GLOSARIO DE CIBERSEGURIDAD N°1

JULIO 2022

Grupo de investigación de Ciberespacio

Ciberseguridad y ciberguerras

Sein, Candelaria[1]

Cita sugerida: Sein, C. (2022). Glosario de Ciberseguridad N°1. Julio 2022. *Centro de Estudios Estratégicos de Relaciones Internacionales,* p. 1-16.

Resumen: El presente glosario ha sido creado con el objetivo de servir de herramienta a la hora de encarar el amplio y complejo mundo de la ciberseguridad y el ciberespacio. La mayoría de los términos abordados tienen un nacimiento relativamente reciente, lo que nos da cuenta del constante crecimiento que se está desarrollando en el área, así como de la complejidad, y a la vez, la necesidad de comenzar a definir y acordar ideas comunes. En razón de lo anterior, el documento se irá actualizando con nuevos conceptos y acepciones. En esta primera versión, encontramos que la mayoría de la producción de definiciones proviene de organismos estadounidenses, con poca presencia del Sur Global.

Palabras clave: Ciberespacio; ciberseguridad; ciberataque; ciberterrorismo.

[1] Sein, Candelaria. Estudiante de la Licenciatura en Relaciones Internacionales, Universidad Nacional del Centro de la Provincia de Buenos Aires (UNICEN). candesein@gmail.com

***Air gap* (en español: brecha de aire).**

i. Una interfaz entre dos sistemas en la que (a) no están conectados físicamente y (b) ninguna conexión lógica está automatizada (es decir, los datos se transfieren a través de la interfaz solo de forma manual, bajo control humano) (IETF RFC 4949 Ver 2, 2007, p. 16).

ii. Término usado para describir que dos redes están absolutamente separadas (CCN, 2015, p. 47).

APT (*advanced persistent threat*; en español: amenaza persistente avanzada).

i. Un adversario que posee sofisticados niveles de experiencia e importantes recursos que le permiten crear oportunidades para lograr sus objetivos utilizando múltiples líneas de ataque (cibernéticas, físicas y engaños). Estos objetivos incluyen establecer y extender los puntos de apoyo dentro de la infraestructura IT (*Information Technology,* en español: tecnología de la información) de las organizaciones atacadas con el propósito de extraer información y/o perjudicar o dificultar aspectos críticos de un programa, misión u organización; o posicionarse para llevar a cabo estos objetivos en el futuro. Las APT (amenazas persistentes avanzadas) persiguen sus objetivos repetidamente durante un periodo prolongado de tiempo, adaptándose a los esfuerzos del defensor para resistirla y manteniendo el nivel de interacción necesaria para ejecutar sus objetivos (NIST SP 800-30, 2012, p.B-1).

ii. Un ataque selectivo de ciberespionaje o cibersabotaje llevado a cabo bajo el auspicio o la dirección de un país, por razones que van más allá de las meramente financieras/delictivas o de protesta política [...]. La motivación del adversario, y no tanto el nivel de sofisticación o el impacto, es el principal diferenciador de un ataque APT (amenaza persistente avanzada) de otro llevado a cabo por ciberdelincuentes o hacktivistas[2] (McAfee en CCN, 2015, p. 67).

iii. Consiste en un tipo de ataque informático que se caracteriza por realizarse con sigilo, permaneciendo activo y oculto durante mucho tiempo, utilizando diferentes formas de ataque. Suelen estar patrocinados por compañías, mafias o un Estado. El objetivo principal es vigilar, filtrar datos o modificar los recursos de una empresa u organización de forma integrada y continuada en el tiempo. Generalmente, este tipo de *malware* hace

[2] Hacktivista: un *hacker* que usa sus conocimientos informáticos para llevar a cabo acciones en el ciberespacio con una finalidad y una motivación políticas o ideológicas (LISA Institute, 2021).

uso de *exploits* aprovechando vulnerabilidades de tipo *Zero Day* presentes en el software de la víctima (INCIBE, 2021, p. 14).

Ataque de *replay* o de *playback* (en español: ataque de reproduccion o de reinyección).

i. Un ataque en el que el atacante puede reproducir mensajes capturados previamente (entre un Reclamante legítimo y un Verificador[3]) para hacerse pasar por ese Reclamante ante el Verificador o viceversa (NIST SP 800-53 Rev.5, 2020, p. 412).

ii. Ataque consistente en capturar una transmisión de datos correcta y reproducirla posteriormente. Es un ataque típico para capturar secuencias de autenticación correctas y reproducirlas luego para que el atacante logre los mismos derechos de acceso (CCN, 2015, p. 107).

