Glosario

A

ACL: Acrónimo de Access Control List - lista de control de acceso, mecanismo para asignar permisos sobre algún objeto.
Active Directory: Acrónimo de Directorio Activo, servicio que brindan los sistemas operativos de Microsoft en su versión de servidores para brindar una administración centralizada y robusta de los dispositivos que conforman la red.
Activo: Cualquier bien que tenga valor para la organización.
ADSL: Acrónimo de Asymmetric Digital Subscriber Line - Línea de Suscripción Digital Asimétrica, especifica diferente velocidad en la recepción y el envío de datos.
AES: Advanced Encryption Standard - Estándar de cifrado avanzado, algoritmo de cifrado simétrico.
Algoritmo simétrico: Algoritmo que utiliza la misma clave secreta para cifrar y descifrar.
Algoritmo: Método expresado de manera matemática (código de cómputo) para ejecutar una función u operación específica.
Amenaza: Cualquier entidad físico, lógico y natural que provoque un evento, permitiendo desencadenar un incidente en la organización.
Análisis de riesgo: Uso sistemático de la información para identificar fuentes y estimar el riesgo que presentan los activos de una organización.
AP: Acrónimo de Access Point - punto de acceso, dispositivo empleado para brindar acceso inalámbrico en los estándares 802.11a/b/g/n.
Appliance: Cualquier sistema que se vende como listo para ser usado, presentado como una caja negra, en la que el aplicativo está preinstalado. No sirve para ejecutar otras tareas que aquellas para las cuales ha sido su desarrollo.
ARP: Address Resolution Protocol –Protocolo de Resolución de Dirección física.
ARPA: Acrónimo de Advanced Research Proyect Agency - Agencia de Proyectos de Investigación Avanzada del gobierno de los Estados Unidos.
ARPAnet: Red de computadoras creada por un proyecto del gobierno de los Estados Unidos como medio de comunicación para los diferentes organismos del país.
Ataque: Es la explotación por medio de una amenaza a una vulnerabilidad.
Autenticación: Proceso de determinar la identidad de un usuario.

B

Back Door: Conocida como puerta trasera, es empleada para generar una conexión hacia algún equipo de manera no autorizada.
Backbone: Nivel más alto en una red jerárquica.
Bastion host: Host con procedimientos de Hardening aplicados.
BCP: Acrónimo de Business Continuity Plan- Plan de continuidad del negocio, conjunto de tareas que permite a las organizaciones continuar su actividad en situaciones que un evento afecte sus actividades.

Bien: Cualquier cosa que represente un valor para la organización.
BIOS: Basic Input Output System- Sistema de entrada y salida básico, empleado como la base de comunicación en la configuración lógica del hardware.
Blowfish: Algoritmo de cifrado por bloques, simétrico, generado como algoritmo de uso general, opción de sustitución a DES.
BOOTP: Bootstrap Protocol – Protocolo Bootstrap, empleado para asignar IP a estaciones UNIX antes de cargar el sistema operativo.
Bot: Programa informático que realiza funciones muy diversas, tratando de imitar el comportamiento humano.
Botnet: Red de equipos comprometidos, controlados por software de manera centralizada, empleados principalmente para un fin malicioso.
Bridge (puente): Utilizado para unir dos redes a nivel de capa de enlace (capa 3 modelo OSI).
Broadcast: Transmisión de un paquete que será recibido por todos los miembros de un segmento de red.
BRP: Acrónimo de Business Recovery Plan, Plan de recuperación del negocio.
Buffer overflow: Ataque caracterizado por sobrecargar la memoria de un programa o proceso, un buffer es creado para contener una cantidad de datos finitos, en caso de llenar de más el buffer ocasiona fallas en el programa.

