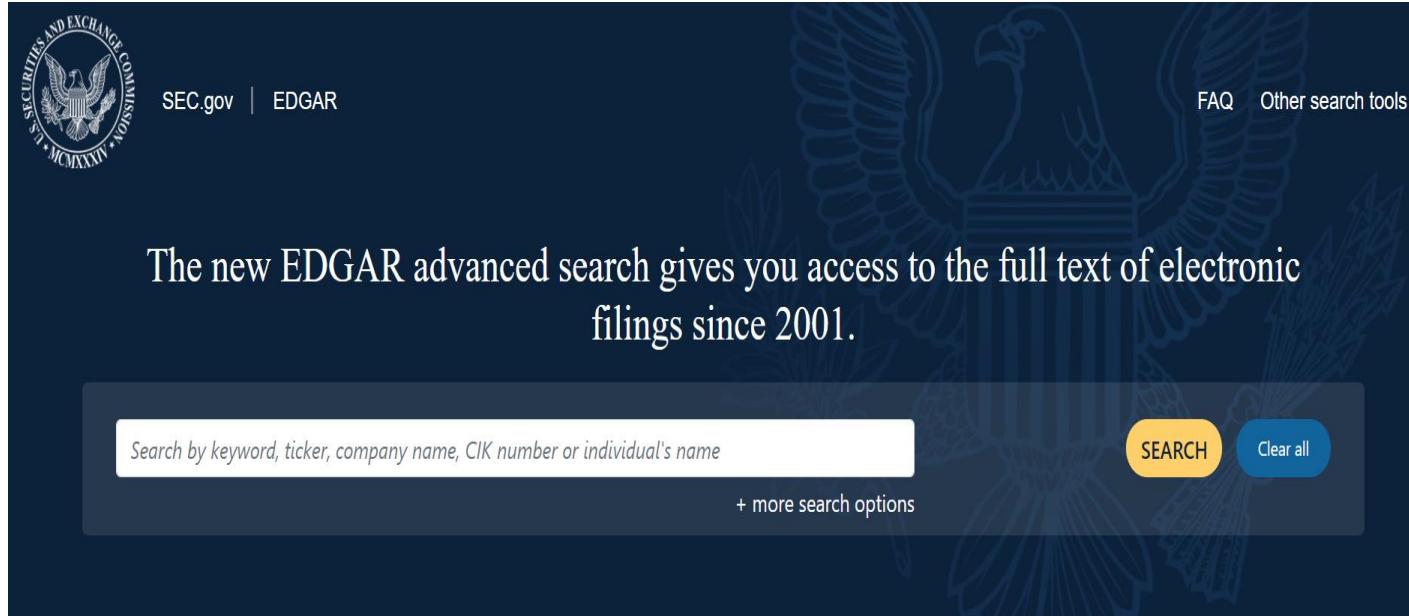
Centralizar los esfuerzos en implementar varias estrategias de defensa proactivas y avanzadas.

Usado por las organizaciones para monitorear, detectar y escalar varias amenazas que se encuentran dentro de las redes de las organizaciones.

Técnicas de correlación comúnmente utilizadas:

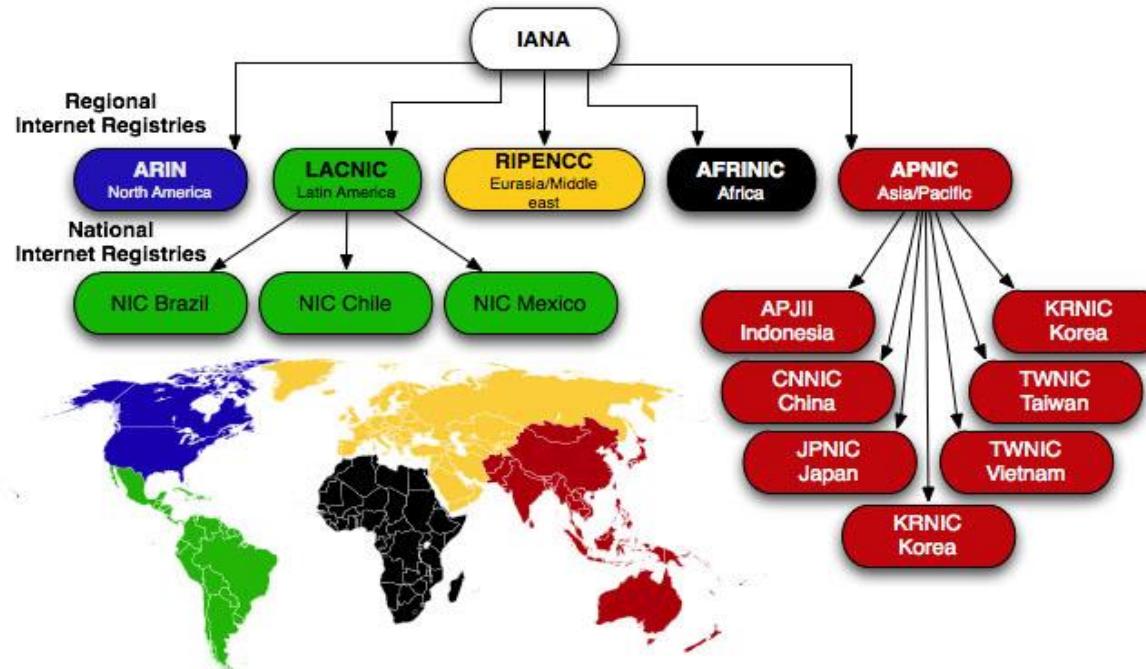
- Relacionar múltiples tipos y orígenes de incidentes a través de múltiples nodos
- Secuencia del incidente
- Persistencia del incidente
- Recopilación de datos orientada a incidentes