Bomba lógica.

i. Clase de virus que carece de la capacidad de replicación y que consiste en una cadena de código que se ejecuta cuando una determinada condición se produce, por ejemplo, tras encender el ordenador una serie de veces, o pasados una serie de días desde el momento en que la bomba lógica se instaló en nuestro ordenador (CCN, 2015, p. 152).

ii. Un fragmento de código insertado intencionalmente en un sistema de software que activará una función maliciosa cuando se cumplan las condiciones especificadas (CNSSI-4009, 2015, p. 77).

***Botnet*.**

i. Un acrónimo de "robot" y "red". Se refiere a redes de, a veces, millones de máquinas infectadas que están controladas de forma remota por actores malintencionados. Una sola computadora infectada puede denominarse computadora “zombi”. Los dueños de la computadora controlada remotamente a menudo no son conscientes de la infección. Los propietarios de una red de bots pueden utilizar la potencia de procesamiento de la red y el ancho de banda combinados para enviar spam, instalar *malware* y montar ataques DDoS o pueden alquilar la red de bots a otros actores malintencionados (Berkman Klein Center, 2012).

ii. Un conjunto de ordenadores (denominados bots) controlados remotamente por un atacante que pueden ser utilizados en conjunto para realizar actividades maliciosas como

[3] La parte que debe autenticarse se llama reclamante (*claimant*) y la parte que verifica esa identidad se llama verificador (*verifier*). Cuando un reclamante demuestra con éxito la posesión y el control de uno o más autenticadores a un verificador a través de un protocolo de autenticación, el verificador puede verificar que el reclamante es un suscriptor válido (NIST SP 800-63-3, 2017, p.9).

envío de spam, ataques de DDoS, etc. Las botnets se caracterizan por tener un servidor central (C&C, de sus siglas en inglés *Command & Control*) al que se conectan los bots para enviar información y recibir comandos. Existen también los llamados botnets P2P que se caracterizan por carecer de un servidor C&C único (INCIBE, 2021, p. 23).

iii. Red de equipos infectados por un atacante remoto. Los equipos quedan a su merced cuando desee lanzar un ataque masivo, tal como envío de spam o denegación (distribuida) de servicio (CCN, 2015, p. 154).

Ciberataque.

i. Aquella operación cibernética, ya sea ofensiva o defensiva, de la que cabe esperar razonablemente que cause lesiones o la muerte de personas o el daño o la destrucción de bienes (Schmitt, 2017, p. 415).

ii. Forma de ciberguerra o ciberterrorismo donde, combinado con ataque físico o no, se intenta impedir el empleo de los sistemas de información del adversario o el acceso a el mismo (Real Academia de Ingeniería, s.f., definición 1).

iii. Ataques llevados a cabo en el ciberespacio que crean efectos de negación notables (por ejemplo, degradación, interrupción o destrucción) en el ciberespacio o manipulación que conduce a efectos de negación en los dominios físicos. A diferencia de las acciones de explotación del ciberespacio, que a menudo pretenden permanecer clandestinas para ser efectivas, los ciberataques serán evidentes para los operadores o usuarios del sistema, ya sea de forma inmediata o eventualmente, ya que eliminan algunas funciones del usuario (DoD JP 3-12, 2018, p.GL-3).

iv. Uso del ciberespacio para atacar a los sistemas y servicios presentes en el mismo o alcanzables a través suyo. El atacante busca acceder sin autorización a información, o alterar o impedir el funcionamiento de los servicios (CCN, 2015, p. 204).

v. Acción producida en el ciberespacio que compromete la disponibilidad, integridad y confidencialidad de la información mediante el acceso no autorizado, la modificación, degradación o destrucción de los sistemas de información y telecomunicaciones o las infraestructuras que los soportan (CCN, 2015, p. 203).

Ciberdefensa.

i. Concepto que engloba todas las actividades ofensivas y defensivas en las que se utilizan como medio aquellos relacionados con las infraestructuras TIC (Tecnologías de la Información y la Comunicación); por ejemplo: redes de ordenadores, ordenadores,

programas informáticos; y cuyo "campo de batalla" es el ciberespacio. Las actividades de desarrollo de la ciberdefensa van encaminadas hacia la capacitación de los gobiernos y naciones en la denominada "Ciberguerra" (ISDEFE-6:2009 en CCN, 2015, p. 205).

ii. Acciones tomadas dentro del ciberespacio para derrotar amenazas específicas que han infringido o amenazan con infringir las medidas de seguridad del ciberespacio e incluyen acciones para detectar, caracterizar, contrarrestar y mitigar amenazas, incluidos los *malwares* o las actividades no autorizadas de los usuarios, y restaurar el sistema a un configuración segura (DoD JP 3-12, 2018, p. GL-3).

