

Glosario



Instituto Tecnológico de Tlalnepantla Tecnologías de seguridad en software



Docente: Hilda Díaz Rincón

Alumna: Espino Horta Maria Jose

Grupo: T92 Fecha: 30/08/21

ADWARE



- Malware oculto, que muestra anuncios
- Referencia:
- <https://es.malwarebytes.com/adware/>

AMENAZA



- Todo lo que va en contra a la seguridad de información
- Vulnerabilidades
- Referencia:
- <http://www.seguridadinformatica.unlu.edu.ar/?q=node/12>

Antivirus



- Software
 - Detecta
 - Evita
 - Malware
-
- Referencia:
 - <https://espanol.verizon.com/info/definitions/antivirus/>

Borrado seguro



- Finaliza el ciclo de vida de la información
 - Enfoque de seguridad
 - Destrucción de la información
-
- Referencia:
 - https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_ciberseguridad_borrado_seguro_metad_o.pdf

Bots



- Spiders, rastreadores y bots web
 - Control total de un equipo
-
- Referencia:
 - <https://mx.norton.com/internetsecurity-malware-what-are-bots.html>

Bug



- Problema en un computador o software
 - Resultado indeseado
-
- Referencia:
 - <https://www.eleconomista.com.mx/tecnologia/que-es-un-bug-20200131-0079.html>

Centro de respaldo



- Procesamiento de datos
 - Principal
 - Contingencia
-
- Referencia:
 - <https://glosarios.servidor-alicante.com/ciberseguridad/centro-de-respaldo>

Certificado de autenticidad



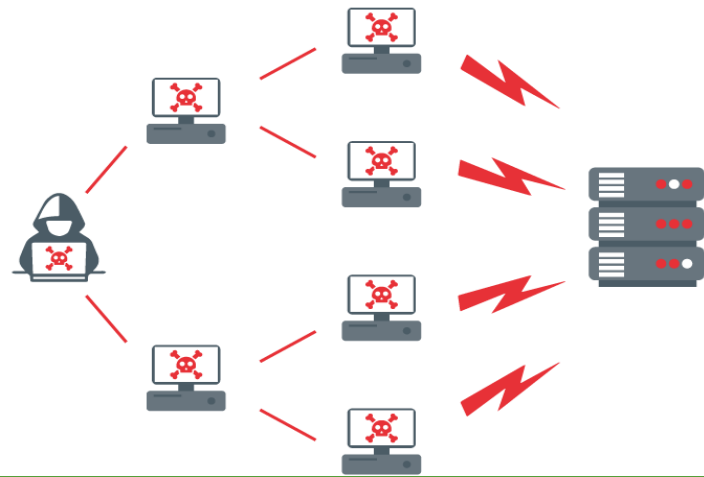
- Etiqueta
 - Seguridad
 - Licencia legal
 - Impedir falsificaciones
-
- Referencia:
 - <https://glosarios.servidor-alicante.com/ciberseguridad/certificado-de-autenticidad>

Ciberataque



- Conjunto de acciones
 - Sistemas de información
 - Perjudicar
-
- Referencia:
 - <https://www.iberdrola.com/innovacion/ciberataques>

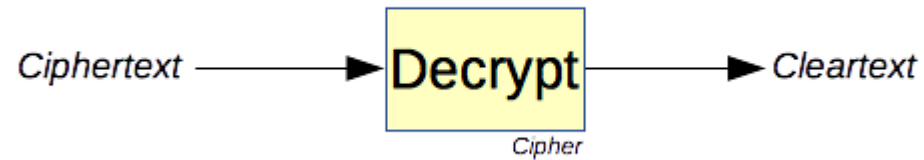
Denegación de servicio



- Ataques no planificados
- Solicitudes
- Saturar una red o servidor
- Dispositivos de red.
- Referencia:
 - https://www.f5.com/es_es/services/resources/glossary/denial-of-service

Descifrado

- Transformar un texto cifrado
- Texto simple
- Algoritmo criptográfico
- Referencia:
- <https://developer.mozilla.org/es/docs/Glossary/Decryption>



Detección de anomalías



- Detectar tendencias
- Identificar datos atípicos
- Anticipar de fluctuaciones de trafico

• Referencia:

• <https://www.atinternet.com/es/glosario/deteccion-de-anomalias/>

Equipo azul



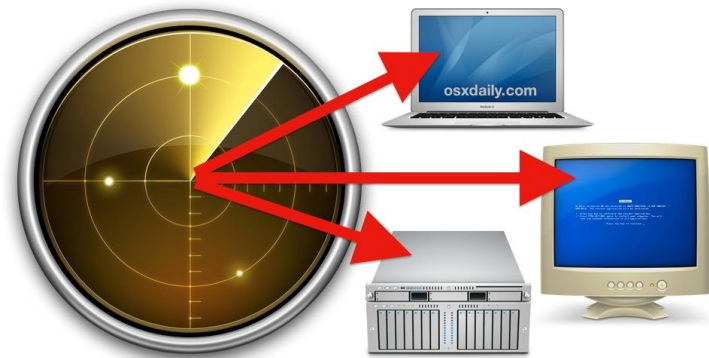
- Profesionales en seguridad
- Cualquier tipo de amenaza
- Fortalecer
- Intruso
- Defensas
- Referencia:
- <https://intelequia.com/blog/post/2088/red-team-y-blue-team-funciones-y-diferencias-en-ciberseguridad>

Equipo rojo



- Emuladores de ataques
 - Explotación de vulnerabilidades
 - Defenderse
 - Ataques
 - Blueteam
-
- Referencias:
 - <https://www.unir.net/ingenieria/revista/red-blue-purple-team-ciberseguridad/>

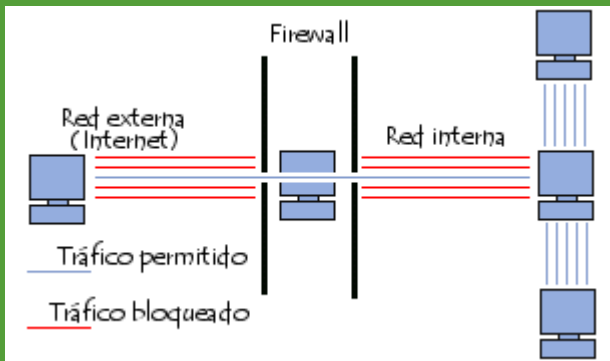
Escaneo de puertos



- Sistema informático
- Acceso a información
- Detectar vulnerabilidades
- Fines no éticos

- Referencia:
- https://protecciondatos-lopd.com/empresas/escaneo-de-puertos/#Que_es_el_escaneo_de_puertos

Filtrado de paquetes



- Control de acceso a una red
 - Análisis de paquetes
 - Limitar servicios
-
- Referencias:
 - <https://www.ibm.com/docs/es/i/7.2?topic=handling-ip-packet-filtering>

Fraude del CEO



- Delincuentes
- Engañar empleados
- Transferencias de alto valor económico

- Referencia:
- <https://www.xataka.com/seguridad/que-fraude-ceo-que-no-hay-que-fiarse-tu-jefe-asi-enganan-ciberdelicuentes-logran-saltarse-filtros-antispam>

Fuga de datos



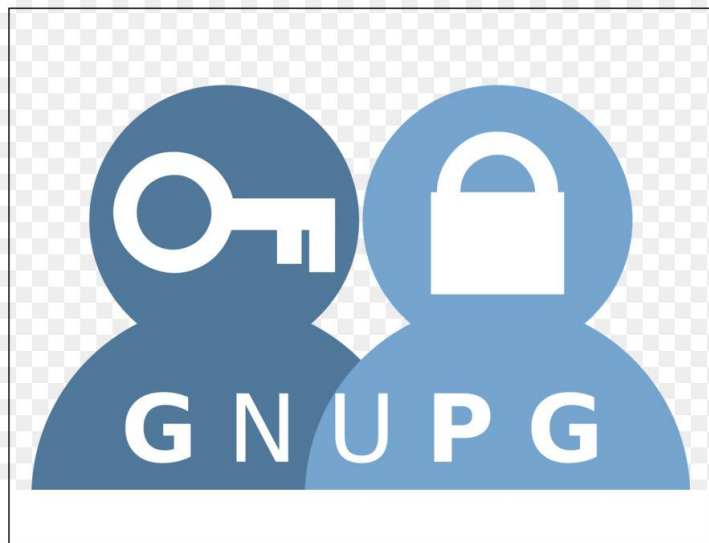
- Datos sensibles
 - Expuestos involuntariamente
 - Almacenamiento mal configurado
-
- Referencia:
 - <https://www.micromouse.com/2021/05/19/que-es-la-fuga-de-datos-y-como-prevenir-la/>