C

CA: Acrónimo de Certificate Authority - autoridad certificadora.
CEH: Acrónimo de Certified Ethical Hacker – Certificación Hacker Ético.
CERT: Acrónimo de Computer Emergency Response Team, Equipo de Respuesta a Incidentes de Cómputo.
Checksum: También conocido como resumen hash, es una cadena de tamaño fijo que identifica una cantidad de datos de tamaño variable.
CIA: Acrónimo de Confidenciality, Integrity, Availability - Confidencialidad, Integridad y Disponibilidad, los tres pilares de la seguridad.
Cifrado asimétrico: Emplea dos contraseñas diferentes, una para ocultar la información y otra para recuperarla.
Cifrado simétrico: Emplean una misma contraseña para ocultar y para recuperar la información.
Cliente – Servidor: Arquitectura en donde básicamente un cliente realiza peticiones a un programa (servidor) el cual da respuesta a las peticiones.
COBIT: Acrónimo de Control OBjetives for Information and related Technology – Objetivos de Control para tecnología de la información, modelo que permite implementar un marco de control y gobernabilidad de TI.
Confidencialidad: La propiedad de que la información esté disponible y no sea divulgada, a personas, entidades o procesos no autorizados.
Contraseña: Un secreto conocido por un usuario y por un sistema, utilizado como mecanismo para identificar a un usuario.

Control de Acceso: Es la metodología de seguridad que permite acceso a la información o recurso con base en la identidad.
Control: Políticas, procedimientos, prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido.
CPU: Acrónimo de Central processing unit- Unidad central de procesamiento.
Criptografía: Es la ciencia de cifrar y descifrar información, utilizando técnicas que hagan posible el intercambio de mensajes de manera segura, que sólo pueden ser leídos por las entidades a quien va dirigido.
Cross Site Scripting: Vulnerabilidad que aprovecha la falta de mecanismos de filtrado en los campos de entrada, y permite el ingreso y envío de datos sin validación alguna.
Cuenta de usuario: Registro que contiene información que identifica un usuario, incluyendo su password.
Cybercrimen: Symantec define Cybercrimen como un crimen que es realizado utilizando una computadora, red o hardware.

D

Datagrama: Parte de un paquete de información.
DB: Acrónimo de Data Base –Base de Datos.
DCA: Acrónimo de Defense Communications Agency-Agencia de defensa para las comunicaciones del gobierno de los Estados Unidos.
DDoS: Acrónimo de Distributed Denial of Service – Denegación de servicio distribuido, tipo de ataque lógico.
Denegación de Servicio: concepto utilizado para referirse a la no disponibilidad.
DES: "Data Encription Standard", estándar de cifrado de clave secreta, emplea el algoritmo Lucifer desarrollado por IBM.
DGTIC: Dirección General de Cómputo y Tecnologías de Información y Comunicación
DHCP: Dynamic Host Configuration Protocol –Protocolo de configuración dinámica de host.
Dial-up: Conexión a INTERNET vía telefónica.
Diffie – Hellman: Estándar de intercambio de claves.
DISA: Defense Information Systems Agency- Agencia para la defensa de sistemas de información del gobierno de los Estados Unidos.
Disponibilidad: La propiedad de estar disponible y utilizable cuando lo requiera una entidad autorizada.
DMZ: Acrónimo de Desmilitarized Zone -Zona desmilitarizada, una red local que se ubica entre la red interna de una organización y una red externa.
DNS: Domain Name System- Sistema de nombre de Dominios, conjunto de protocolos y mecanismos que permiten la traducción de las URL en una dirección de Internet (IP- Internet Protocol).
DoS: Por sus siglas Denial of Services – Denegación de servicio, familia de ataques que atenta contra la disponibilidad.

DRP: Inglés Disaster Recovery Plan- Un plan de recuperación ante desastres, proceso de recuperación que cubre datos, hardware y software, para que un negocio pueda comenzar de nuevo sus operaciones.
DSL: Digital Subscriber Line -línea de abonado digital.

