ANEXO II

Glosario de Términos de Ciberseguridad

Acceso: utilización de los recursos de un sistema de información (CCN, 2015, pág. 27).

Acceso remoto: la habilidad para acceder a una computadora desde una ubicación apartada. (Techopedia, 2019)

Activo de información: es cualquier información o sistema relacionado con el tratamiento de la misma que tenga valor para la organización. Pueden ser procesos de negocio, datos, aplicaciones, equipos informáticos, personal, soportes de información, redes, equipamiento auxiliar o instalaciones (CCN, 2015, pág. 7).

Adware: aplicaciones que durante su funcionamiento despliegan publicidad en ventanas emergentes o barreras de herramientas a cambio de la gratuidad en su utilización. Se diferencian de los programas gratuitos o freeware en que incorporan publicidad (CCN, 2015, pág. 42).

AES – *Advanced Encryption Standard*: es un cifrado simétrico que puede cifrar bloques de datos de 128 bits utilizando claves simétricas 128, 192 y 256 (Medina Vargas & Miranda Mnedez, 2015, pág. 19).

Amenaza: circunstancia desfavorable que puede ocurrir y que cuando sucede tiene consecuencias negativas sobre los activos provocando su indisponibilidad, funcionamiento incorrecto o pérdida de valor. Una amenaza puede tener causas naturales, ser accidental o intencionada (CCN, 2015, pág. 57).

APT – Amenaza Persistente Avanzada: un actor que representa una amenaza y que posee niveles sofisticados de pericia e importantes recursos que le permiten crear las oportunidades para lograr sus objetivos mediante la utilización de múltiples vectores de ataque. Una amenaza persistente avanzada (i) persigue repetidamente su objetivo durante un período extenso de tiempo, (ii) de adapta a los esfuerzos de los defensores para resistirlos y (iii) está decidido a ejecutar sus objetivos. (Board, 2018, pág. 7)

Análisis de riesgos: es un proceso que comprende la identificación de activos de información, sus vulnerabilidades y las amenazas a los que se encuentran expuestos, así como la probabilidad de ocurrencia y el impacto de las mismas, a fin de determinar los controles adecuados para tratar el riesgo (CCN, 2015, pág. 19). Permite comprender la naturaleza del riesgo y determinar el nivel de riesgo[1].

Ancho de banda: es el rango de frecuencia que pasa por un cierto canal de transmisión. El ancho de banda determina la velocidad a la que se puede transmitir la información a través del circuito: cuanto mayor sea el ancho de banda, más información se puede enviar en un período de tiempo determinado (Gartner, 2019).

Antivirus: es un programa informático específicamente diseñado para detectar, bloquear y eliminar código malicioso (virus, troyanos, gusanos, etc.) así como proteger los equipos de otros programas peligrosos conocidos genéricamente como *malware* (CCN, 2015, pág. 83).

Aplicaciones: es un tipo de software que permite la interacción entre el usuario y la computadora (comunicación) y le permite al usuario elegir opciones y ejecutar acciones que el programa le ofrece (Benítez Jiménez, 2012).

Ataque de fuerza bruta: es un procedimiento para averiguar una contraseña que consiste en probar todas las combinaciones posibles hasta encontrar la combinación correcta. Utilizan el método de prueba y error. (CCN, 2015, pág. 104)

Autenticación: el acto de verificar la identidad de un usuario y su elegibilidad para acceder a la información computarizada. La autenticación está diseñada para proteger contra conexiones de acceso fraudulentas[2].

***Backup*:** Copia de seguridad que se realiza sobre ficheros o aplicaciones contenidas en un ordenador con la finalidad de recuperar los datos en el caso de que el sistema de información sufra daños o pérdidas accidentales de los datos almacenados (CCN, 2015, pág. 311).

[1] ISO/IEC Guía 73:2010.
[2] COBIT:2006

Bases de datos: una gran cantidad de información que ha sido sistematizada para su correcto almacenamiento, de forma tal que los datos que allí están contenidos puedan ser utilizados cuando se considere necesario, pudiendo ser posteriormente reordenados u organizados (Sistemas, 2019).

BCP: Abreviatura de «*Business Continuity Plan*». Es un conjunto formado por planes de actuación, planes de emergencia, planes financieros, planes de comunicación y planes de contingencias destinados a mitigar el impacto provocado por la concreción de determinados riesgos sobre la información y los procesos de negocio de una compañía (CCN, 2015, pág. 673).

BIA: Abreviatura de «*Business Impact Analysis*» o análisis del impacto del negocio. Se trata de un informe que muestra el coste ocasionado por la interrupción de los procesos críticos de negocio. Este informe permitirá asignar una criticidad a los procesos de negocio, definir los objetivos de recuperación y determinar un tiempo de recuperación a cada uno de ellos (CCN, 2015, pág. 69).

***Blade*:** es un tipo de servidor para Centros de Procesos de Datos que está diseñado para aprovechar el espacio, reducir el consumo y simplificar su explotación. Se encuentra dentro de un chasis o carcasa que alberga múltiples servidores físicos o cuchillas dentro de él. Todo el sistema está a menudo está montado en racks (Brok Solutions, 2019).

Certificación digital: documento digital firmado digitalmente por un certificador, que vincula los datos de verificación de firma a su titular[3].