Ciberdelito o delito informático.

i. Actividad delictiva que emplea el ciberespacio como objetivo, herramienta o medio. Ejemplos: fraude, suplantación de personalidad, robo, crimen organizado, etc. (CCN, 2015, p. 206).

ii. Toda aquella acción ilegal que se da por las vías informáticas o que tiene como objetivo destruir y dañar ordenadores, medios electrónicos y redes de internet (Centeno, 2015, p.2).

Ciberespacio.

i. Entorno formado por componentes tangibles e intangibles para almacenar, modificar e intercambiar información usando redes de ordenadores (Schmitt, 2017, p.564).

ii. Ámbito virtual creado por medios informáticos (RAE, 2021).

iii. La red interdependiente de infraestructuras de tecnología de la información (incluyendo Internet), redes de telecomunicaciones, sistemas informáticos, y procesadores y controladores integrados en industrias críticas (NSPD-54/HSPD-23, 2008, p. 3).

iv. Es el ambiente complejo que resulta de la interacción de personas, software, y servicios en internet por medio de dispositivos y redes conectadas. No posee existencia física sino que es un dominio virtual que engloba todos los sistemas TIC (Tecnologías de la Información y la Comunicación) (CCN, 2015, p. 208).

Ciberguerra.

i. Lucha armada —en este caso las armas son las TIC (Tecnologías de la Información y la Comunicación)— entre dos o más naciones o entre bandos de una misma nación, en la que se utiliza el ciberespacio como campo de batalla. (ISDEFE-6:2009 en CCN, 2015, p. 204).

ii. Acciones de un Estado-nación para penetrar las computadoras o redes de otra nación con el fin de causar daño o interrupción (Clarke, 2014, p. 10).

iii. La ciberguerra puede ser entendida como una agresión promovida por un Estado y dirigida a dañar gravemente las capacidades de otro para imponerle la aceptación de un objetivo propio o, simplemente, para sustraer información, cortar o destruir sus sistemas de comunicación, alterar sus bases de datos, es decir, lo que habitualmente hemos entendido como guerra, pero con la diferencia de que el medio empleado no sería la violencia física sino un ataque informático que va desde 'la infiltración en los sistemas informáticos enemigos para obtener información hasta el control de proyectiles mediante computadoras, pasando por la planificación de las operaciones, la gestión del abastecimiento', etc (Colle, 2000)" (Sanchez Medero, 2012, p. 125).

Ciberinteligencia. Actividades de inteligencia en soporte de la ciberseguridad. Se trazan ciberamenazas, se analizan las intenciones y oportunidades de los ciberadversarios con el fin de identificar, localizar y atribuir fuentes de ciberataques (CNN, 2015, p. 212).

Ciberseguridad.

i. Conjunto de acciones que persigue la protección de la información de las organizaciones y en general de toda la comunidad que está en el ciberespacio (Cornejo Montoya, Verdezoto & Villacís, 2019, p. 439).

ii. Prevención de daños, protección y restauración de computadoras, sistemas de comunicaciones electrónicas, servicios de comunicaciones electrónicas, comunicaciones por cable y comunicaciones electrónicas, incluida la información contenida en ellos, para garantizar su disponibilidad, integridad, autenticación, confidencialidad y no repudio[4] (NSPD-54/HSPD-23, 2008, p. 3).

iii. Situación deseada en la que la protección del ciberespacio es proporcional a las ciberamenazas y las posibles consecuencias de los ciberataques. La Ciberseguridad de Defensa (*Defense Cyber Security*) se compone de tres pilares: Ciberdefensa, Ciberinteligencia y Ciber-contraofensiva (NATO - Cyber Security Strategy for Defence,- ACST–Strategy-CyberSecurity-001, 2014 en CCN, 2015, p. 214).

[4] Con la expresión "no repudio" se hace referencia a la capacidad de afirmar la autoría de un mensaje o información, evitando que el autor niegue la existencia de su recepción o creación (Glosario Inteco en CCN, 2015, p.621).