<https://www.sec.gov/edgar/search/>



The image shows the SEC.gov EDGAR search interface. At the top left is the SEC logo (Seal of the Securities and Exchange Commission). To its right are links for "SEC.gov" and "EDGAR". On the far right are links for "FAQ" and "Other search tools". A large, faint watermark of an eagle is visible across the background. The main text area reads: "The new EDGAR advanced search gives you access to the full text of electronic filings since 2001." Below this is a search bar with the placeholder text "Search by keyword, ticker, company name, CIK number or individual's name". To the right of the search bar are two buttons: a yellow "SEARCH" button and a blue "Clear all" button. Below the search bar is a link "+ more search options".

Registros de dominios



Diagnóstico DNS WhoIS Soporte Es En



WHOIS.MX

La herramienta "WHOIS" buscará en la base de datos del Registry .MX, el nombre proporcionado correspondiente al tipo de objeto seleccionado:

› **Nombre del objeto:**

› **Tipo de objeto:**

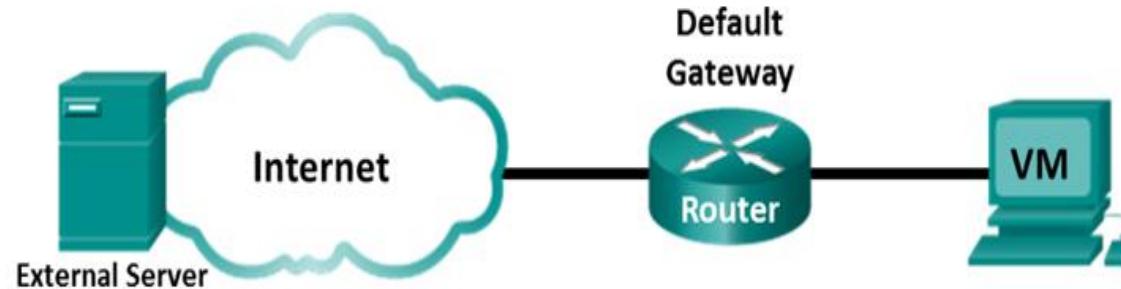
Nombre de Dominio (No es necesario escribir www)

Contacto

Buscar

Laboratorio - Explorando Maltego

Topología



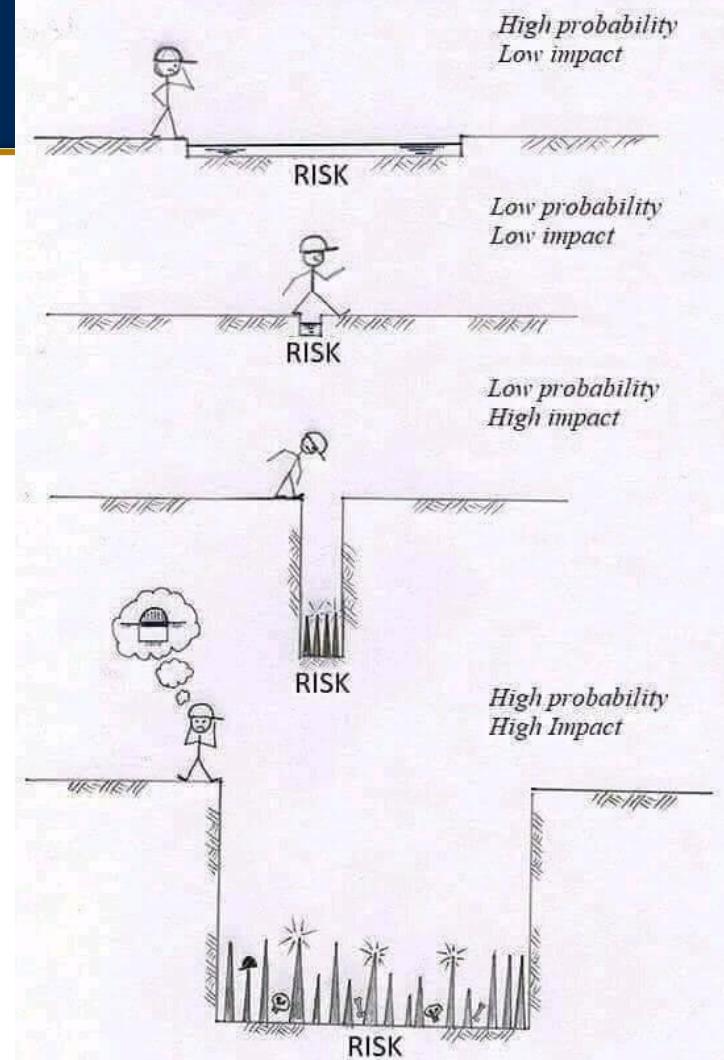
Objetivos del laboratorio

Parte 1: Instalar y configurar Maltego

Parte 2: Realizar un gráfico básico con Maltego

Laboratorio FootPrinting





Nuestros dispositivos informáticos

A menos que haya seleccionado recibir los resúmenes en papel para todas sus cuentas, usted utiliza sus dispositivos informáticos para acceder a los datos.

Si desea una copia digital del último resumen de la tarjeta de crédito, utiliza sus dispositivos informáticos para acceder a la página web del emisor de la tarjeta de crédito.

Si desea pagar su factura de la tarjeta de crédito en línea, accede a la página web de su banco para transferir los fondos con sus dispositivos informáticos



¿Qué es lo que motiva a los ciberdelincuentes?