Ciberamenaza: amenaza a los sistemas y servicios presentes en el ciberespacio o alcanzables a través de éste (CCN, 2015, pág. 202).

Ciberataque: 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, pág. 203)

[3] Art. 13, ley 25.506

Ciberespacio: 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[4] sino que es un dominio virtual que engloba todos los sistemas TICs (CCN, 2015, pág. 208).

Ciberdiplomacia: es la diplomacia puesta al servicio de la cooperación y creación de normas para el ciberespacio. (Riordan, 2019)

Ciberseguridad: es la preservación de la confidencialidad, integridad y disponibilidad de la información en el ciberespacio[5].

Cifrado: proceso para convertir información en un formato ilegible aplicando un algoritmo criptográfico y se utiliza para proteger la información de la divulgación no autorizada. Sinónimo de algoritmo de cifra (CCN, 2015, pág. 218).

***Cloud Computing* o computación en la nube:** paradigma que permite ofrecer servicios de computación a través de una red que usualmente es Internet. Permite almacenar información, ficheros y datos en servidores de terceros de forma que puedan ser accesibles desde cualquier terminal con acceso a la nube o a la red (INCIBE, pág. 17).

***Cookie* o galletita informática:** pequeño fichero que almacena información enviada por un sitio web y que se almacena en el equipo del usuario de manera que el sitio web puede consultar la actividad previa del usuario. Tiene como funciones: llevar el control de usuarios y recabar información sobre los hábitos de navegación del usuario (INCIBE, pág. 18).

Confidencialidad: es la propiedad de la información por la que se garantiza que está accesible únicamente a personal autorizado a acceder a dicha información (INCIBE, pág. 17).

Contraseña: información confidencial y secreta que permite el acceso a algo, a alguien o a un grupo de personas. En general es un grupo de caracteres que permite la autenticación de un usuario, entidad o recurso (CCN, 2015, pág. 286).

[4] ISO/IEC 27032: 2012.
[5] ISO/IEC 27032: 2012.

Criptografía: técnica que consiste en cifrar un mensaje (texto en claro) convirtiéndolo en un mensaje cifrado o criptograma que resulta ilegible para todo aquel que no conozca el sistema mediante el cual se ha cifrado (INCIBE, pág. 19).

Cuarentena: almacenar los archivos que contienen malware o software malicioso/dañino de forma aislada para su futura desinfección o examen (NICCS, 2018).

***Data Mining* o minería de datos**: es el proceso o técnica utilizada para analizar grandes conjuntos de información para descubrir patrones o correlaciones (NICCS, 2018).

***Defacement* o desfigurar:** es un ataque sobre un servidor web que cambia su apariencia con motivos ilegales (CCN, 2015, pág. 357).

Denegación de servicio o DoS: un conjunto de técnicas que tienen por objetivo dejar un servidor inoperativo. Mediante este tipo de ataques se busca sobrecargar un servidor y de esta forma impedir que los usuarios legítimos puedan utilizar los servicios por prestados por él. El ataque consiste en saturar con peticiones de servicio al servidor provocando su colapso (INCIBE, pág. 20).

Denegación de servicio distribuida o DDoS: ataque de denegación de servicio que se realiza utilizando múltiples puntos de ataque simultáneamente (CCN, 2015, pág. 363).

Dependencia de las infraestructuras críticas: una conexión específica e individual entre dos infraestructuras relacionadas unidireccionalmente a través de la cual el estado de una infraestructura influye o se correlaciona con el estado de la otra (Rinaldi, Peerenboom, & Kelly, 2001).

Desbordamiento de búfer: es una vulnerabilidad que aprovecha defectos en la programación y que tiene como objetivo acceder de manera remota al sistema atacado. Provoca un error o cuelgue del sistema de forma intencionada donde se desborda el límite de la memoria y se escriben datos en el espacio de memoria adyacente (INCIBE, pág. 20).

DES o *Data Encryption Standard*: algoritmo de cifrado simétrico basado en un secreto compartido o clave que cifra el texto en bloques de 64 bits. Está normalizado por ISO/IEC 8731-1 con el nombre de DEA (*Data Encryption Algorithm*) (CCN, 2015, pág. 375).

Descifrado: proceso ejecutado mediante técnicas criptográficas por el que se obtiene un texto en claro a partir del texto cifrado (CCN, 2015, pág. 372). Es la operación inversa de un cifrado reversible[6].

Dirección IP: del acrónimo en inglés «*Internet Protocol*» son un número único e irrepetible con el cual se identifica a todo sistema conectado a una red. Las direcciones IP pueden ser públicas (si son accesibles directamente desde cualquier sistema conectado a Internet) o privadas (si son internas a una red LAN) y solo accesibles desde los equipos conectados a esa red privada (INCIBE, pág. 20).

Dirección MAC o "*Media Access Control*": es un valor de 48 bits único e irrepetible que identifica todo dispositivo conectado a una red (INCIBE, pág. 21).

Disponibilidad: se trata de la capacidad de un servicio, un sistema o una información de ser accesible y utilizable por los usuarios o procesos autorizados cuando éstos lo requieran (INCIBE, pág. 21).