Gestión de incidentes



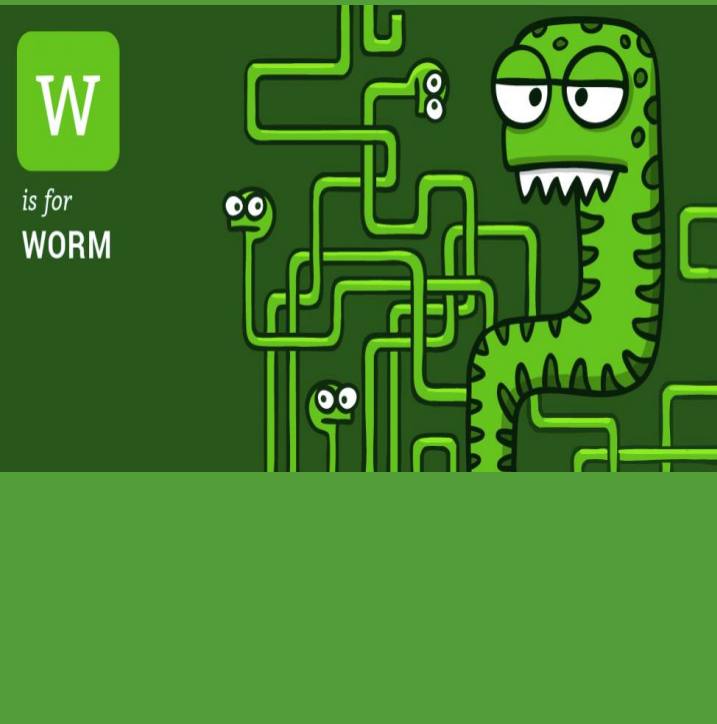
- Minimizar impactos
 - Empresas
 - Corrección de errores
 - Soporte técnico
-
- Referencia:
 - <https://www.zendesk.com.mx/blog/gestion-de-incidentes/>

GNU Privacy Guard



- Sistema de gestión
 - Claves
 - Comandos
 - Integración de aplicaciones
-
- Referencia:
 - <https://gnupg.org/>

Gusano



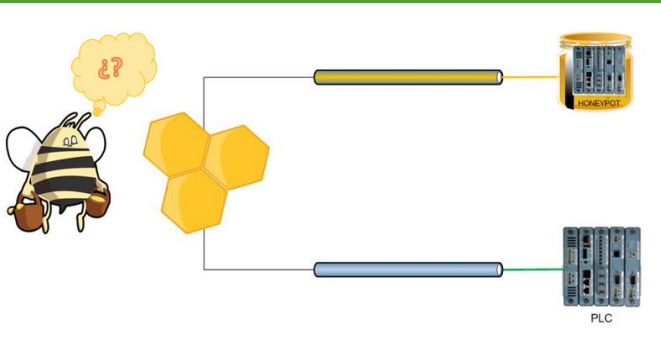
- Malware
 - Duplica
 - Infecta otras computadoras
-
- Referencia:
 - <https://www.avast.com/es-es/c-computer-worm>

Hacker



- Persona o comunidad
 - Conocimientos informáticos
 - Modificaciones
-
- Referencia:
 - <https://www.significados.com/hacker/>

Honeypot



- Señuelo
 - Para obtener información
 - Cibercriminales
 - Distracción de objetivos
-
- Referencia:
 - <https://latam.kaspersky.com/resource-center/threats/what-is-a-honeypot>