A corto plazo quieren nuestro dinero



Caso: American Airlines

The State of Security

NEWS. TRENDS. INSIGHTS.

FEATURED ARTICLES LATEST SECURITY NEWS RESOURCES

Hackers Compromise United and American Airlines Customer Accounts, Book Free Trips



MARITZA SANTILLAN

 Follow @mrtzsanti

JAN 13, 2015 | LATEST SECURITY NEWS



A largo plazo quieren nuestra identidad digital

Además de robar su dinero para obtener una ganancia monetaria a corto plazo, los delincuentes desean obtener ganancias a largo plazo robando su identidad.



Ejemplo: robo de identidad médica

A medida que aumentan los costos médicos, el robo de la identidad médica también aumenta. Los ladrones de identidad pueden robar su seguro médico y usar sus beneficios de salud para ellos mismos, y estos procedimientos médicos ahora están en sus registros médicos.

Ejemplo: robo de identidad financiera

Los procedimientos anuales de declaración de impuestos pueden variar de un país a otro; sin embargo, los delincuentes ciberneticos consideran esto como una oportunidad. Por ejemplo, la población de los Estados Unidos necesita presentar sus impuestos antes del 15 de abril de cada año. El Servicio de impuestos internos (IRS) no marca la declaración de impuestos en comparación con la información del empleador hasta julio. Un ladrón de identidad puede generar una declaración de impuestos falsa y recolectar el reembolso. Los usuarios legítimos notarán cuando sus reembolsos sean rechazados por el IRS.

Tipos de datos de la organizaciones

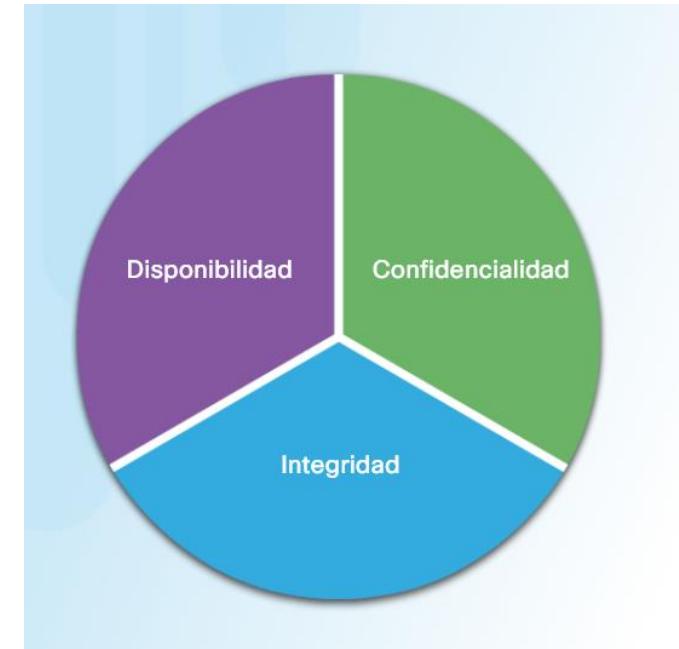
Los datos corporativos incluyen información del personal, propiedades intelectuales y datos financieros. La información del personal incluye el material de las postulaciones, la nómina, la carta de oferta, los acuerdos del empleado, y cualquier información utilizada para tomar decisiones de empleo.

La propiedad intelectual, como patentes, marcas registradas y planes de nuevos productos, permite a una empresa obtener una ventaja económica sobre sus competidores.

Los datos financieros, como las declaraciones de ingresos, los balances y las declaraciones de flujo de caja de una empresa brindan información sobre el estado de la empresa.

Conceptos de Seguridad de la Información (1/3)

- Confidencialidad (Confidentiality) - C
- Integridad (Integrity) - I
- Disponibilidad (Availability) - D
- Autenticidad (Authenticity)
- No repudio (Non-Repudiation)



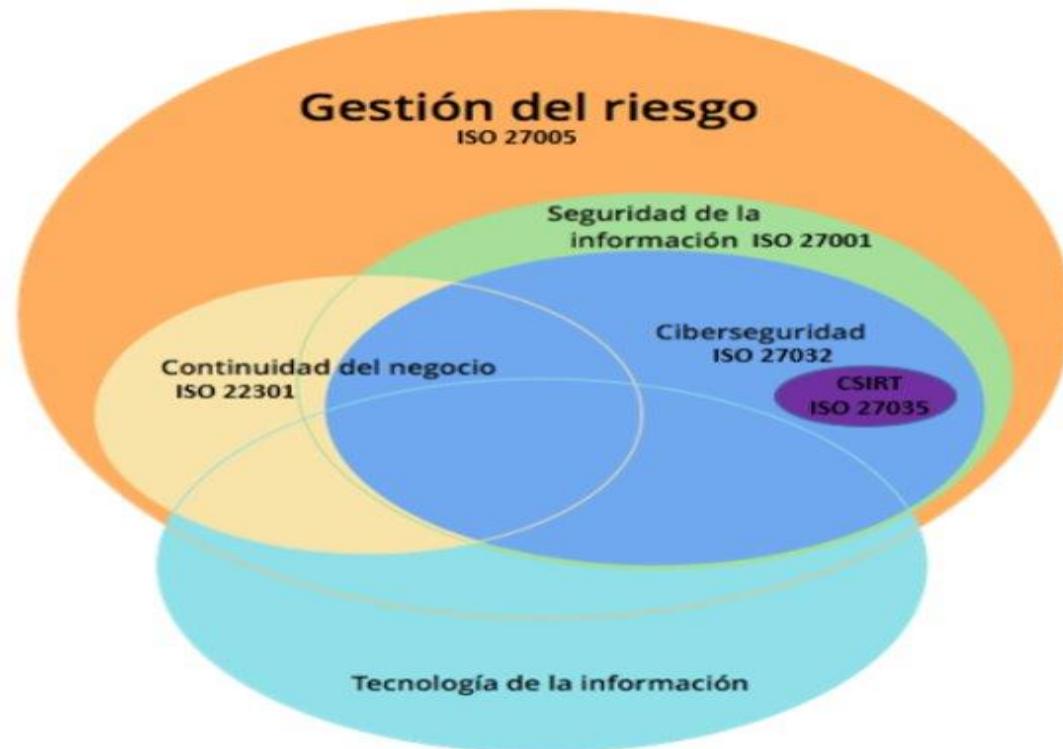
Conceptos de Seguridad de la Información (2/3)