DMZ: Abreviatura de "*demilitarized zone*" o zona desmilitarizada. Sub-red física o lógica que proporciona una capa de seguridad adicional a la red privada interna de una organización. La DMZ agrega una capa de seguridad de red adicional entre Internet y la red interna de una organización, de modo que las partes externas sólo tengan conexiones directas a los dispositivos de la DMZ y no a toda la red interna. (CCN, 2015, pág. 939)

Documento digital: representación digital de actos o hechos, con independencia del soporte utilizado para su fijación, almacenamiento o archivo[7].

[6] ISO/IEC 7498-2
[7] Art. 6, ley 25.506.

Evaluación del riesgo: proceso de comparación de los resultados del análisis del riesgo con los criterios de riesgo para determinar si el riesgo y/o magnitud son aceptables o tolerables[8]. Ayuda a la toma de decisiones sobre el tratamiento del riesgo[9].

Evento o suceso de seguridad de la información: ocurrencia o cambio detectado en el estado de un sistema, servicio o red que indica una posible violación de la política de seguridad de la información, un fallo de los controles o una situación desconocida hasta el momento y que puede ser relevante para la seguridad[10].

Exploit: secuencia de comandos que aprovecha un fallo o una vulnerabilidad en el sistema (CCN, 2015, pág. 437) y cuyo objetivo es violar la seguridad de una red o sistema de información incumpliendo con la política de seguridad (NICCS, 2018) y provocar un comportamiento no deseado o imprevisto (INCIBE, pág. 22).

Fibra óptica: la tecnología y medio utilizado en la transmisión de datos como pulsos de luz a través de un cable o medio de fibra de vidrio o plástico (Techopedia, 2019).

Ficheros ocultos de contraseñas: archivo del sistema que almacena las contraseñas para autenticar a los usuarios y permanecen fuera del alcance de éstos (CCN, 2015, pág. 446).

***Firewall* o cortafuegos:** sistema de seguridad compuesto o bien de programas (*software*) o de dispositivos *hardware* situados en los puntos limítrofes de una red que tienen el objetivo de permitir y limitar el flujo de tráfico entre los diferentes ámbitos que protege sobre la base de un conjunto de normas y otros criterios. La funcionalidad básica es asegurar que todas las comunicaciones entre la red e Internet se realicen conforme a las políticas de seguridad de la organización o corporación. Estos sistemas suelen poseer características de privacidad y autentificación (INCIBE, pág. 18).

Firma digital: el resultado de aplicar a un documento digital un procedimiento matemático que requiere información de exclusivo conocimiento del firmante, encontrándose ésta bajo su control absoluto. La firma digital debe ser susceptible de

[8] ISO/IEC GUIA 73:2010
[9] ISO/IEC 27000:2014.
[10] ISO/IEC 27000:2014

verificación por terceras partes, tal que dicha verificación simultáneamente permita identificar al firmante y detectar cualquier alteración del documento digital posterior a su firma[11].

Firma electrónica: conjunto de datos electrónicos integrados, ligados o asociados de manera lógica a otros datos electrónicos, utilizado por el signatario como su medio de identificación, que carezca de alguno de los requisitos legales para ser considerada firma digital[12].

***Firmware*:** es un programa de *software* grabado de forma permanente en un dispositivo de *hardware* y está programado para dar instrucciones permanentes para comunicarse con otros dispositivos y realizar funciones básicas como entrada y salida (Techopedia, 2019).

Fuga de datos o fuga de información: es la pérdida de la confidencialidad de la información privada de una persona o empresa (INCIBE, pág. 22).

Funciones críticas: aquellas cuya interrupción, perturbación o afectación total o parcial puede tener un efecto significativo para la sociedad.

FTP o *File Transfer Protocol*: servicio de transferencia de ficheros a través de una red así como los servidores que permiten prestar este servicio (INCIBE, pág. 23).

Gestión de eventos o sucesos: plan de acción para atender a los incidentes e incorporar medidas de desempeño que permitan detectar futuras tendencias (CCN, 2015, pág. 480).

Gestión del riesgo: actividades coordinadas para dirigir y controlar una organización con respecto al riesgo[13].

Gobernanza de Internet: es el desarrollo y la aplicación por parte de los gobiernos, el sector privado y la sociedad civil, en sus respectivos roles, de principios, normas, reglas,

[11] Art. 2, ley 25.506
[12] Art. 5, ley 25.506
[13] ISO/IEC 27000:2014.

procedimientos de toma de decisiones y programas comunes que dan forma a la evolución y utilización de Internet (Unión Internacional de Telecomunicaciones, 2005).

Gusano informático: es un programa malicioso o *malware* que se propaga rápidamente ya que realizan copia de sí mismos e infectan otros ordenadores (INCIBE, pág. 23).

***Hash* (código):** bits obtenidos como resultado de aplicar una función resumen a unos datos (CCN, 2015, pág. 203).

Hosteado: cualquier dispositivo en una red TCP/IP con dirección IP. (CompTIA IT Glossary, 2010)

***Hostname*:** es un nombre o etiqueta exclusivo asignado a cualquier dispositivo conectado a una red de computadora. Facilita la diferenciación de distintas máquinas o dispositivos conectados a internet y/o una red (Techopedia, 2019).

HTTP o Protocolo de Transferencia de Hipertexto: es un protocolo que sigue un esquema petición-respuesta donde la información enviada se encuentra en texto claro (INCIBE, pág. 23).