Ciberterrorismo.

i. Es la convergencia entre terrorismo y ciberespacio […]. Para calificar como ciberterrorismo, un ataque debe ocasionar violencia contra personas o contra la propiedad, o al menos causar el daño suficiente como para generar miedo. Ataques que deriven en muertes o personas heridas, explosiones, choques de aviones, contaminación de agua o severas pérdidas económicas pueden servir de ejemplo (Denning, 2000, p. 2).

ii. El uso de las nuevas tecnologías con fines terroristas (Chicarro Lázaro, 2013, p. 6).

iii. Es el ataque premeditado y políticamente motivado contra información, sistemas computacionales, programas de computadoras y datos que puedan resultar en violencia contra objetivos no combatientes por parte de grupos subnacionales o agentes clandestinos (Pollitt, 1998, p. 9).

iv. Un acto delictivo perpetrado mediante el uso de computadoras y capacidades de telecomunicaciones, que resulta en violencia, destrucción y/o interrupción de los servicios para crear miedo al causar confusión e incertidumbre dentro de una población determinada, con el objetivo de influir en un gobierno o población para que se ajuste a un agenda política, social o ideológica particular (FBI en Berkman Klein Center, 2012).

DDoS (*Distributed Denial of Service*; en español: denegación de servicio distribuido).

i. El adversario usa múltiples sistemas de información comprometidos para atacar un solo objetivo, lo que provoca la denegación de servicio para los usuarios de los sistemas de información objetivo (NIST SP 800-30, 2012, p.E-4).

ii. Ataque de denegación de servicio que se realiza utilizando múltiples puntos de ataque simultáneamente (CCN, 2015, p. 363).

iii. Los ataques de denegación de servicio distribuido (DDoS) son ataques de denegación de servicio (DoS) ejecutados por muchas computadoras al mismo tiempo. Actualmente hay varias formas en las que se pueden realizar los ataques DoS y DDoS. Incluyen, por ejemplo, enviar consultas con formato incorrecto a un sistema informático; exceder el límite de capacidad para los usuarios; y enviar a servidores de correo electrónico más correos de los que el sistema puede recibir y manejar (Convención de cibercrimen de Budapest en CCN, 2015, p.361).

DoS (*Denial of Service*, en español: denegación de servicio).

i. Rechazo de un acceso autorizado a los recursos del sistema o demora en las operaciones críticas en el tiempo (ISO-7498-2 en CNN, 2015, p. 360).

ii. Es un ataque a una red o sistema de computadoras que causa que un servicio o recurso sea inaccesible a los usuarios legítimos, que se generan mediante la saturación de los puertos con múltiples flujos de información, haciendo que el servidor se sobrecargue (Lazar & Costescu, 2019, p. 160).

iii. El adversario intenta hacer que un recurso accesible por Internet no esté disponible para los usuarios previstos, o evitar que el recurso funcione de manera eficiente o en absoluto, de forma temporal o indefinida (NIST SP 800-30, 2012, p.E-4).

iv. Los ataques de denegación de servicio (DoS) son intentos de hacer que un sistema informático no esté disponible para los usuarios a través de una variedad de medios. Estos pueden incluir saturar las computadoras o redes de destino con solicitudes de comunicación externa, lo que dificulta el servicio a los usuarios legítimos (Convención de cibercrimen de Budapest en CNN, 2015, p. 361).

Exploit. Un tipo de software, un fragmento de datos, o una secuencia de comandos que aprovecha un fallo o una vulnerabilidad en el sistema de un usuario para provocar un comportamiento no deseado o imprevisto. Las acciones que se suelen realizar son la toma de control de un sistema, una escalada de privilegios o un ataque de denegación de servicio (Glosario Inteco en CCN, 2015, p. 437).

Inyección de SQL (*Structured Query Language*; en español lenguaje de consulta estructurada).

i. Es un método de infiltración de código intruso que se aprovecha de una vulnerabilidad en la validación de los contenidos introducidos en un formulario web y puede permitir la obtención ilegítima de los datos almacenados en la base de datos del sitio web (Glosario Inteco en CCN, 2015, p. 560)

ii. Los ataques de inyección de SQL (lenguaje de consulta estructurado) incorporan código malicioso en aplicaciones vulnerables, lo que genera resultados de consultas en la base de datos de *backend* y ejecuta comandos o acciones similares que el usuario no solicitó (IBM, 2022a).

***Flooding* (en español: inundación).** Un ataque que intenta causar una falla en un sistema al proporcionar más información de la que el sistema puede procesar correctamente (IETF RFC 4949 Ver 2, 2007, p. 131).

***Hacking*.** Intento no autorizado, con éxito o sin él, de acceder a un sistema de información, usualmente con malas intenciones (CCN, 2015, p. 502).

Hacktivismo.

i. Activismo digital antisocial. Sus practicantes buscan el control de ordenadores o sitios web para promover su causa, defender su posicionamiento político, o interrumpir servicios, impidiendo o dificultando el uso legítimo de los mismos (CCN, 2015, p. 502).

ii. El uso no violento de herramientas digitales ilegales o legalmente ambiguas con fines políticos. Estas herramientas incluyen *defacing* (desfiguración) de sitios web, redireccionamientos, ataques de denegación de servicio, robo de información, protestas virtuales, sabotaje virtual y desarrollo de software (Samuel A. en Berkman Klein Center, 2012).