E

EAP: Acrónimo de Extensible Authentication Protocol – Protocolo de autenticación extensible, permite utilizar nuevos métodos de autenticación para medios cableados e inalámbricos.
ECC: Acrónimo de Elliptic Curve Cryptography – Criptografía con Curvas Elípticas.
Enumeración: Organizar la información recopilada como lo es nombres de usuario, nombres de equipos, redes, puertos abiertos, sistema operativo utilizado, obtener este tipo de información requiere de una constate interacción entre el sistema y el intruso, razón por la cual puede ser identificado.
Estándar: Orientaciones obligatorias que buscan cumplir las políticas.
Ethernet: Es el estándar de red de área local más ampliamente utilizado, define las características de cableado, señalización de nivel físico y los formatos de trama del nivel del enlace de datos del modelo OSI.
Exploit: Del inglés *to exploit*, explotar o aprovechar es una pieza de software, un fragmento de datos, o una secuencia de comandos que se aprovecha de un error, falla o vulnerabilidad para obtener beneficios, dañar el sistema.

F

Falso negativo: Cuando una acción legítima es considerada un problema.
Falso positivo: Cuando un problema no es identificado y se considera una acción legítima.
Fibra Óptica: medio físico utilizado en las redes de datos, para la transmisión de paquetes.
Fingerprinting: Técnica para identificar datos en la red por medio de información pública del objetivo.
Firewall: Un dispositivo físico o lógico que filtra paquetes entre una red privada y una red pública decide qué información puede ser entregada con base en políticas programadas.
Firma digital: Es un conjunto de datos asociados a un mensaje digital que permitan asegurar la integridad del mensaje y la autenticación del emisor.
Firmware: Programa grabado en una memoria ROM y establece la lógica de más bajo nivel que controla los circuitos.
FLOPS: Acrónimo de Floating Point Operation Per Second –Operaciones de punto flotante por segundo.
FTP: Acrónimo de File Transport Protocol - Protocolo de transferencia de archivos.

G

Gateway: Punto de conexión entre diferentes redes.
GPS: Acrónimo de Global Positioning System – Sistema de posicionamiento Global.
Gusano: Algún programa que toma medidas activas para reproducirse él mismo.

H

Hacker: Profesional de la seguridad en cómputo, según CEH, Certification Ethical Hacker- Certificación de Hacker Ético.
Handshake: Saludo de tres vías, empleado para comenzar una comunicación entre dos equipo dentro de TCP/IP.
Hardening: Es el proceso de asegurar un sistema, acción compuesta por un conjunto de actividades para reforzar al máximo la seguridad de un equipo, que permite disminuir el riesgo de ser vulnerados.
Hash: Se refiere a una función o método para generar claves o llaves que representen de manera casi unívoca a un documento, registro o archivo.
Help Desk: Recurso para información y asistencia, planteado para resolver problemas relacionados con equipos de cómputo y similares.
HIDS: Acrónimo de Host-based Intrusion Detection System- Sistema detector de intrusos basado en host, el IDS basado en host implica utilizar programas instalados en los sistemas que se requiere sean monitoreados.
Hombre en el medio: técnica de ataque lógico para ver toda la comunicación entre 2 equipos.
Host: Nombre empleado en el argot de redes para hacer referencia a un equipo de cómputo.
Hotspot: También conocido como portal cautivo, mecanismo de seguridad para redes inalámbricas el cual brinda control de acceso y privacidad.
HTTP: Hypertext Transfer Protocol – Protocolo de transferencia de hipertexto.

I

El robo de información sobre un objeto por un atacante.
IANA: Acrónimo de Internet Assigned Numbers Authority - Agencia de Asignación de Números de Internet.
ICMP: Acrónimo de Internet Control Messages Protocol, protocolo de la pila TCP/IP encargado de hacer pruebas de conexión.
IDEA: Acrónimo de International Data Encryption Algorithm – Algoritmo Internacional de Cifrado de datos, algoritmo de bloques cifrado simétrico.