- La Información como un activo del negocio
- Defensa en profundidad
- Políticas de seguridad de la información
 - Técnicas - configuración
 - Administrativas - comportamiento

Políticas de Seguridad de la Información: Las 4 P's

- Promiscuo (Promiscuous)
- Permisivo (Permissive)
- Prudente (Prudent)
- Paranóico (Paranoid)

Dimensiones de Seguridad de la Información



Laboratorio: comparar datos con un hash



= 79054025
255fb1a2
6e4bc422
aef54eb4

Las consecuencias a una violación a la seguridad

Proteger a las organizaciones contra cualquier ciberataque posible no es factible, por algunos motivos:

- La experiencia necesaria para configurar y mantener la red segura puede ser costosa.
- Los atacantes siempre seguirán encontrando nuevas maneras de apuntar a las redes.
- Con el tiempo, un ciberataque avanzado y dirigido tendrá éxito.

¿Qué es lo importante?

La prioridad, luego, será con qué rapidez su equipo de seguridad puede responder al ataque para minimizar la pérdida de datos, el tiempo de inactividad y la pérdida de ingresos.



¿Qué es lo importante?

El costo monetario de un ataque es mucho mayor que solo reemplazar los dispositivos perdidos o robados, invertir en la seguridad existente y fortalecer la seguridad física del edificio.

La empresa será responsable de comunicarse con todos los clientes afectados por la infracción y es posible que deba prepararse para un proceso jurídico.

Con toda esta confusión, los empleados pueden elegir irse de la empresa. Es posible que la empresa necesite centrarse menos en el crecimiento y más en la reparación de su reputación.

Ejemplo 1 de violación de seguridad

LastPass



Ejemplo 1 de violación de seguridad

El administrador de contraseñas en línea, LastPass, **detectó actividad inusual** en su red en julio de 2015. Resultó que los hackers habían **robado las direcciones de correo electrónico** de los usuarios, los recordatorios de la contraseña y **los hashes de autenticación**. Afortunadamente para los usuarios, los hackers no pudieron obtener el repositorio de la contraseña cifrada de nadie.

Aunque hubo una violación a la seguridad, LastPass pudo de todos modos proteger la información de las cuentas de los usuarios. LastPass **requiere la verificación de correo electrónico o la autenticación de varios factores** cada vez que hay un nuevo inicio de sesión desde un dispositivo o una dirección IP desconocidos. Los hackers también necesitarían la contraseña principal para acceder a la cuenta.

Los usuarios de LastPass también tienen cierta responsabilidad en la protección de sus cuentas. Los usuarios deben utilizar siempre contraseñas principales complejas y cambiar las contraseñas principales periódicamente. Los usuarios siempre deben tener cuidado con los ataques de phishing.

Reflexión

Si los usuarios y los proveedores de servicios usan las herramientas y los procedimientos adecuados para proteger la información de los usuarios, los datos de los usuarios podrían protegerse, incluso en el caso de una brecha en la seguridad.



Ejemplo 2 de violación de seguridad



Ejemplo 2 de violación de seguridad

El fabricante de juguetes de alta tecnología para niños, Vtech, sufrió una **violación de seguridad** en su **base de datos** en noviembre de 2015. Esta violación de seguridad podría afectar a millones de clientes en todo el mundo, incluidos los niños. La violación de seguridad de los datos expuso información confidencial, incluidos nombres de clientes, direcciones de correo electrónico, contraseñas, imágenes y registros de chat.

Las tablets de juguete se habían convertido en un nuevo objetivo para los hackers. Los clientes habían compartido fotografías y habían utilizado las funciones de chat en las tablets de juguete. La información no se aseguró correctamente, y el sitio web de la empresa **no admitía la comunicación segura con SSL**. Aunque la violación de seguridad no expuso la información de ninguna tarjeta de crédito ni datos de identificación personal, la empresa fue suspendida en la bolsa de valores debido a la preocupación por la inmensidad del ataque.

Vtech no protegió la información de los clientes correctamente y se vio expuesta durante la violación de seguridad.

Reflexión

Para los padres, es una llamada de atención para ser más cuidadosos sobre la privacidad de sus hijos en línea y solicitar una mejor seguridad para los productos de los niños.

En cuanto a los fabricantes de productos conectados a la red, deben ser más agresivos en la protección de los datos de clientes y privacidad ahora y en el futuro, ya que el panorama de los ciberataques evoluciona.