Huella digital

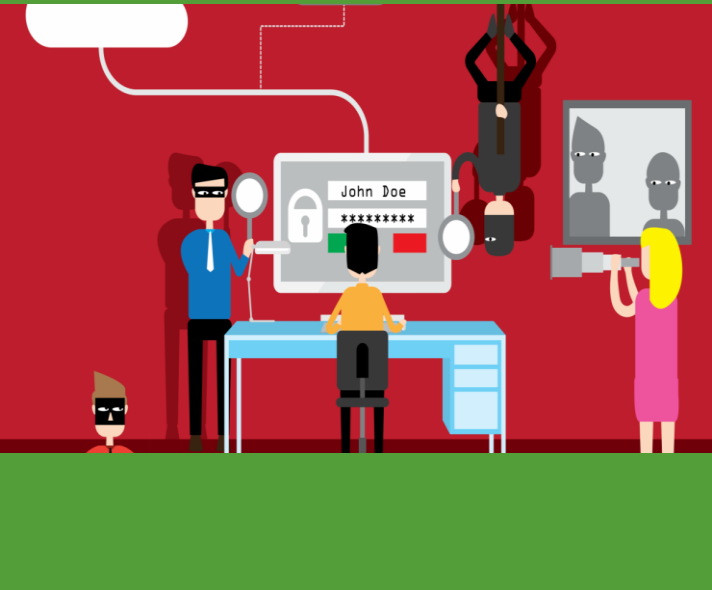


- Marca de identidad
- Internet
- Comportamiento en la red
- Referencia:
- <https://recfaces.com/es/articles/huella-digital>

Identificación

- Decirle al sistema quien esta “entrando”

- Referencia:
- <https://www.infosecuritymexico.com/es/ciberseguridad.html>



Incidente de seguridad



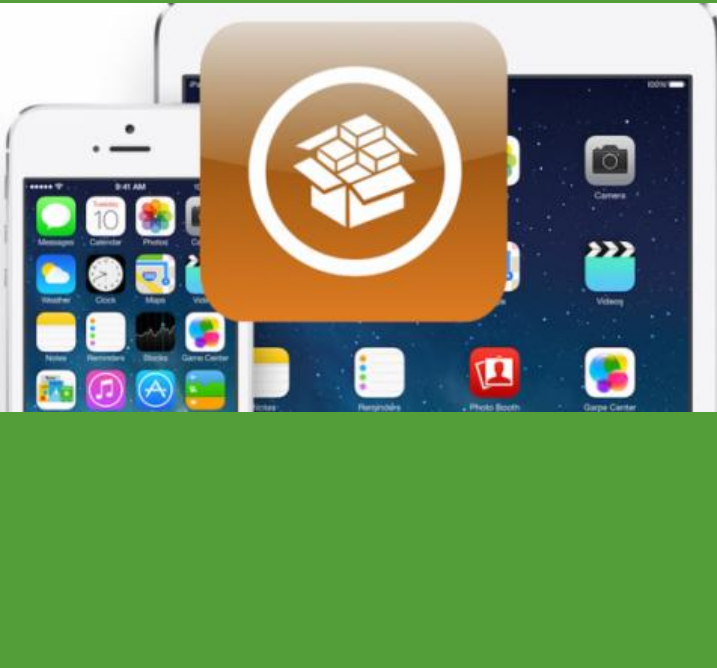
- Serie de eventos
 - Comprometer las operaciones del negocio
 - Perdidas uso indebido de información
-
- Referencia:
 - <https://www.uv.mx/csirt/que-es-un-incidente-de-ciberseguridad/>

Insider



- Ex –empleados
 - Acceso a información
 - Flujo de información
-
- Referencia:
 - <https://www.lisainstitute.com/blogs/blog/insiders-amenaza-interna>

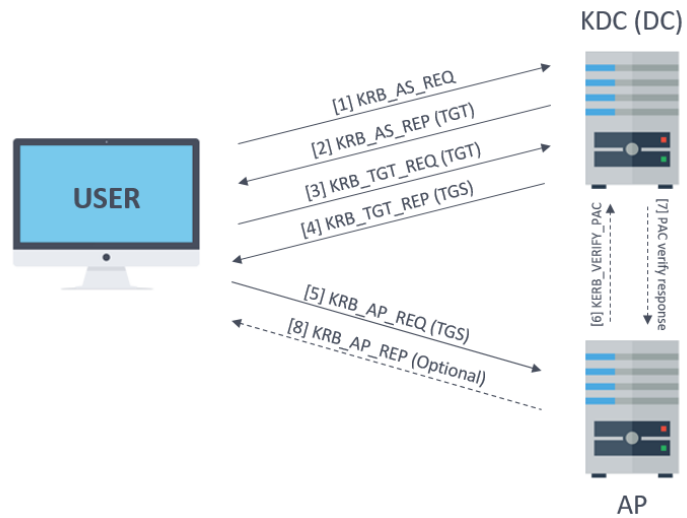
Jailbreak



- Eliminar
 - Limitaciones
 - Apple
 - IOS
-
- Referencia:
 - <https://www.applesfera.com/tag/jailbreak>