IDS: Acrónimo de Intrusion Detection System – Sistema detector de intrusos, conjunto de programas y dispositivos que permiten la detección de actividades inusuales, incorrectas o anómalas en una red o equipo en particular.
IEC: Acrónimo de Electrotechnical Commission –Comisión Electrónica Internacional.
IETF: Acrónimo de Internet Engineering Task Force – Destacamento de Ingeniería en Internet.
IMAP: Internet Message Access Protocol – Protocolo de acceso a mensajes de internet
Incidente de seguridad: Situación que posiblemente compromete algún activo de la institución.
Incidente de seguridad: Un solo o una serie de eventos de seguridad de la información no deseados o inesperados que tienen una significativa probabilidad de comprometer las operaciones comerciales y amenazan la seguridad de la información.
Integridad: Propiedad de salvaguardar la exactitud de los archivos.
Intrusión: Acción de introducirse sin derecho en una jurisdicción, cargo, propiedad, etcétera.
IP Homologada: Denominación que se le da a toda dirección que tiene acceso directo en internet.
IP: Parte de la suite de protocolos TCP/IP que es responsable de la transferencia de paquetes de información en la red.
IPS: Acrónimo de Intrusion Prevention System – Sistema de prevención de intrusos.
IPS: Internet Protocol Suite – conjunto de protocolos de internet, es un nombre con el que también se conoce al conjunto de protocolos TCP/IP.
IPSec: Protocolo de seguridad para datos en tránsito.
Iptables: Es el subsistema de firewalling de Linux 2.4.x/2.5.x. Ofrece la funcionalidad de filtrado de paquetes (ya sea *stateless* o *stateful*), todos los diferentes tipos de NAT (Network Address Translation), la manipulación de paquetes (modificar TOS -Type of Service- y encabezados) y también facilita el trabajo al subsistema de QoS (Quality of Service) de Linux.
ISN: Initial Sequence Number – Número inicial de secuencia empleado para establecer comunicaciones en el protocolo TCP).
ISO: Acrónimo de International Organization for Standardization - Organización Internacional de Estándares.

K

Kerberos: Protocolo de autenticación de redes de ordenador, que permite a dos computadoras en una red insegura demostrar su identidad mutuamente de manera segura.
Keylogger: Deriva del inglés Key (Tecla) y Logger (Registrador), en conjunto, un software o hardware registrador de teclas.

L

L2TP: Layer 2 Tunneling Protocol – Protocolo de túnel capa 2, protocolo VPN como alternativa y mejora de PPTP.
LAN: Acrónimo de Local Area Network- Red de área local, clasificación de la red según su tamaño.

LCC: Acrónimo de Logical Link Control**-** Control de enlace lógico, estándar para la transmisión de datos lógicos.
LM Hash: También conocido como LAN Manager hash, es uno de los formatos que se emplean en el almacenamiento de cuentas de usuario en los sistemas operativos anteriores a Windows Vista, con longitud de 16 caracteres.
Log: Hace referencia a un registro de algo.
LSA: Acrónimo de Level Service Agreement, es un acuerdo de nivel de servicio, contrato escrito entre un proveedor de servicio y su cliente con el objetivo de fijar el nivel de calidad del servicio, en aspectos como tiempo de respuesta, disponibilidad de horario, documentación disponible, personal asignado al servicio.

M

MAC_1: Media Access Control- Control de acceso al medio, en redes.

MAC_2: Message Authentication Code – código de autenticación de mensaje en criptografía.
Malware: Denominación que se le recibe cualquier tipo de software malicioso, el término malware incluye virus, gusanos, troyanos, rootkits.
MAN: Metropolitan Área Network-Redes de Área Metropolitana, clasificación de redes según su tamaño.
MBSA: Acrónimo de Microsoft Baseline Security Analyzer, herramienta para ayudar a determinar el estado de seguridad de un sistema de acuerdo con las recomendaciones de seguridad de Microsoft.
MD5: Abreviatura de Message-Digest Algorithm 5, Algoritmo de Resumen del Mensaje 5, es un algoritmo de reducción criptográfico de 128 bits.
Mecanismo de seguridad: Es un control que se utiliza para implementar un servicio, diseñado para detectar, prevenir o recobrarse de un ataque de seguridad.
MIB: Management Information Base – Base de información gestionada, tipo de base de datos que contiene información de los dispositivos gestionados en una red de comunicación.
MILNET: Military Network – Red militar, fue el nombre que se le dio a parte de la red de ARPANET, diseñada para tráfico clasificado por el departamento de defensa de los Estados Unidos.
Mirror: Del inglés Mirror – Espejo, en redes se refiere a la réplica del tráfico de red de un Puerto en otro.
MIT: Acrónimo de Massachusetts Institute of Technology – Instituto de tecnología de Massachusetts