***Jamming* (en español: interferencia intencionada).**

i. Interferencia producida deliberadamente por emisiones destinadas a hacer ininteligibles o falsear en todo o en parte una señal deseada (Real Academia de Ingeniería, s.f., definición 1).

ii. Interferencia de radio que dificulta o impide la recepción de señales radiadas (CCN, 2015, p.566).

***Malware* (en español: programa maligno).**

i. Software o *firmware*[5] (en español: soporte lógico inalterable) destinado a realizar un proceso no autorizado que tendrá un impacto adverso en la confidencialidad, integridad o disponibilidad de un sistema. Un virus, gusano, troyano u otra entidad basada en código que infecta un anfitrión. El *spyware* y algunas formas de *adware* (en español: software publicitario) también son ejemplos de código malicioso (NIST SP 800-53, Rev. 5, 2020, p. 406).

ii. Software o *firmware* desarrollado para infiltrarse en una computadora o dañarla sin conocimiento ni consentimiento del propietario, con la intención de comprometer la confidencialidad, integridad o disponibilidad de los datos, las aplicaciones o el sistema

[5] Un software que maneja físicamente al hardware.

operativo del propietario. Por lo general, esta clase de software se infiltra en una red durante diversas actividades aprobadas por el negocio, lo que permite explotar las vulnerabilidades del sistema (CCN, 2015, p. 254).

iii. Software malintencionado que puede inutilizar los sistemas infectados. La mayoría de las variantes de *malware* destruyen datos al eliminar o limpiar archivos críticos para la capacidad de ejecución del sistema operativo (IBM, 2022a).

***Pharming*.**

i. Ataque informático que aprovecha la vulnerabilidad del software de los servidores DNS (*Domain Name System*: en español: Sistema de Nombres de Dominio) y que consiste en modificar o sustituir el archivo del servidor de nombres de dominio cambiando la dirección IP legítima de manera que al momento en que el usuario escriba el nombre del dominio, sea redirigido a una web falsa que suplantar la identidad legítima obteniendo las claves de acceso (INCIBE, 2021, p. 61).

ii. Un ataque en el que un atacante corrompe un servicio de infraestructura, como DNS (*Domain Name System*: en español: Sistema de Nombres de Dominio), lo que hace que el suscriptor sea redirigido a un verificador falsificado, lo que podría hacer que el suscriptor revele información confidencial, descargue software dañino o contribuir a un acto fraudulento (NIST SP 800-63-3, 2017, p. 50).

***Phishing* (en español: suplantación de identidad).**

i. Método o técnica de ataque que busca obtener información personal o confidencial de los usuarios por medio del engaño y suplantando su identidad digital (CCN, 2015, p. 662).

ii. Es un intento de estafa para robar las credenciales de los usuarios o datos confidenciales como números de tarjetas de crédito. Los estafadores envían correos electrónicos a los usuarios o mensajes de servicio de mensajes cortos (SMS), comúnmente conocidos como mensajes de texto, diseñados para que parezca que provienen de una fuente legítima, por medio de hipervínculos falsos (IBM, 2022b).

iii. Una técnica para intentar adquirir datos confidenciales, como números de cuentas bancarias, a través de una solicitud fraudulenta por correo electrónico o en un sitio web, en la que el perpetrador se hace pasar por una empresa legítima o una persona de confianza (IETF RFC 4949 Ver 2, 2007, p. 222).

iv. Un ataque en el que se atrae al suscriptor (generalmente a través de un correo electrónico) para que interactúe con un verificador/RP falso (parte de confianza) y se le engaña para

que revele información que puede usarse para hacerse pasar por ese suscriptor ante el verificador/RP real (NIST SP 800-63-3, 2017, p. 51).

***Ransomware* (en español: *malware* de rescate).**

i. Es un malware sofisticado que se aprovecha de las debilidades del sistema y utiliza un cifrado sólido para mantener los datos o la funcionalidad del sistema como rehenes. Los ciberdelincuentes utilizan *ransomware* para exigir un pago a cambio de liberar el sistema. Un desarrollo reciente de *ransomware* es el complemento de tácticas de extorsión (IBM, 2022a).

ii. Es un código malicioso que se emplea para secuestrar datos o información y el atacante encripta los datos de la víctima y exige un pago por la clave de descifrado (CCN, 2015, p. 727).