Kerberos

- Protocolo
- Verificar dispositivos
- Conexión



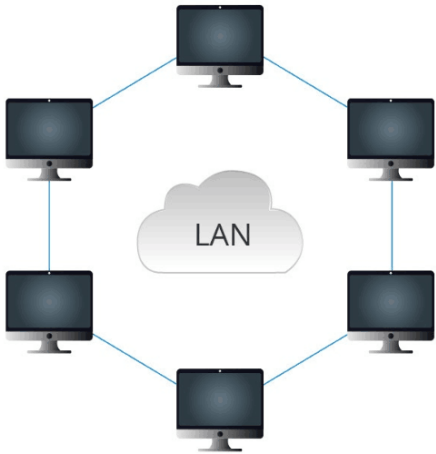
- Referencia:
- <https://www.redeszone.net/tutoriales/redes-cable/kerberos-protocolo-seguridad-redes/>

Keylogger



- Programa malicioso
 - Registrar y almacenar
 - Pulsaciones
 - Robo de información
 - Espiar
-
- Referencia:
 - <https://www.welivesecurity.com/la-es/2021/03/04/que-es-keylogger-herramienta-para-espiar/>

LAN



- Grupo
 - Computadoras y dispositivos
 - Comparten línea de comunicaciones
-
- Referencias:
 - <https://searchdatacenter.techtarget.com/es/definicion/Red-de-area-local-LAN>

Lista negra



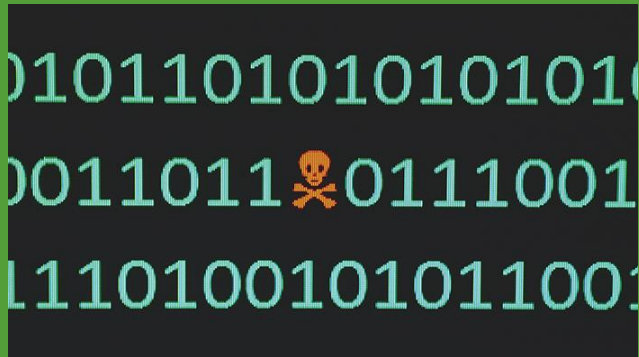
- Entidades
 - Sospechosas/ maliciosas
 - Negación de acceso y derechos
 - Red
 - Sistema
-
- Referencias:
 - <https://protecciondatos-lopdp.com/empresas/lista-blanca-gris-negra/#:~:text=En%20el%20mundo%20de%20la,%2C%20dominios%2C%20procesos%20u%20organizaciones.>

LSSI-CE



- Normativa
- Regulación de actividades económicas
- Productos/Servicios
- Paginas web

Malware



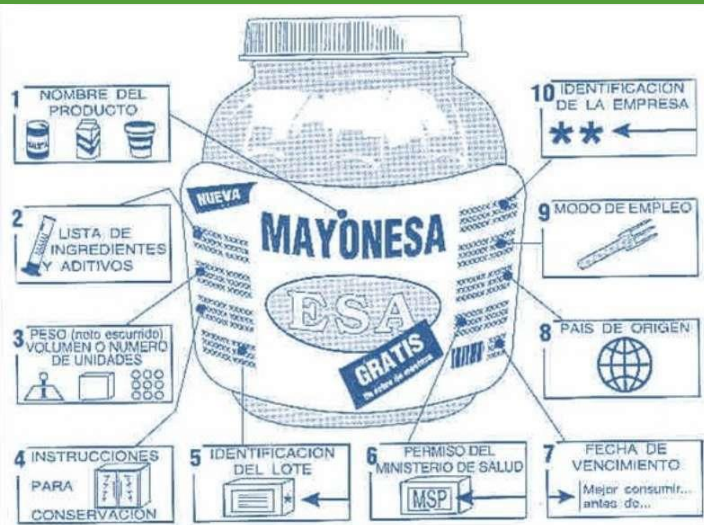
- Programa
 - Código
 - Malicioso
 - Dañino para sistemas
-
- Referencia:
 - <https://es.malwarebytes.com/malware/#:~:text=Malware%20o%20%E2%80%9Csoftware%20malicioso%E2%80%9CD%20es,es%20da%C3%B1ino%20para%20los%20sistemas.&text=La%20intenci%C3%B3n%20del%20malware%20es%20sacarle%20dinero%20al%20usuario%20il%C3%ADcitamente.>