N

NAS: Acrónimo de Network Attached Storage, brinda un lugar central de almacenamiento de datos, permitiendo acceso a clientes heterogéneos por diversos medios de conexión, estos dispositivos han ganado popularidad en medios virtuales por su rápido acceso a datos, facilidad, administración y configuración simple.

NAT: Acrónimo de Network Address Translation – Traducción de direcciones de red.
NetBios: Network Basic Input/Output System, especificación de interfaz para acceso a servicios de red, es decir, una capa de software desarrollado para enlazar un sistema operativo de red con hardware específico.
NIC: Acrónimo de Network Interface Controller – controlador de interfaz de red, también llamada adaptador de red que permite la comunicación entre diversos dispositivos.
NIDS: Acrónimo de Network IDS – Sistema detector de intrusos de red.
NIST: Acrónimo de National Institute of Standards and Technology- Instituto Nacional de Normas y Tecnología.
No repudio: Servicio de seguridad que permite probar la irrenunciabilidad del envío o recepción de información.
NOC: Acrónimo de Network Operations Center – Centro de operaciones de Red, responsable del monitoreo del estado de la red y de la atención, resolución y análisis de incidentes a problemas que afecten a la disponibilidad y funcionalidad de la infraestructura de red.
NTFS: NT File System, sistema de archivos empleado por algunos sistemas operativos de la familia Microsoft, el cual incorpora principalmente la posibilidad de cifrado, permisos y compresión.

O

OECD: Acrónimo de Organization for Economic Co-operation and Development –Organización para la Cooperación y Desarrollo Económico.
OSI: Acrónimo de Open System Interconnection –Sistema de interconexión abierto, modelo para redes de datos.
Outsoursing: Es el contrato con alguna compañía o persona para realizar una función en particular.

P

Password: Secreto conocido sólo por el sistema y el usuario, utilizado para probar la identidad de un usuario.
PC: Acrónimo de Personal Computer - computadora de propósito general.
PDCA: Acrónimo de Plan-Do-Check-Act, modelo para aplicar a los procesos de Sistemas de Gestión de la Seguridad de la Información, definido en ISO 27001.
PDCA: Ciclo PDCA de mejora continua de la calidad (planear, hace, revisar, actuar).
PF: Packet Filter, sistema de filtrado TCP/IP y traducción de direcciones de red, normalización de paquetes TCP/IP, control de ancho de banda y priorización de paquetes. Parte genérica del sistema operativo OpenBSD a partir de su versión 3.
Pharming: Es la explotación de una vulnerabilidad en el software de los servidores DNS (Domain Name System) o en el de los equipos de los propios usuarios que permite a un atacante redirigir un nombre de dominio (domain name) a otra máquina distinta.

Phishing: Es una modalidad de estafa diseñada con la finalidad de robarle la identidad, el delito consiste en obtener información tal como números de tarjetas de crédito, contraseñas, información de cuentas u otros datos personales por medio de engaños.

Plan de contingencia: Tipo de plan preventivo, predictivo y reactivo. Presenta una estructura y operativa que ayudará a controlar una situación de emergencia y a minimizar sus consecuencias.

Política: Declaración general de los principios que representan la posición de la administración para un área de control definida.

PPTP: Point to Point Tunneling Protocol. Protocolo de túnel punto a punto, método para implementar VPN.

Print Server: Acrónimo de servidor de impresión que conecta una impresora a la red para que cualquier dispositivo pueda utilizarlo.

Protocolo: Es una regla formal o comportamiento, en relaciones internacionales, los protocolos minimizan el problema causado por diferencia cultural por acordar un conjunto común de reglas que son ampliamente conocidas e independientes de cualquier país.