Ejemplo 3 de violación de seguridad



Ejemplo 3 de violación de seguridad

Equifax Inc. es una de las agencias nacionales de informes de crédito para el consumidor de Estados Unidos. Esta empresa recopila información de millones de clientes particulares y empresas en todo el mundo. En función de la información recopilada, se crean puntajes de crédito e informes de crédito acerca de los clientes. Esta información podría afectar a los clientes al solicitar préstamos y buscar empleo.

Ejemplo 3 de violación de seguridad

En septiembre de 2017, Equifax anunció públicamente un evento de violación de datos. Los atacantes aprovecharon una vulnerabilidad en el software de aplicaciones web Apache Struts. La empresa cree que los delincuentes ciberneticos tuvieron acceso a millones de datos personales sensibles de los consumidores estadounidenses entre mayo y julio de 2017. Los datos de carácter personal incluyen nombres completos de los clientes, números de seguro social, fechas de nacimiento, direcciones y otra información personal identificatoria. Hay evidencia de que la violación podría haber afectado a clientes de Reino Unido y Canadá.

Ejemplo 3 de violación de seguridad

Equifax creó un sitio web exclusivo que permite a los consumidores determinar si su información se vio comprometida, e iniciar sesión para que puedan controlar el crédito y protegerse contra el robo de identidad. Mediante el uso de un nuevo nombre de dominio en lugar de utilizar un subdominio de equifax.com, se permitió que personas maliciosas crearan sitios web no autorizados con nombres similares. Estos sitios web pueden utilizarse como parte de un plan de suplantación de identidad que intenta engañar para que se proporcione información personal. Además, un empleado de Equifax proporcionó un enlace web incorrecto en medios sociales para clientes preocupados. Afortunadamente, este sitio web fue dado de baja dentro de las 24 horas. Fue creado por una persona que lo utilizaba como una oportunidad educativa para revelar las vulnerabilidades que existen en la página de respuesta de Equifax.

Reflexión

En estas situaciones, lo único que puede hacer es estar alerta cuando proporcione información personal de identificación en Internet. Revise sus informes crediticios periódicamente (una vez al mes o una vez por trimestre). Denuncie de inmediato cualquier información falsa, como solicitudes de crédito que no inició o compras en sus tarjetas de crédito que no realizó.

El centro de operaciones de seguridad moderno

Elementos de un SOC

Los centros de operaciones de seguridad (SOC) proporcionan una amplia gama de servicios:

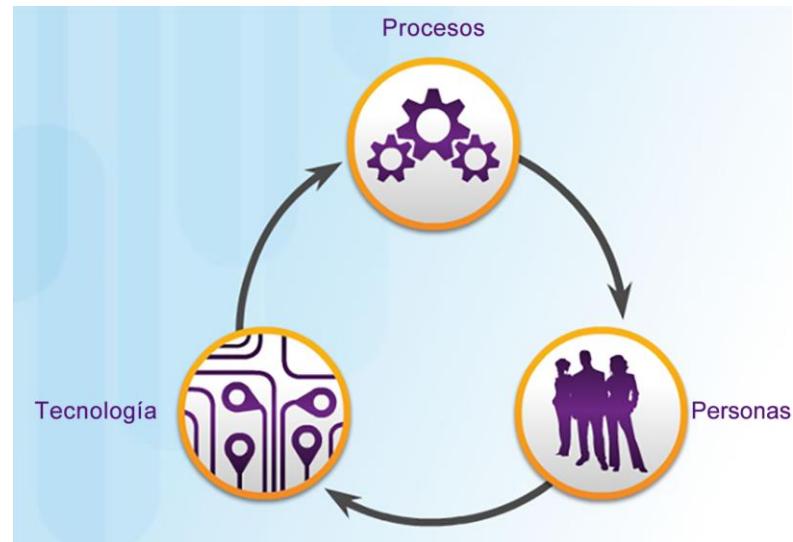
- Monitoreo
- Administración
- Soluciones completas de amenazas
- Seguridad alojada

Los SOC pueden:

- encontrarse dentro de la empresa, ser de su propiedad y ser operados por esta.
- Los elementos pueden ser contratados para los proveedores de seguridad.

Los elementos principales de un SOC son:

- Personas
- Procesos
- Tecnología



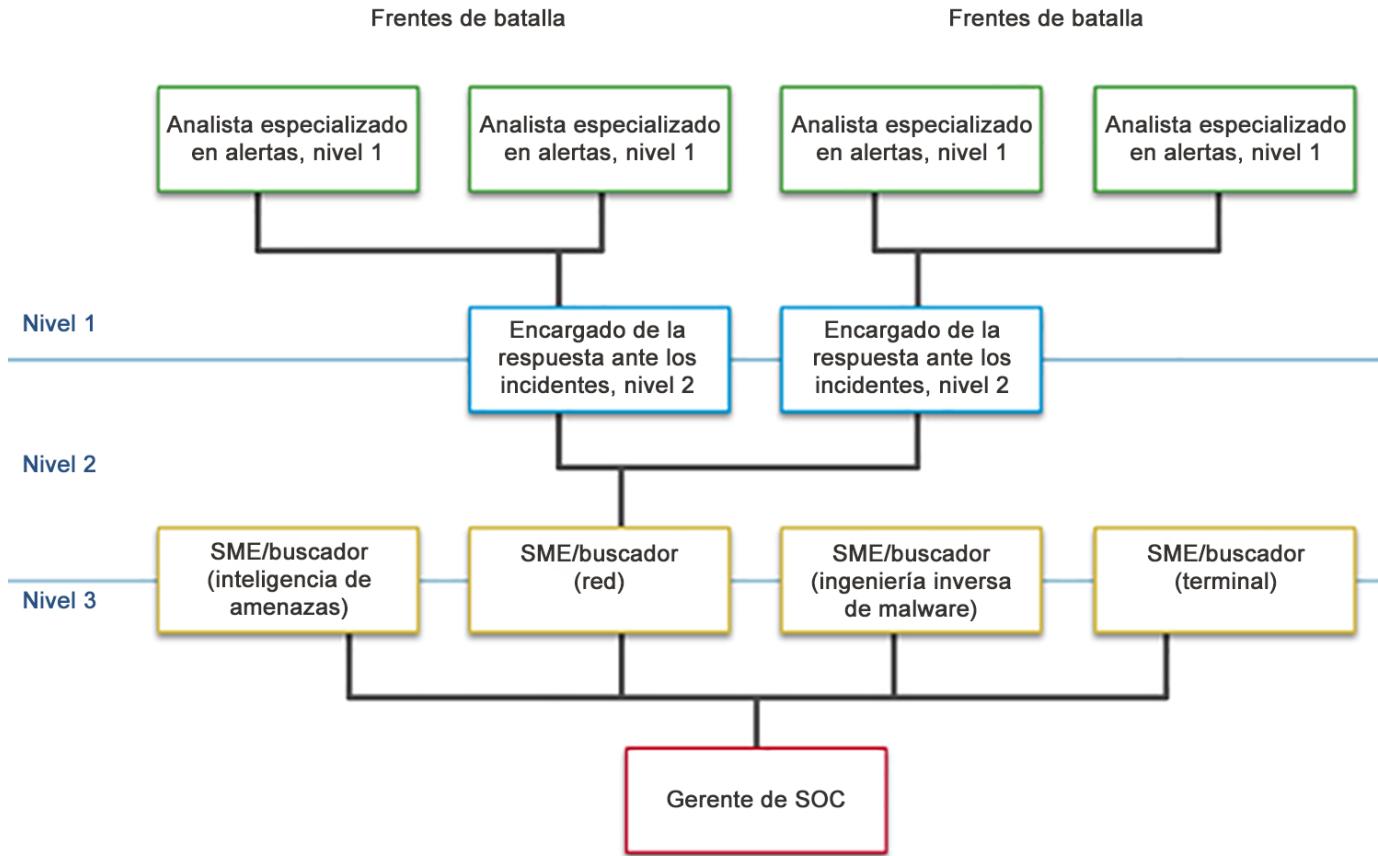
El centro de operaciones de seguridad moderno

Personas en el SOC

SANS Institute (www.sans.org) divide en cuatro los roles de la gente en los SOC:

- **Nivel 1: Analista de alertas**
- **Nivel 2: Encargado de respuesta ante incidentes**
- **Nivel 3: Experto en la materia (SME)/Cazador**
- **Gerente de SOC**

¿Pueden adivinar las responsabilidades de cada uno de los cargos de trabajo?



El centro de operaciones de seguridad moderno

Proceso en el SOC

- Un analista de alerta de nivel 1 comienza con el monitoreo de las colas de alertas de seguridad.
- Un analista de alerta de nivel 1 comprueba si una alerta que se activó en el software de emisión de boletos representa un verdadero incidente de seguridad.
- El incidente puede reenviarse a investigadores o resolverse como falsa alarma.

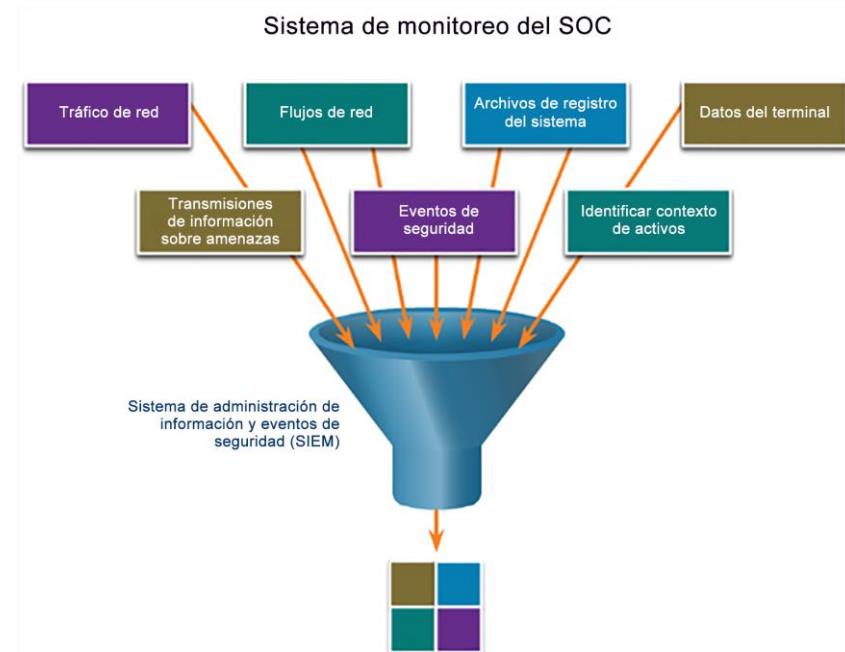


El centro de operaciones de seguridad moderno

Tecnologías en el SOC

Sistemas de administración de información y eventos de seguridad (SIEM):

- Recopilar y filtrar datos.
- Detectar y clasificar amenazas.
- Analizar e investigar las amenazas.
- Implementar medidas preventivas.
- Examinar amenazas futuras.



El centro de operaciones de seguridad moderno

Seguridad empresarial y administrada

Las organizaciones pueden implementar un SOC de nivel empresarial.