Man-in-the-Middle



- Atacante identifica
 - Comunicación entre usuario y aplicación
 - Suplantación
 - Intercambio de información normal
-
- Referencia:
 - <https://www.imperva.com/learn/application-security/man-in-the-middle-attack-mitm/>

Metadatos



- Suministrar información
- Datos producidos
- Contenido
- Calidad

- Referencias:

- <https://www.geoidep.gob.pe/conoce-las-ides/metadatos/que-son-los-metadatos#:~:text=La%20definici%C3%B3n%20m%C3%A1s%20concreta%20de,otras%20caracter%C3%ADsticas%20de%20los%20datos.>

NGFW



- Sistema de seguridad
 - Redes
 - Hardware
 - Detecta y previene
 - Ataques
 - Nivel aplicación y protocolos de comunicación
-
- Referencia:
 - <https://cerounosoftware.com.mx/2016/07/18/que-es-un-next-generation-firewall-ngfw/>

No repudio



- Probar la participación
- Diversas partes
- Comunicación

Ofuscar



- Dificultad
 - Entendimiento
 - Datos/software
 - Sin afectar su funcionalidad.
-
- Referencia:
 - <https://auditoriadecodigo.com/glosario-vocabulario-ciberseguridad-seguridad/#Ofuscar>

OTP (One-Time Password)



- Contraseña de un solo uso
- Proceso de inicio de sesión
- Referencia:
- <https://www.ionos.mx/digitalguide/servidores/seguridad/que-es-una-one-time-password-otp/>

Pishing



- Ciberdelincuencia
 - Fraude y engaño
 - Manipulación para el robo de información
-
- Referencia
 - <https://www.avast.com/es-es/c-phishing>

PIN



- Contraseña de 4 dígitos
 - Servicios y dispositivos
 - Acceso al sistema
-
- Referencia:
 - https://es.wikipedia.org/wiki/Ataque_de_control_de_pin

Pluggin



- Programa complementario
- Aplicaciones web
- Programas de escritorio
- Amplia miento de funciones

Red privada virtual



- Conexión cifrada
- Dispositivo a red
- Transmisión segura de datos

- Referencia:
- https://www.cisco.com/c/es_mx/products/security/vpn-endpoint-security-clients/what-is-vpn.html

Respuesta de incidentes

- Reacción rápida
- Problema
- Seguridad de información



- Referencia:
- <https://web.mit.edu/rhel-doc/4/RH-DOCS/rhel-sg-es-4/ch-response.html#:~:text=Una%2orespuesta%2oa%2oincidentes%2oes,la%2oviolaci%C3%B3n%2ode%2ola%2oseguridad.>

Router



- Dispositivo que ofrece conexión wi-fi
- Conexión con modem
- Información de internet a dispositivos personales

- Referencia:
- <https://support.google.com/wifi/answer/6274087?hl=es>

Seguridad por oscuridad



- Uso secreto
 - Diseño
 - Implementación
 - Método principal
 - Seguridad
-
- Referencia:
 - elespanol.com/invertia/disruptores-innovadores/innovadores/tecnologicas/20200306/tecnologia-empresarial-seguridad-oscuridad/471954497_o.html

SFTP



- Seguridad
- Movilizar archivos
- Admite el cifrado
- Referencia:
- <https://www.hostinger.mx/tutoriales/como-usar-sftp>

Software



- Componente intangible
- Aplicaciones y programas
- Es parte de los dispositivos