En comunicaciones de datos, conjunto de reglas utilizadas por dispositivos, para comunicarse entre ellos, la naturaleza de los protocolos requieren procesos de estandarización abierta y documentación de los estándares disponible públicamente, los estándares de internet están desarrollados por Internet Engineering Task Force (IETF) dentro de presentaciones abiertas y públicas, los protocolos desarrollados en este proceso son publicados como Request for Comment(RFCs).

R

RADIUS: Remote Authentication Dial-In User Server – Servidor, protocolo centralizado de autenticación, autorización y auditoría para aplicaciones de acceso a la red.

RC5: Algoritmo simétrico de cifrado de bloques, diseñado por Ronald Rivest en 1994.

RFCs: Acrónimo de Request for Comments - petición de comentarios, serie de documentos que describe el conjunto de protocolos de internet.

RFID: Acrónimo de Radio Frequency IDentification – Identificador por radio frecuencias, sistema de almacenamiento y recuperación de datos por radio frecuencia.

Riesgo residual: El riesgo remanente después del tratamiento de los riesgos.

Riesgo: La posibilidad de que una amenaza explote una vulnerabilidad, es la posibilidad de que suceda un evento.

RIPEMD: Acrónimo de RACE Integrity Primitives Evaluation Message Digest – Primitivas de integridad del resumen del mensaje, algoritmo de resumen, también conocido como función hash.

RMON: Remote Monitoring – Monitoreo remoto, protocolo empleado para el monitoreo de la red.

Robo de identidad: Hacerse pasar por otra entidad haciendo creer a un tercero que se es un usuario verdadero.

Rootkit: Colección de herramientas o utilerías que habilitan niveles de acceso de administrador a una computadora.

Router: Conmutador de paquetes que opera a nivel de red del modelo OSI.

RSA: "Rivest, Shamir y Adleman" - Algoritmo de cifrado asimétrico, desarrollado en 1977.

S

S/MIME: Secure / Multipurpose Internet Mail – Correo de propósito múltiple seguro, estándar de cifrado asimétrico y firma de correo.
SANS: Organización dedicada al entrenamiento en seguridad en cómputo.
Screened subnet: Arquitectura de firewall equivalente a una DMZ.
Seguridad convergente: Seguridad que contempla tanto la seguridad física como lógica, para asegurar un host.
Seguridad de información: Preservación de la confidencialidad, integridad y disponibilidad de la información, pueden estar involucradas otras propiedades como la autenticación, responsabilidad, no repudio y confiabilidad.
Seguridad: Consiste en mantener libre de peligro, daño o riesgo un activo.
Servicio de seguridad: Referido a ofrecer confidencialidad, integridad, no repudio, autenticación, control de acceso, disponibilidad.
Servicio no orientado a conexión: Servicio el cual utiliza el protocolo UDP para su transmisión.
Servicio orientado a conexión: Servicio el cual utiliza el protocolo TCP para su transmisión.
SET: Secure Electronic Transaction – Transacción electrónica segura, protocolo elaborado por iniciativa de VISA o Mastercard, protocolo asimétrico similar a PGP.
SGSI: Acrónimo de Sistema de Gestión de la Seguridad de la Información.
SHA1: Algoritmo de resumen criptográfico, genera cadenas de 128 y 256 bits.
Site: Lugar o sitio, en el cual se tiene el conjunto de dispositivos de telecomunicaciones y servidores con condiciones idóneas como clima, presión, monitoreo, control de acceso, corriente regulada, UPS, sistemas de tierra y obra civil, principalmente.
SLA: Service Level Agreement - acuerdo de nivel de servicio, contrato escrito entre un proveedor de servicios y su cliente con el objeto de fijar el nivel acordado para la calidad de dicho servicio.
SMB: Server Message Block, protocolo empleado para compartir acceso a recursos, impresoras, puertos, entre otros.
SMTP: Simple Message Transport Protocol – Protocolo de transporte de mensajes simple.
Sniffer: Programa de captura de las tramas de red, generalmente se usa para gestionar la red con una finalidad administrativa, aunque también puede ser utilizado con fines maliciosos.
SNMP: Simple Network Management Protocol - Protocolo simple de administración de red.
SPAM: Correo no solicitado enviado por internet.
Spoofing: Ataque que se caracteriza por la suplantación de identidad.
SQL injection: Es una técnica de inyección de código que explota una vulnerabilidad que ocurre en la base de datos o en la capa de aplicación.
SQL: Acrónimo de Structure Query Languaje - Lenguaje de consulta estructurado, aplicación para bases de datos.
SSH: Secure Shell -intérprete de órdenes seguro, protocolo seguro de administración remota.