El SOC puede ser:

- Una solución interna completa
- Terciarizada en al menos una parte de las operaciones del SOC a un proveedor de soluciones de seguridad.



Comparación entre seguridad y disponibilidad

- La mayoría de las redes empresariales deben funcionar en todo momento.
- El tiempo de actividad buscado suele medirse por la cantidad anual de minutos de inactividad. Un tiempo de actividad de "cinco nueves" indica que la red estuvo activa el 99,999% del tiempo (o inactiva no más de 5 minutos en el año).
- Logre siempre un equilibrio entre un buen nivel de seguridad y la posibilidad de que la empresa funcione.

Disponibilidad %	Tiempo de inactividad
99,8%	17,52 horas
99,9% ("tres nueves")	8,76 horas
99,99% ("cuatro nueves")	52,56 minutos
99,999% ("cinco nueves")	5,256 minutos
99,9999% ("seis nueves")	31,5 segundos
99,99999% ("siete nueves")	3,15 segundos

Ciberguerra (Cyberwar)

La guerra cibernética es un conflicto basado en Internet que implica la penetración de sistemas de computación y redes de otros países.

Estos atacantes tienen los recursos y conocimientos para lanzar ataques masivos basados en Internet contra otros países para causar daños o para interrumpir los servicios, como apagar toda la red de energía.

Anatomía de un ataque cibernético

¿Cuál es el propósito de la ciberguerra?

- **Ganar ventajas sobre los adversarios:**

Invadir la infraestructura de otro país

Robar los secretos de defensa

Recopilar información sobre la tecnología para reducir las brechas en sus sectores industriales y militares.



¿Cuál es el propósito de la ciberguerra?

- Dañar la infraestructura de otros países y costar vidas en las naciones específicas:

Ej. Afectar la red eléctrica de una ciudad importante.

El tráfico se puede ver interrumpido.

El intercambio de bienes y servicios se detiene.

Los pacientes no pueden obtener el cuidado necesario en situaciones de emergencia.



¿Cuál es el propósito de la ciberguerra?

Si el gobierno no puede defenderse de los ataques cibernéticos, los ciudadanos pueden perder la confianza en la capacidad del gobierno de protegerlos.

La guerra cibernética puede **desestabilizar una nación**, interrumpir el comercio y afectar la fe de los ciudadanos en su gobierno sin invadir físicamente el país objetivo.



Vulnerabilidades en la seguridad de la información

Las vulnerabilidades de seguridad son cualquier tipo de defecto en software o hardware.

Después de obtener conocimientos sobre una vulnerabilidad, los usuarios malintencionados intentan explotarla.

Un *ataque* es el término que se utiliza para describir un programa escrito para aprovecharse de una vulnerabilidad conocida.

Clasificación de las vulnerabilidades en la seguridad

- 1. Desbordamiento del búfer.**
- 2. Entrada no validada.**
- 3. Condiciones de carrera.**
- 4. Debilidades en las prácticas de seguridad.**
- 5. Problemas de control de acceso.**

Actividad: identificar la terminología de la vulnerabilidad

Término	Descripción
Entrada no validada	Datos que entran al programa con contenido malicioso, diseñado para que este se comporte de manera no deseada.
Debilidad en las prácticas de seguridad	Cuando los desarrolladores intentan crear sus propias aplicaciones de seguridad.
Condiciones de carrera	Cuando el resultado de un evento depende de los resultados ordenados o temporizados.
Desbordamiento del buffer	Cuando una aplicación maliciosa accede a la memoria asignada a otros procesos.
Problemas de control de acceso	Regulación incorrecta de quién hace qué y qué puede hacer con los recursos.

Tipos de malware y sus síntomas



Tipos de Malware

Malware, acrónimo para el inglés “Malicious Software” (Software malicioso), es cualquier código que pueda utilizarse para robar datos, evitar los controles de acceso, ocasionar daños o comprometer un sistema.

Tipos de Malware

Spyware

Adware

Bot

Ransomware

Scareware

Rootkit

Virus

Troyano

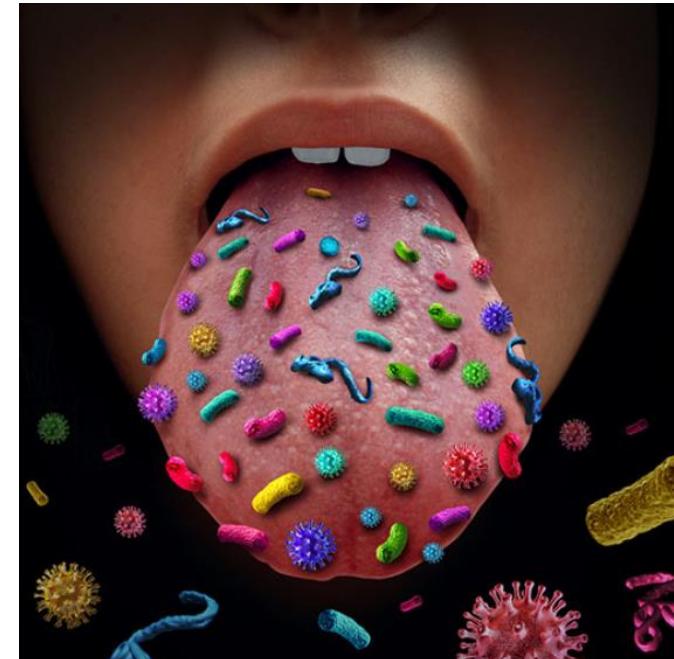
Gusanos

Hombre en el medio (MitM)

Hombre en el móvil (MitMo)

Síntomas del Malware

1. Aumento del uso de la CPU.
2. Disminución de la velocidad de la computadora.
3. La computadora se congela o falla con frecuencia.
4. Hay una disminución en la velocidad de navegación web.
5. Existen problemas inexplicables con las conexiones de red.
6. Se modifican los archivos.
7. Se eliminan archivos.
8. Hay una presencia de archivos, programas e iconos de escritorio desconocidos.
9. Se ejecutan procesos desconocidos.
10. Los programas se cierran o reconfiguran solos.