HTTPS o Protocolo Seguro de Transferencia de Hipertexto: es un protocolo de red basado en el protocolo HTTP destinado a la transferencia segura de datos de hipertexto. En HTTPS el tráfico es cifrado mediante un algoritmo de cifrado simétrico cuya clave ha sido previamente intercambiada entre el navegador y el servidor (INCIBE, pág. 23). Proporciona autenticación y comunicación cifrada en la web sobre un túnel SSL (CCN, 2015, pág. 508).

IDS: un sistema de detección de intrusos o en inglés *Intrusion Detection System* es una aplicación usada para detectar accesos no autorizados a un ordenador o a una red. Estos accesos pueden ser ataques realizados por usuarios malintencionados con conocimientos de seguridad o usando herramientas automáticas. A diferencia de los IPS, estos sistemas sólo detectan intentos de acceso y no tratan de prevenir su ocurrencia (INCIBE, pág. 24).

Impacto: consecuencia que sobre un activo tiene la materialización de una amenaza (CCN, 2015, pág. 518).

Incidente: una ocurrencia que real o potencialmente resulte en una consecuencia adversa o amenaza para un sistema de información o la información que el sistema procesa, almacena o transmite y que puede requerir una acción de respuesta para mitigar las consecuencias (NICCS, 2018).

Incidente de seguridad: cualquier suceso que afecte a la confidencialidad, integridad o disponibilidad de los activos de información de la empresa u organismo (INCIBE, pág. 24).

Informática forense: proceso de investigación de los sistemas de información para detectar toda evidencia que pueda ser presentada como prueba fehaciente en un procedimiento judicial. Se aplican técnicas científicas y analíticas especializadas que permiten identificar, preservar, analizar y presentar datos que sean válidos dentro de un proceso legal (INCIBE, pág. 24).

Infraestructuras críticas de información: son las tecnologías de información, operación y comunicación, así como la información asociada, que resultan vitales para el funcionamiento o la seguridad de las Infraestructuras Críticas.

Infraestructuras críticas: son aquellas que resultan indispensables para el adecuado funcionamiento de los servicios esenciales de la sociedad, la salud, la seguridad, la defensa, el bienestar social, la economía y el funcionamiento efectivo del Estado, cuya destrucción o perturbación, total o parcial, los afecte y/o impacte significativamente.

Infraestructura tecnológica: el conjunto de dispositivos de hardware, software y comunicaciones utilizados por la organización para el cumplimiento de sus funciones, incluyendo el ámbito físico donde se encuentran ubicados.

Ingeniería inversa: el arte de acceder a información sensible a base de desensamblar y analizar el diseño de un sistema o componente (CCN, 2015, pág. 539).

Ingeniería social: tácticas utilizadas para obtener información o datos de naturaleza sensible de una persona (INCIBE, pág. 25). Suelen valerse de la buena voluntad y falta de precaución de los usuarios (CCN, 2015, pág. 539).

Integridad: propiedad de la información por la que se garantiza la exactitud de los datos transportados o almacenados asegurando que no se ha producido su alteración, pérdida o destrucción, ya sea de forma accidental o intencionada, por errores de *software* o *hardware* o por condiciones medioambientales (INCIBE, pág. 25.).

Interdependencia de las infraestructuras críticas: una relación bidireccional entre dos infraestructuras a través de las cuales el estado de cada infraestructura influye o se correlaciona con el estado de la otra (Rinaldi, Peerenboom, & Kelly, 2001).

Interfaces: La interfaz **es** una conexión entre dos sistemas, la región de contacto (Glosario IT, 2019).

Intranet: una red privada basada en el protocolo TCP/IP que pertenece a una organización u organismo y es accesible solo por sus miembros, empleados u otros con la autorización específica para ello (CCN, 2015, pág. 554).

Inyección de código: es una amenaza que se crea por métodos de codificación poco seguros y que tiene como resultado una validación de entradas impropias que permite que el atacante transfiera código malicioso al sistema (CCN, 2015, pág. 558).

Inyección de SQL: 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 (CCN, 2015, pág. 559).

IPS: Siglas de *Intrusion Prevention System* o sistema de prevención de intrusiones es un *software* que se utiliza para proteger a los sistemas de ataques y abusos. La tecnología de prevención de intrusos puede ser considerada como una extensión de los sistemas de detección de intrusos (IDS), pero en realidad es una tecnología más cercana a los firewalls (CCN, 2015, pág. 844).

***Jamming*:** interferencia de radio que dificulta o impide la recepción de señales radiadas (CCN, 2015, pág. 565).

LAN (del inglés *Local Area Network*) o Red de Área Local es una red informática de pequeña amplitud geográfica que suele limitarse a espacios como una oficina, una vivienda o un edificio. Una Red de Área Local permite interconectar distintos dispositivos de todo tipo. (INCIBE, pág. 26)

Lenguaje de programación: es una notación utilizada para escribir programas. Un lenguaje tiene una sintaxis (las palabras y símbolos utilizadas para escribir códigos de programa), una gramática (las reglas que definen una secuencia de palabras y símbolos significativos y correctos) y semántica (Apéndice W4 - Glosario de términos de Programación, pág. 10).