- Referencia:
- <https://concepto.de/software/>

TCP/IP



Transmission Control Protocol/Internet Protocol

- Conjunto de protocolos
- Comunicación entre la red
- Enrutar paquetes de datos

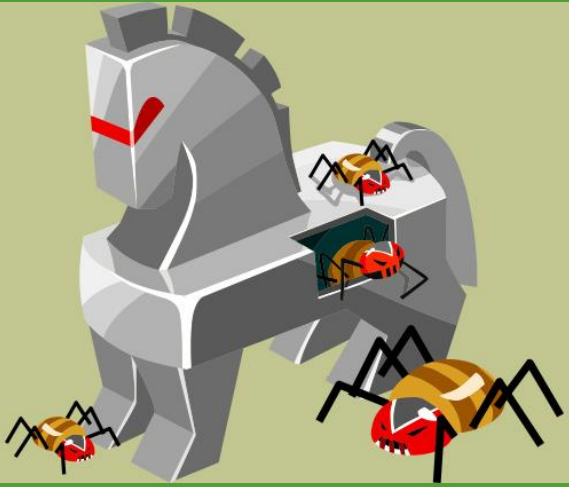
- Referencia:
- https://upanama.edu.com/archivos/repositorio/6000/6126/html/51_proto.htm

Token



- Método de autenticación
- Multifactor
- Fortalecimiento de seguridad
- Referencia:
- <https://www.arame.com.mx/blog/que-es-un-token/>

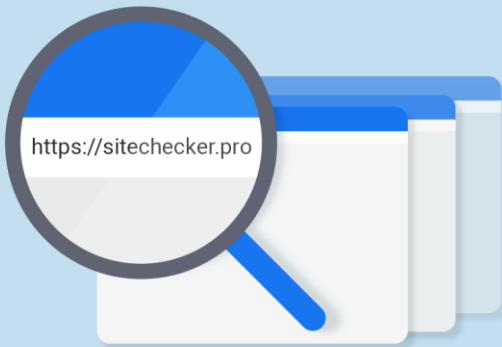
Troyano



- Malware
 - Programas que instala otros
 - Robo de información
 - Daño al sistema.
-
- Referencia:
 - <https://www.hornetsecurity.com/es/knowledge-base/troyanos/#definicion-troyano>

URL

- Dirección
- Localizar dominios



- Referencia:
- [https://support.google.com/google-ads/answer/14095?hl=es-419#:~:text=Es%20la%20ubicaci%C3%B3n%20de%20una,de%20un%20archivo%20en%20Internet.&text=As%C3%AD%20como%20los%20edificios%20y,\(Localizador%20uniforme%20de%20recursos\).](https://support.google.com/google-ads/answer/14095?hl=es-419#:~:text=Es%20la%20ubicaci%C3%B3n%20de%20una,de%20un%20archivo%20en%20Internet.&text=As%C3%AD%20como%20los%20edificios%20y,(Localizador%20uniforme%20de%20recursos).)

UTM



- Gestor
- Centralizado de amenazas

- Referencias:
- <https://www.sophos.com/es-es/products/unified-threat-management.aspx>

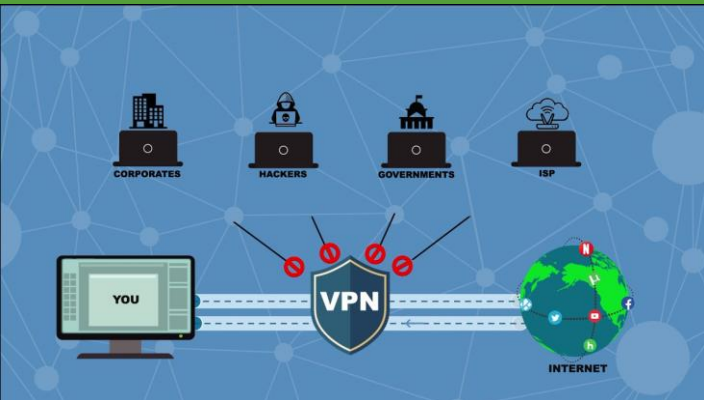
Virus



- Malware
- Programa malicioso
- Robo de datos
- Funcionamiento no correcto del dispositivo

- Referencia:
- osi.es/es/contra-virus#:~:text=El%20malware%2C%20apodado%20com%C3%BAnmente%20como,a%20cabo%20otras%20acciones%20maliciosas.