Actividad: identificar los tipos de malware

Término	Descripción
Bot	Malware diseñado para entrar en acción de manera automática, generalmente en línea.
Ransomware	Malware diseñado para mantener cautivo un sistema computacional o los datos que contiene hasta que se realice un pago.
Rootkit	Malware diseñado para modificar el sistema operativo a fin de crear una puerta trasera.
Spyware	Generalmente agrupado con software legítimo, este malware está diseñado para realizar un seguimiento de la actividad del usuario.
Troyano	Código malintencionado que se adjunta a otros archivos ejecutables, generalmente de programas legítimos.
Virus	Malware que ejecuta operaciones maliciosas bajo la apariencia de una operación deseada.
Adware	Agrupado en algunos casos con otro software, este malware está diseñado para mostrar automáticamente anuncios publicitarios.
MitMo	Malware que se utiliza para tomar el control de un dispositivo móvil.
Scareware	Malware diseñado para persuadir al usuario para que realice alguna acción específica en función del temor.
Gusano	Código malicioso que se replica atacando de manera independiente las vulnerabilidades en las redes.

Métodos de infiltración



La ingeniería social es un **ataque de acceso** que intenta manipular a las personas para que realicen acciones o divulguen información confidencial.

Los ingenieros sociales con frecuencia dependen de la **disposición de las personas para ayudar**, pero también se aprovechan de sus vulnerabilidades.



Tipos de ataques de Ingeniería Social

Pretexto: esto es cuando un atacante llama a una persona y miente en el intento de obtener acceso a datos privilegiados. Un ejemplo implica a un atacante que pretende necesitar datos personales o financieros para confirmar la identidad del objetivo.

Seguimiento: esto es cuando un atacante persigue rápidamente a una persona autorizada a un lugar seguro.

Algo por algo (quid pro quo): esto es cuando un atacante solicita información personal de una parte a cambio de algo, por ejemplo, un obsequio.

Decodificación de contraseñas Wi-Fi

La decodificación de contraseñas Wi-Fi es el proceso de detección de la contraseña utilizada para proteger la red inalámbrica. Estas son algunas técnicas utilizadas en la decodificación de contraseñas:

Ingeniería social.

Ataques por fuerza bruta.

Monitoreo de la red.

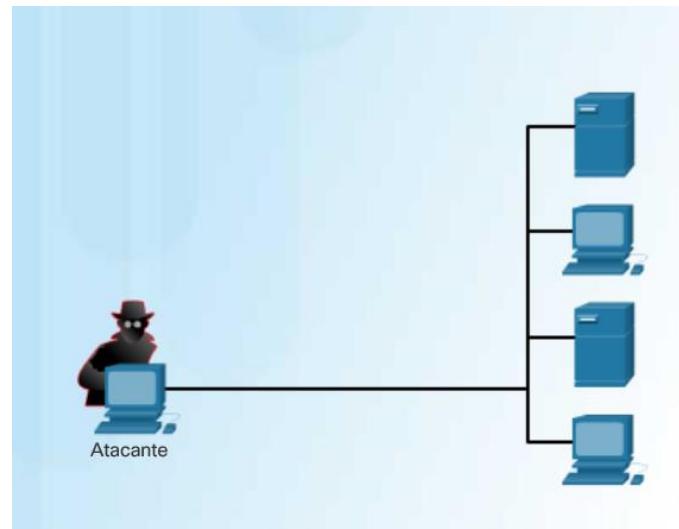
Suplantación de identidad

La suplantación de identidad es cuando una persona maliciosa envía un correo electrónico fraudulento disfrazado como fuente legítima y confiable. El objetivo de este mensaje es engañar al destinatario para que instale malware en su dispositivo o comparta información personal o financiera.



Aprovechamiento de vulnerabilidades

El aprovechamiento de vulnerabilidades es otro método común de infiltración. Los atacantes analizan las computadoras para obtener información.



Existen dos tipos principales de ataques DoS:

Cantidad abrumadora de tráfico: esto ocurre cuando se envía una gran cantidad de datos a una red, a un host o a una aplicación a una velocidad que no pueden administrar.

Paquetes maliciosos formateados: esto sucede cuando se envía un paquete malicioso formateado a un host o una aplicación y el receptor no puede manejarlo.

Un ataque DoS distribuido (DDoS) es similar a un ataque DoS pero proviene de múltiples fuentes coordinadas. Por ejemplo, un ataque DDoS podría darse de la siguiente manera:

Un atacante crea una red de hosts infectados, denominada botnet. Los hosts infectados se denominan zombies. Los zombies son controlados por sistemas manipuladores.

Envenenamiento SEO

El objetivo más común del envenenamiento SEO es aumentar el tráfico a sitios maliciosos que puedan alojar malware o ejercer la ingeniería social. Para forzar un sitio malicioso para que califique más alto en los resultados de la búsqueda, los atacantes se aprovechan de los términos de búsqueda populares.