Login: procedimiento seguido por un usuario para establecer una sesión con un sistema de información (CCN, 2015, pág. 581).

***Malware*:** o código malicioso/dañino es un *software* que compromete la operación de un sistema al realizar una función o proceso no autorizado (NICCS, 2018). Acorde a la ISO/IEC, fue diseñado específicamente para dañar o interrumpir un sistema[14] sin conocimiento ni consentimiento del propietario (CCN, 2015, pág. 254).

Máquina virtual: es una implementación de *software* de una arquitectura similar al *hardware* que ejecuta instrucciones predefinidas de manera similar a una unidad de procesamiento central física. (Gartner, 2019)

Matriz de riesgo: herramienta que permite presentar conjuntamente varios riesgos de forma que quede clara su importancia (CCN, 2015, pág. 586).

Metadatos: el conjunto de datos relacionados con un documento y que recogen información fundamentalmente descriptiva del mismo, así como información de administración y gestión (INCIBE, pág. 26).

[14] ISO/IEC 18028-4:2005

Monitorización de la red: ataque de interceptación en red donde el atacante accede a los paquetes que circulan por la red y los analiza para descubrir contraseñas de los usuarios (CCN, 2015, pág. 613).

MPLS: es un mecanismo que se utiliza en las infraestructuras de red de computadoras para acelerar el tiempo que tarda un paquete de datos en fluir de un nodo a otro. Principalmente implementa y utiliza etiquetas para tomar decisiones de enrutamiento. El mecanismo de conmutación basado en etiquetas permite que los paquetes de red fluyan en cualquier protocolo. Funciona asignando una etiqueta o identificador único a cada paquete de red. (Techopedia, 2019)

NAC: un proceso de control de acceso a la red agrega políticas a la red para controlar el acceso de los dispositivos y los usuarios. Las políticas pueden basarse en la autenticación del dispositivo y/o usuario y el estado de la configuración del punto final. (Gartner, 2019)

Nivel de riesgo: magnitud de un riesgo o combinación de riesgos expresados en términos de las consecuencias y su probabilidad (CCN, 2015, pág. 618).

No repudio: es la capacidad de demostrar la identidad del emisor de esa información para certificar que los datos provienen de la fuente que dice ser (INCIBE, pág. 27). Permite afirmar la autoría de un mensaje o información (CCN, 2015, pág. 620).

Ocultación: técnica utilizada por algunos virus para no ser localizables (CCN, 2015, pág. 636).

P2P o *Peer-to-peer*: es un modelo de comunicaciones entre sistemas o servicios en el cual todos los nodos/extremos son iguales, tienen las mismas capacidades y cualquiera de ellas puede iniciar la comunicación. Todos los nodos actúan como servidores y clientes a la vez (INCIBE, pág. 27).

Parche de seguridad: conjunto de cambios que se aplican aun *software* para corregir errores de seguridad en programas o sistemas operativos. Suelen ser desarrollados por el fabricante a partir de la detección de una vulnerabilidad (INCIBE, pág. 27).

Penetración: violación de un sistema de seguridad permitiendo el acceso a los recursos supuestamente protegidos de forma ilícita (CCN, 2015, pág. 655).

***Pentest* o prueba de penetración**: es un ataque a un sistema *software* o *hardware* con el objetivo de encontrar vulnerabilidades. Se aplica un análisis activo de cualquier vulnerabilidad potencial, configuraciones deficientes o inadecuadas desde la posición de un atacante. El objetivo es determinar la viabilidad de un ataque y el impacto (INCIBE, pág. 28).

***Performance*:** el desempeño con respecto al rendimiento de una computadora, un dispositivo, un sistema operativo, un programa o una conexión a una red (Typhon Empresa Desarrolladora de Software, 2019).

PGP o *Pretty Good Privacy*: es un programa para proteger la información transmitida por internet mediante el uso de criptografía de clave pública, así como facilitar la autenticación de documentos mediante firma digital (CCN, 2015, pág. 660).

***Pharming*:** ataque informático que aprovecha la vulnerabilidad del *software* de los servidores DNS 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, pág. 28).

Phishing: 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, pág. 662).

Política: orientaciones o directrices que rigen la actuación de una persona o entidad en un asunto o campo determinado (CCN, 2015, pág. 679). Tiene como propósito influenciar y guiar en la toma de decisiones presentes y futuras describiendo, además, las consecuencias de la falta de cumplimiento de las mismas[15].

Política de seguridad: decisiones o medidas de seguridad que el organismo toma respecto a la seguridad de sus sistemas de información luego de evaluar el valor de sus

[15] COBIT 2006

activos y los riesgos (INCIBE, pág. 30). Suele plasmarse en un documento escrito (CCN, 2015, pág. 682).

Potencial de ataque: percepción de las posibilidades de éxito de un ataque expresado en función de la capacidad del atacante y su motivación para atacar (CCN, 2015, pág. 690).

PPP o *Point-to-Point Protocol*: es un protocolo estándar de internet que permite establecer una comunicación a nivel de enlace entre dos computadoras (CCN, 2015, pág. 691).

Privilegio: atributo, propiedad o capacidad asignada a una entidad o persona por una autoridad para el uso de un servicio controlado o restringido (CCN, 2015, pág. 697).