Rootkit.

i. Un conjunto de herramientas utilizadas por un atacante después de obtener acceso de raíz a un anfitrión para ocultar las actividades del atacante en el anfitrión y permitir que el atacante mantenga el acceso a través de medios encubiertos (CNSSI-4009, 2015, p.105).

ii. Es una herramienta que sirve para ocultar actividades ilegítimas en un sistema. Una vez que ha sido instalado, permite al atacante actuar con el nivel de privilegios del administrador del equipo. Está disponible para una amplia gama de sistemas operativos (CCN, 2015, p.771).

***Spyware* (en español: software espía).**

i. Cualquier forma de tecnología que se usa para recoger información sobre una persona o empresa, o información referente a equipos o redes, sin su conocimiento o consentimiento. También puede venir implementado en su hardware. Puede capturar datos de navegación, mensajes de correo, contraseñas y datos bancarios para transmitirlos a otro destino en Internet. Al igual que los virus puede ser instalado al abrir un adjunto de correo infectado, pulsando en una ventana de publicidad o camuflado junto a otros programas que instalemos (Glosario Inteco en CCN, 2015, p.859).

ii. Software que se instala de forma secreta o oculta en un sistema de información para recopilar información sobre personas u organizaciones sin su conocimiento; es un tipo de código malicioso (NIST SP 800-53 Rev.5, 2020, p.419).

SCADA (*Supervisory control and data acquisition,* en español: Supervisión, Control y Adquisición de Datos).

i. Un nombre genérico para un sistema computarizado que es capaz de recopilar y procesar datos y aplicar controles operativos a largas distancias. Los usos típicos incluyen transmisión y distribución de energía y sistemas de tuberías. SCADA fue diseñado para los desafíos únicos de comunicación (por ejemplo, demoras, integridad de datos) que plantean los diversos medios que deben usarse, como líneas telefónicas, microondas y satélite (NIST SP 800-82 Rev 2, 2015, p.B-16).

ii. Sistemas y redes (generalmente industriales) que se comunican con los sistemas de control para proporcionar datos a los operadores con el fin de supervisar, controlar y gestionar procesos (CCN, 2015, p. 782).

***SYN flood* (en español: inundación SYN o ataque de medio abierto).** Ataque de denegación de servicio por el que se inunda un sistema de peticiones de conexión TCP syn (*synchronize* o sincronización) a un anfitrión con la intención de interrumpir su operación (CCN, 2015, p. 871).

***Trojan horse* (en español: troyano).**

i. Programa que no se replica ni hace copias de sí mismo. Su apariencia es la de un programa útil o inocente, pero en realidad tiene propósitos dañinos, como permitir intrusiones, borrar datos, etc. (CCN-STIC-430:2006 en CCN, 2015, p. 158).

ii. Un programa de computadora que parece tener una función útil, pero también tiene una función oculta y potencialmente maliciosa que evade los mecanismos de seguridad, a veces explotando las autorizaciones legítimas de una entidad del sistema que invoca el programa (CNSSI-4009, 2015, p. 126).

Tunelización de DNS (*Domain Name System*, en español: Sistema de Nombres de Dominio). Los ciberdelincuentes utilizan el túnel de DNS, un protocolo transaccional, para intercambiar datos de aplicaciones, como extraer datos de forma silenciosa o establecer un canal de comunicación con un servidor desconocido, como un intercambio de comando y control (C&C) (IBM, 2022a).

Virus.

i. Segmento de código que puede copiarse, tras la satisfacción de alguna condición lógica o temporal, para infectar otros programas, a los que ataca modificándolos, destruyéndolos, etc. (Ribagorda,1997 en CCN, 2015, p. 917)

ii. Un programa de computadora que puede copiarse a sí mismo e infectar una computadora sin permiso o conocimiento del usuario. Un virus puede corromper o eliminar datos en una computadora, usar programas de correo electrónico para propagarse a otras computadoras o incluso borrar todo en un disco duro (CNSSI-4009, 2015, p.131).

Vulnerabilidad.

i. Debilidad o falta de control que permitiría o facilitaría que una amenaza actuase contra un objetivo o recurso del sistema (CCN, 2015, p.920)

ii. Debilidad en un sistema de información, procedimientos de seguridad del sistema, controles internos o implementación que podría ser aprovechada por una amenaza (CNSSI-4009, 2015, p. 131).

iii. Existencia de una falla (o "*bug*") en el software que puede permitir que un tercero o un programa obtenga acceso no autorizado a la falla y la explote (U.S. Air Force Software Protection Initiative en Berkman Klein Center, 2012).