SSL: Secure Socket Layer, protocolo de seguridad que permite cifrar la información en el transporte de la misma, desarrollado por Netscape Communications.
Switch: Es un dispositivo de red, que habilita a los dispositivos de red comunicarse uno con otro eficientemente, dentro de los diversos dispositivos que comunica se encuentran computadoras, puntos de acceso, servidores, print servers, móviles, entre otros.
Syskey: Sistema que añade una capa de seguridad en el almacenamiento de contraseñas en plataformas Microsoft.

T

TCP/ IP: Transmission Control Protocol – Internet Protocol (Protocolo de Control de Transmisión – Protocolo de Internet), es un conjunto de protocolos que forman la base de Internet.
TELNET: The Network Terminal Protocol – Protocolo de terminal para la red.
Texto en claro: Nombre empleado para definir a los datos que viajan sin cifrado.
TI: Acrónimo de Tecnologías de la información.
TKIP: Acrónimo de Temporal Key Integrity Protocol – Protocolo de integridad de clave temporal
TLS: Acrónimo Transport Layer Security – Seguridad en la capa de transporte, protocolo de seguridad de los datos en tránsito.
Trap: Para el protocolo SNMP, se refiere a un reporte de ciertas condiciones y cambios de estado a un proceso de administración.
TRIPLE DES: Algoritmo de cifrado simétrico con claves de 112 o 168 bits.

U

UDP: Acrónimo de User Datagram Protocol, es un protocolo del nivel de transporte basado en el intercambio de datagramas.
UPS: Acrónimo de Uninterruptible Power Supply–Entrega de alimentación ininterrumpida
USB: Acrónimo de Universal Serial Bus – bus serial universal, especificación para establecer comunicación entre dispositivos y un host.
UTP: Acrónimo de Unshielded Twisted Pair – Cable de par trenzado

V

Virus: Malware que tiene por objeto alterar el normal funcionamiento de la computadora
VoIP: Acrónimo de Voz sobre IP, es una de las familias de protocolos de comunicación enfocada a tecnología de transmisión de voz.
VPN: Acrónimo de Virtual Network Private - Red Privada Virtual.
Vulnerabilidad: Hace referencia a un punto débil dentro de un sistema

W

WAN: Wide Area Network- Redes de Área Amplia, clasificación de la red según su tamaño.
Wardriving: Búsqueda de redes inalámbricas desde un vehículo en movimiento.
WEP: Wireless Equivalent Privacity –Privacidad equivalente al cableado, protocolo de seguridad en redes inalámbricas.
WiFi: Wireless Fidelity – Fidelidad Inalámbrica, tecnología de comunicaciones inalámbricas.
Wireless hacking: Hackeo de redes inalámbricas.
Wireless: Tecnología de transmisión inalámbrica por medio de ondas magnéticas a diferentes frecuencias dependiendo el estándar.
WLAN: Wireless Local Area Network – Red Inalámbrica de Area Local.
WMAN: Wireless Metropolitan Area Network –Red Inalámbrica de Área Metropolitana.
WPA: Wi-Fi Protect Access – Acceso protegido Wi-Fi, protocolo de seguridad para redes inalámbricas, creado para corregir las deficiencias de WEP.
WPA2: Wi-Fi Protected Access 2 - Acceso Protegido Wi-Fi 2, sucesor de WPA, utilizando para garantizar confidencialidad AES.