Protocolo: sistema de reglas que permiten que dos o más entidades se comuniquen entre ellas para transmitir información por medio de cualquier tipo de medio físico. Pueden ser implementados por hardware, software o una combinación de ambos (INCIBE, pág. 30).

***Proxy Services*:** El proxy es tanto el equipo, como el *software* encargado de dar el servicio que hacen de intermediario en las peticiones de los equipos de las redes LAN hacia Internet. Su objetivo es centralizar el tráfico entre Internet y una red privada, de forma que se evita que cada una de las máquinas de la red privada tenga que disponer necesariamente de una conexión directa a Internet y una dirección IP pública (INCIBE, pág. 30).

Puerta encubierta: mecanismo oculto que permite acceder a un sistema obviando los mecanismos autorizados de acceso (CCN, 2015, pág. 719).

Puerta trasera: cualquier punto débil de un programa o sistema mediante el cual una persona no autorizada puede acceder a un sistema (INCIBE, pág. 30). Pueden haber sido errores o fallas o haber sido creado a propósito por los propios autores (CCN, 2015, pág. 719).

Puertos: es la parte de una interfaz que se encuentra en el lado de la computadora a la que se conecta un conector de género opuesto de un cable (CompTIA IT Glossary, 2010).

Punto de acceso (AP): en una red local inalámbrica es el punto donde se conecta a la red terrestre o cableada (CCN, 2015, pág. 723).

Punto de acceso inalámbrico (WAP): dispositivo que interconecta equipos inalámbricos entre sí y con la red fija creando una red inalámbrica (CCN, 2015, pág. 723).

Rack: es un marco o estructura que contiene servidores informáticos o equipos de red, generalmente por medio de estantes o placas de montaje. La altura del equipo informático se expresa en unidades de rack (U), que equivalen a la distancia entre los incrementos de estantes en un rack estándar. (Gartner, 2019)

***Ransomware*:** 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, pág. 727).

Red: cualquier número de computadoras (por ejemplo, PC y servidores) y dispositivos (por ejemplo, impresoras y módems) unidos por un enlace de comunicaciones físicas (Gartner, 2019).

Red *Datacenter*: un servicio que va más allá de hacer que la funcionalidad del centro de datos esté disponible en una red. Emplea tecnología de red para tratar múltiples centros de datos y la red como un sistema único para acceder y procesar aplicaciones de manera eficiente. (Gartner, 2019)

Redundancia: el suministro de equipos o enlaces duplicados y de respaldo que asuman de inmediato la función del equipo o las líneas de transmisión que fallan. (Gartner, 2019)

Registro de actividad o *log*: es un registro oficial de eventos durante un rango de tiempo en particular que se emplea para registrar los datos o información sobre quién, qué, cuándo, dónde y porqué un evento ocurre (CCN, 2015, pág. 741).

Resiliencia: capacidad de un sistema o red para recuperarse de forma automática de una interrupción[16].

Riesgo: potencial de que una amenaza específica explote las debilidades de un activo o grupo de activos para ocasionar pérdida y/o daño a los activos. Por lo general se mide por medio de una combinación del impacto y la probabilidad de ocurrencia (CCN, 2015, pág. 756).

***Rootkit*:** *malware* o *software* malicioso instalado en una computadora que le da acceso privilegiado a un atacante como si fuera el administrador del equipo (CCN, 2015, pág. 771). Permite ocultar actividades ilegitimas en un sistema.

***Router*:** es un dispositivo que distribuye tráfico de red entre dos o más redes. Suele estar conectado al menos a dos redes (INCIBE, pág. 32).

RSA: sistema criptográfico de clave pública desarrollado por los criptográficos Rivest, Shamir y Adelman. Permite cifrar documentos como firmarlos digitalmente (INCIBE, pág. 32). Se basa en operaciones de potenciación en aritmética modular y su fortaleza radica en la dificultad de factorizar números extraordinariamente grandes (CCN, 2015, pág. 773).

***Sandbox* o entorno restringido:** un entorno de ejecución restringida y controlada que evita que un *malware* o *software* malicioso/dañino acceda a cualquier recurso del sistema, excepto aquellos para los cuales el *software* está actualizado (CCN, 2015, pág. 781).

Servidor: puede entenderse como servidor tanto el *software* que realiza ciertas tareas en nombre de los usuarios, como el ordenador físico en el cual funciona ese *software*. Se entiende por servidor tanto el equipo que almacena una determinada información

[16] COBIT 2006

como el programa de *software* encargado de gestionar dicha información y ofrecerla (INCIBE, pág. 32).

SCADA o *Supervisory Control and Data Acquisition*: 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, pág. 782).

SGSI o Sistema de Gestión de la Seguridad de la Información: es un conjunto de políticas, procesos, estándares, líneas maestras y herramientas de seguridad que permiten que la organización u organismo alcance sus objetivos (CCN, 2015, pág. 839). Siguen la norma ISO/IEC 27001 (INCIBE, pág. 33).

Sistemas de reputación: permiten conocer la opinión de otros compradores y sus experiencias para valorar si el sitio merece confianza. Se suele adoptar en los servicios de compraventa online (INCIBE, pág. 33).

Sistema informático: todo dispositivo aislado o conjunto de dispositivos interconectados o relacionados entre sí, cuya función, o la de alguno de sus elementos, sea el tratamiento automatizado de datos en ejecución de un programa (Ciberseguridad Glosario, s.f.).