XSS (*cross-site scripting*, en español: ataque de secuencias de comandos entre sitios).

i. Los ataques XSS insertan código malicioso en un sitio web legítimo o en un script de aplicación para obtener información del usuario, a menudo utilizando recursos web de terceros (IBM, 2022a).

ii. En un ataque por XSS, una aplicación web se envía con un *script* (en español: secuencia de comandos o guión) que se activa cuando lo lee el navegador de un usuario o una aplicación vulnerable. Dado que los sitios dinámicos dependen de la interacción del usuario, es posible ingresar un *script* malicioso en la página, ocultándolo entre solicitudes legítimas. Los puntos de entrada comunes incluyen buscadores, foros, *blogs* y todo tipo de formularios en línea en general. Una vez iniciado el XSS, el atacante puede cambiar configuraciones de usuarios, secuestrar cuentas, envenenar *cookies*, exponer conexiones SSL (*Secure Sockets Layer*; en español: capa de *sockets* seguros), acceder sitios restringidos y hasta instalar publicidad en el sitio víctima (Glosario Inteco en CCN, 2015, p. 342).

***Watering hole attack* (en español: ataque de abrevadero).**

i. Estrategia de ataque informático. El atacante quiere atacar a un grupo en particular (organización, sector o región). El ataque consiste en tres fases: 1. Adivinar (u observar) los sitios web que el grupo utiliza a menudo. 2. Infectar uno o más de estos sitios web con *malware*. 3. Con el tiempo, algunos miembros del grupo objetivo se infectarán. Esta

estrategia basa su eficacia en la confianza que el grupo ha depositado en las páginas web que sus miembros visitan con asiduidad. Es eficaz incluso con grupos concienciados que son resistentes a *spear phishing*[6] y otras formas de *phishing* (CCN, 2015, p. 931).

ii. Se produce cuando el atacante infecta una página legítima, que es visitada regularmente por las víctimas a quien se dirige la acción, para que esos visitantes queden infectados al visitarla (INCIBE, 2021, p. 78).

***Worm* (en español: gusano).**

i. Un programa autorreplicante, de autopropagación e independiente que utiliza mecanismos de la red para propagarse (CNSSI-4009, 2015, p. 133).

ii. Es un programa malicioso (o *malware*) que tiene como característica principal su alto grado de "dispersabilidad", es decir, lo rápidamente que se propaga. Mientras que los troyanos dependen de que un usuario acceda a una web maliciosa o ejecute un fichero infectado, los gusanos realizan copias de sí mismos, infectan a otros ordenadores y se propagan automáticamente en una red independientemente de la acción humana (INCIBE, 2021, p. 46).

***Web bug* (en español: error web).** Código malicioso, invisible para un usuario, colocado en sitios web de tal manera que permite a terceros rastrear el uso de servidores web y recopilar información sobre el usuario, incluida la dirección del IP (Protocolo de Internet), el nombre del anfitrión, el tipo y la versión del navegador, nombre y versión del sistema operativo, y el historial de *cookies* del navegador web (CNSSI-4009, 2015, p. 131).

***Zero days attack* (en español: ataque de día cero).**

i. Un ataque que explota una vulnerabilidad de hardware, *firmware* o software previamente desconocida (CNSSI-4009, 2015, p. 133).

ii. *Malware* diseñado para explotar un agujero de seguridad recién descubierto, desconocido por el desarrollador de software. "Día cero" se refiere a la cantidad de tiempo que tiene un desarrollador entre el conocimiento de un agujero de seguridad y el momento en que se hace público o cuando los *hackers* de sombrero negro[7] se enteran e intentan usar el agujero de seguridad para fines ilegítimos (Berkman Klein Center, 2012).

[6] Variante del *phishing*. En lugar de dirigirse a un público en general, los delincuentes seleccionan su grupo receptor de forma precisa.
[7] Un *black hat* (también conocido como *cracker*) es un *hacker* criminal o malicioso (CCN, 2015, p. 318).

Bibliografía

Berkman Klein Center for Internet & Society. (2012) *Keyword Index and Glossary of Core Ideas.* Harvard University. Disponible en: https://cyber.harvard.edu/cybersecurity/Keyword_Index_and_Glossary_of_Core_Ideas (consultado el 27/06/2022)

Centro Criptológico Nacional, C. C. (agosto de 2015). Guía de Seguridad (CCN-STIC-401). Glosario y Abreviaturas. Disponible en: https://www.ccn-cert.cni.es/pdf/guias/glosario-determinos/22-401-descargar-glosario/file.html

Chicharro Lázaro. (2013). La violencia terrorista en el ciberespacio: Riesgos y normativa europea sobre ciberterrorismo. En Herrero, J. et al. (Ed.) *La Sociedad Ruido/ Entre el dato y el grito*, La Laguna (Tenerife): Sociedad Latina de Comunicación Social, p. 1-28.