VPN



- Trafico de internet
 - Seguro
 - Ocultando IP
 - Encriptación de datos
 - Datos privados
 - Protección de ciberataques
-
- Referencias:
 - <https://nordvpn.com/es/download/>

Vulnerabilidad



- Fallo técnico
 - Acceso a usuario no legitimo
 - Robo de información
 - Operaciones no permitidas de forma remota
-
- Referencia:
 - <https://www.ealde.es/ataque-amenaza-vulnerabilidad-ciberseguridad/>

WEP



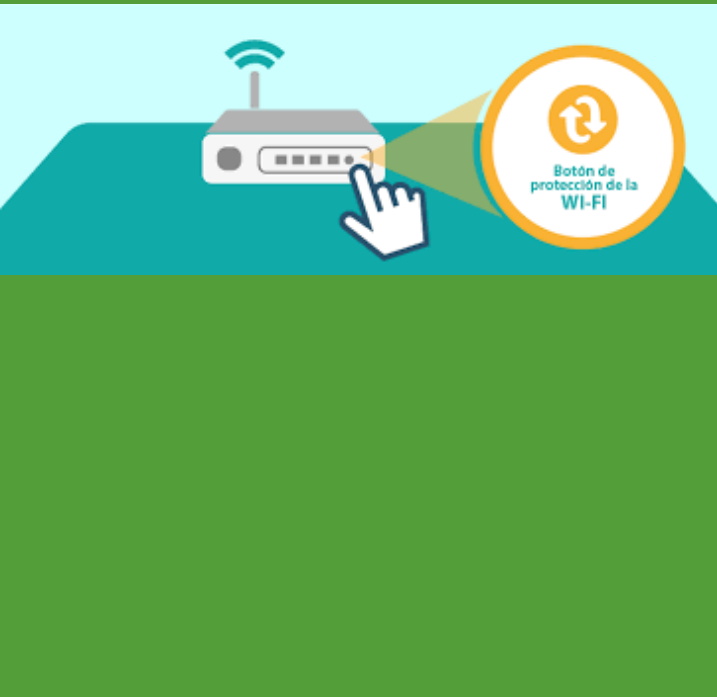
- Protocolo de seguridad
 - En una WLAN
 - Cifra datos dentro de esa red local
-
- Referencia:
 - <https://www.speedcheck.org/es/wiki/wep/>

WPA



- Conexión inalámbrica segura
 - Similitud con WEP
 - Manejo de seguridad y autorización de usuarios
-
- Referencia:
 - <https://techlib.net/definition/wpa.html>

WPS



- Control de conexión wi-fi
- Uso de PIN 8 dígitos
- Referencia:
- <https://www.xataka.com/basics/wps-que-sirve-este-boton-que-trae-algunos-routers>

XSS



- Vulnerabilidad
- Aplicaciones web
- Ejecución de código
- Usuarios

- Referencia:

- <https://www.azsecure.com/blog/los-peligros-de-los-ataques-de-cross-site-scripting-xss/#:~:text=Las%20vulnerabilidades%20de%20tipo%20Cross,frecuentes%20en%20las%20aplicaciones%20web.&text=Los%20ataques%20XSS%20son%20un,a%20un%20sitio%20web%20leg%C3%A1timo.>

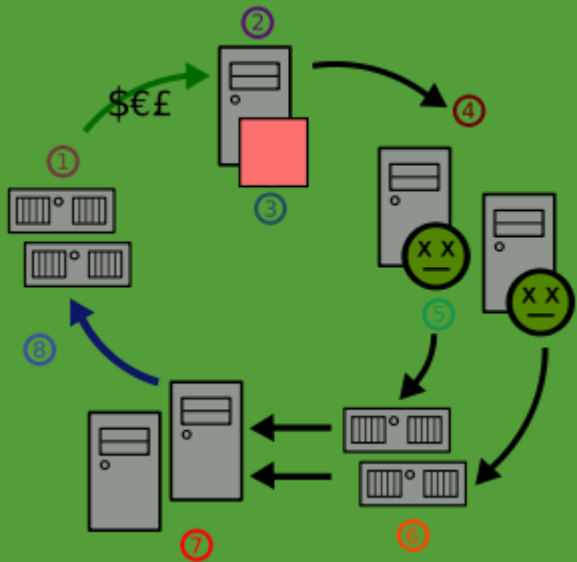
Zero-day

- Vulnerabilidad reciente
- No hay parche de solución
- Aprovechamiento del fallo en la seguridad



- Referencia:
- <https://www.osi.es/es/actualidad/blog/2020/08/28/que-es-una-vulnerabilidad-zero-day>

Zombie



- [illegible]