SLA o *Service Level Agreement*: es un contrato escrito entre un proveedor de servicio y su cliente con el objeto de fijar el nivel acordado para la calidad del servicio (INCIBE, pág. 33).

SMPT o *Simple Mail Transfer Protocol*: es el protocolo simple de transferencia de correo utilizado para el intercambio de mensajes de correo electrónico (INCIBE, pág. 34).

***Sniffer*:** programa que monitoriza la información que circula por la red con el objeto de capturar información (INCIBE, pág. 34).

***Spyware* o programa espía:** es un *malware* o *software* malicioso que recopila información de un ordenador y la envía a una entidad remota sin el consentimiento del propietario del ordenador (INCIBE, pág. 35).

Suplantación o *Spoofing*: es una técnica de suplantación de identidad utilizando una dirección IP falseada para acceder a otra máquina de la red y conseguir acceso a recursos de forma ilegal (CCN, 2015, pág. 866).

Switches: un dispositivo que hace, rompe o cambia las conexiones en un circuito eléctrico; pasar a otro circuito eléctrico mediante un interruptor. En la industria de las telecomunicaciones, el término se usa a menudo como un sinónimo para el intercambio de sucursales privadas (PBX) o el interruptor de la oficina central (CO). (Gartner, 2019)

***Syn flood*:** ataque de denegación de servicio por el que se inunda un sistema de peticiones de conexión TCP syn (*synchronize* o sincronización) a un host con la intención de interrumpir su operación (CCN, 2015, pág. 871).

TCP/IP: familia de protocolos sobre los cuales funciona internet permitiendo la comunicación entre todos los servidores conectados a dicha red. Consta del protocolo IP (*Internet Protocol)* que transfiere los paquetes de datos hasta su destino correcto y el protocolo TCP (*Transfer Control Protocol)* que garantiza que la transferencia se lleve a cabo de forma correcta y confiable (INCIBE, pág. 36).

***TEARDROP* o ataque por fragmentación:** ataque de denegación de servicio que consiste en enviar paquetes IP o fragmentos de paquetes IP que están indebidamente construidos con el propósito de provocar un fallo en el equipo destino (CCN, 2015, pág. 875).

TLS: Abreviatura de *Transport Layer Security* o seguridad de la capa de transporte, es un protocolo criptográfico seguro ampliamente utilizado en la actualidad (INCIBE, pág. 35).

Token: componente de *hardware* o *software* diseñado para almacenar y proteger información criptográfica (CCN, 2015, pág. 889).

Topología de red: la disposición física de los componentes tangibles o el flujo de datos conceptualizado de forma lógica, el arreglo de una red. Ejemplos de topología incluyen diseños de estrella y anillo. (Vista College Professional Development, 2017)

Troyano: tipo de *malware* o *software* malicioso que se caracteriza por carecer de capacidad de autoreplicación (INCIBE, pág. 36).

URL o *Uniform Resource Locator*: es la dirección que identifica un contenido en internet (INCIBE, pág. 36).

Videoconferencia: comunicación por individuos o grupos utilizando sistemas que soportan la transferencia de imágenes, voz y datos a través de redes digitales o circuitos telefónicos. Los sistemas de videoconferencia pueden tomar la forma de grandes unidades dedicadas para reuniones grupales o pueden integrarse con computadoras personales de escritorio (Gartner, 2019)

Virtualización: medio para crear una versión virtual de un dispositivo o recurso (como un servidor o una red) en una máquina física. Generalmente se realiza con el apoyo de un software que implementa una capa de abstracción para que la máquina física y la virtual puedan comunicarse y compartir recursos (INCIBE, pág. 37).

Virus: programa de computadora que puede replicarse, infectar una computadora sin permiso o conocimiento del usuario y luego propagarse a otra computadora (NICCS, 2018).

VLAN: Una red de área virtual o VLAN (acrónimo de *Virtual Local Area Network*) es una red lógica independiente dentro de una red física de forma que es posible crear diferentes una VLAN que este conectadas físicamente a diferentes segmentos de una red de área local o LAN. Los administradores de este tipo de redes las configuran mediante software en lugar de hardware, lo que las hace extremadamente flexibles (INCIBE, pág. 37).

VoIP: señal de voz digitalizada que viaja a través de una red utilizando el protocolo IP (que es el utilizado por internet) y permite mantener conversaciones de voz sin necesidad de una conexión telefónica (INCIBE, pág. 37).

VPN: Una red privada virtual o *Virtual Private Network*, es una tecnología de red que permite una extensión segura de una red local (LAN) sobre una red pública o no controlada como Internet. Al establecerlas, la integridad de los datos y la confidencialidad se protegen mediante la autentificación y el cifrado (INCIBE, pág. 38).

Vulnerabilidad: debilidad de un activo o de un control que puede ser explotada por una o más amenazas[17].