Clarke, R. A., & Knake, R. K. (2014). Cyber war. Old Saybrook: Tantor Media, Incorporated.

Committee on National Security Systems/CNSS (6 de abril de 2015) Glossary. CNSSI No.4009. Disponible en: https://rmf.org/wp-content/uploads/2017/10/CNSSI-4009.pdf

Cornejo Montoya, Y., Verdezoto, V. H., & Villacís, A. (2019). Ciberdefensa, Ciberseguridad y sus efectos en la sociedad. 4(2). *International Multilingual Journal of Science and Technology.*

Denning, D. E. (2000). Cyberterrorism: The logic bomb versus the truck bomb. *Global Dialogue*, 2(4), 29.

Department of Defense Joint Publication (JP) 3-12 (8 de junio de 2018) Cyberspace Operations. Disponible en: https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf

IBM. (2022a). ¿Qué es un ataque cibernético?. Disponible en: https://www.ibm.com/ar-es/topics/cyber-attack?mhsrc=ibmsearch_a&mhq=INyeccion%20de%20sql (consultado el 16/6/2022)

IBM. (2022b) ¿Qué es la seguridad móvil?. Disponible en: https://www.ibm.com/ar-es/topics/mobile-security#:~:text=Phishing,n%C3%BAmeros%20de%20tarjetas%20de%20cr%C3%A9dito (consultado el 16/6/2022).

INCIBE, Instituto Nacional de Ciberseguridad (2021). Glosario de términos de ciberseguridad: una guía de aproximación para el empresario. Disponible en:

https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_glosario_ciberseguridad_2021.pdf

Lazar, E., & Costescu, D. N. (2019). Los ciberataques: una noción sin tipificación, pero con un futuro. *Anuario da Facultade de Dereito da Universidade da Coruña,* 22, 157-175, p.160.

LISA Institute (julio de 2021). *Hacktivismo: definición, tipos, modus operandi y motivaciones.* Disponible en: https://www.lisainstitute.com/blogs/blog/hacktivismo-definicion-tipos-modus-operandi-motivaciones

National Institute of Standards and Technology. (junio de 2017) Digital Identity Guidelines, NIST Special Publication 800-63-3. Disponible en: https://doi.org/10.6028/NIST.SP.800-63-3

National Institute of Standards and Technology. (septiembre de 2012). Guide for Conducting Risk Assessments. NIST Special Publication 800-30, Rev. 1. Disponible en: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf

National Institute of Standards and Technology. (mayo de 2015). Guide to Industrial Control Systems (ICS) Security. NIST Special Publication 800-82, Rev 2. http://dx.doi.org/10.6028/NIST.SP.800-82r2

National Institute of Standards and Technology. (septiembre de 2020). Security and Privacy Controls for Information Systems and Organizations. NIST Special Publication 800-53, Rev 5. Disponible en: https://doi.org/10.6028/NIST.SP.800-53r5

National Security Presidential Directive/NSPD-54 and Homeland Security Presidential Directive/HSPD-23. (8 de enero de 2008) Cybersecurity Policy. Disponible en: https://irp.fas.org/offdocs/nspd/nspd-54.pdf

Pollitt M. M. (1998). Ciberterrorism: Fact or Fancy. Computer Fraud & Security, vol.1998, issue 2. p. 8-10. Disponible en: https://doi.org/10.1016/S1361-3723(00)87009-8

Real Academia de Ingeniería. (s.f.). En *Diccionario Español de Ingeniería 1.0.* Recuperado el 16 de junio de 2022, de https://diccionario.raing.es/es/lema/ciberataque

Real Academia Española. (2021). *Diccionario de la lengua española* (23.ª ed.), [versión 23.5 en línea]. https://dle.rae.es

Sánchez Medero, Gema (2012) La ciberguerra: los casos de Stuxnet y Anonymous. *Derecom*, ISSN-e 1988-2629, Nº. 11.

Sancho, C. (2017). Ciberseguridad. Presentación del dossier/Cybersecurity. Introduction to Dossier. *URVIO. Revista Latinoamericana De Estudios De Seguridad*, (20), 8-15. Disponible en: https://doi.org/10.17141/urvio.20.2017.2859

Schmitt, M. (2017). *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (2nd ed.). Cambridge: Cambridge University Press. https://doi.org/10.1017/9781316822524

Shirey, R.W. (2007). Internet Security Glossary, Version 2. RFC, 4949, 1-365. Disponible en: https://www.rfc-editor.org/rfc/pdfrfc/rfc4949.txt.pdf