WAN – *Wide Area Network*: Una red de comunicaciones que conecta dispositivos informáticos en ubicaciones geográficamente dispersas. Si bien una red de área local (LAN) generalmente sirve para un solo edificio o ubicación, una WAN cubre un área mucho más grande, como una ciudad, estado o país. Las WAN pueden usar líneas telefónicas o líneas de comunicación dedicadas. (Gartner, 2019)

Wi Fi o *Wireless Fidelity*: es una red de dispositivos inalámbricos interconectados entre sí y generalmente también conectados a Internet a través de un punto de acceso inalámbrico. Se trata por tanto de una red LAN que no utiliza un cable físico para el envío de la información (INCIBE, pág. 38).

Zombie: nombre que se le da a los ordenadores controlados de manera remota por un ciberdelincuente al haber sido infectados por un malware (INCIBE, pág. 39).

[17] ISO/IEC 27000:2014.

Referencias

Apéndice W4 - Glosario de términos de Programación. (s.f.). Obtenido de https://www.mhe.es/universidad/informatica/8448136640/archivos/apendice_general_4.pdf

Benítez Jiménez, E. (2012). Aplicaciones Informáticas. *Informática*. Obtenido de https://elisainformatica.files.wordpress.com/2012/11/aplicaciones-informc3a1ticas.pdf

Board, T. F. (12 de November de 2018). *Cyber Lexicon.* Obtenido de https://www.fsb.org/wp-content/uploads/P121118-1.pdf

Brok Solutions. (2019). Obtenido de https://www.broksolutions.com/que-es-un-servidor-blade-bro/

CCN, C. C. (Agosto de 2015). *Guía de Seguridad (CCN-STIC-401) - Glosario y Abreviaturas.* Obtenido de https://www.ccn-cert.cni.es/pdf/guias/glosario-de-terminos/22-401-descargar-glosario/file.html

Ciberseguridad Glosario. (s.f.). Obtenido de https://www.ciberseguridad.gob.cl/glosario/

CompTIA IT Glossary. (1 de Octubre de 2010). Obtenido de https://www.comptia.org/resources/comptia-it-glossary

Gartner. (2019). Obtenido de https://www.gartner.com/it-glossary/

Glosario IT. (2019). Obtenido de https://www.glosarioit.com

INCIBE, I. N. (s.f.). Glosario de términos de ciberseguridad: una guía de aproximación para el empresario. Obtenido de https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_glosario_ciberseguridad_metad.pdf

ISACA Glosario. (s.f.). Obtenido de https://www.isaca.org/Pages/Glossary.aspx

Medina Vargas, Y. T., & Miranda Mnedez, H. A. (2015). Comparación de Algoritmos Basados en la Criptografía Simétrica DES, AES, 3DES. *Revista Mundo FESC Edición 9*, 14-21.

NATO. (2014). Cyber Security Strategy for Defence. *ACST-Strategy-001*.

NICCS, N. I. (2018). *NICCS Glossary*. Obtenido de https://niccs.us-cert.gov/about-niccs/glossary

Rinaldi, S. M., Peerenboom, J. P., & Kelly, T. K. (December de 2001). IEEE Control System Magazine. *Identifying, Understandind and Analyzing Critical Infrastructure Interdependencies*. USA.

Riordan, S. (2019). *Cyberdiplomacy: Managing Security and Governance Online.*

Sistemas. (2019). Obtenido de https://sistemas.com/base-de-datos.php

Techopedia. (2019). Obtenido de https://www.techopedia.com/dictionary

Typhon Empresa Desarrolladora de Software. (2019). Obtenido de http://www.typhon.com.ar

Unión Internacional de Telecomunicaciones. (2005). *Cumbre Mundial sobre la Sociedad de la Información: Documentos Finales.*

University, E. I. (2011). Russia-US Bilateral On Cybersecurity Critical Terminology Foundations. Obtenido de https://www.files.ethz.ch/isn/130080/Russia-U%20S%20%20bilateral%20on%20terminology%20v76%20(2)-1.pdf

Vista College Professional Development. (2017). Obtenido de https://www.vistacollegepro.com/information-technology/comptia-a/comptia-a-glossary-and-definitions-list/

República Argentina - Poder Ejecutivo Nacional
2019 - Año de la Exportación

Hoja Adicional de Firmas
Anexo

Número: IF-2019-78455467-APN-SGM#JGM

CIUDAD DE BUENOS AIRES
Viernes 30 de Agosto de 2019

Referencia: EX-2018-55001386- -APN-DGDA#JGM

El documento fue importado por el sistema GEDO con un total de 23 pagina/s.

Digitally signed by GESTION DOCUMENTAL ELECTRONICA - GDE
DN: cn=GESTION DOCUMENTAL ELECTRONICA - GDE, c=AR, o=SECRETARIA DE GOBIERNO DE MODERNIZACION, ou=SECRETARIA DE MODERNIZACION ADMINISTRATIVA, serialNumber=CUIT 30715117564
Date: 2019.08.30 12:58:48 -03'00'

Leandro de la Colina
Director Nacional
Secretaría de Gobierno de Modernización
Jefatura de Gabinete de Ministros

Digitally signed by GESTION DOCUMENTAL ELECTRONICA - GDE
DN: cn=GESTION DOCUMENTAL ELECTRONICA - GDE, c=AR, o=SECRETARIA DE GOBIERNO DE MODERNIZACION, ou=SECRETARIA DE MODERNIZACION ADMINISTRATIVA, serialNumber=CUIT 30715117564
Date: 2019.08.30 12:58:49 -03'00'