GPF-OCEX 5312 Glosario de Ciberseguridad

Referencia: Glosario del ENS y de INCIBE

Documento elaborado por la Comisión Técnica de los OCEX y aprobado por la Conferencia de Presidentes de ASOCEX el 27/11/2017. Revisado el 29/05/2018: se ha incluido el término en inglés.

Activo (Asset)

Componente o funcionalidad de un sistema de información susceptible de ser atacado deliberada o accidentalmente con consecuencias para la organización. Incluye: información, datos, servicios, aplicaciones (software), equipos (hardware), comunicaciones, recursos administrativos, recursos físicos y recursos humanos. *(Esquema Nacional de Seguridad, en adelante ENS)*

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. Es susceptible de ser atacado deliberada o accidentalmente con consecuencias para la organización. *(Instituto Nacional de Ciberseguridad, en adelante INCIBE)*

Amenaza (Threat)

Eventos que pueden desencadenar un incidente en la Organización, produciendo daños materiales o pérdidas inmateriales en sus activos. *(CCN)*

Amenaza persistente avanzada (Advanced Persistent Threat -APT)

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. No todos los ataques de este tipo son muy avanzados y sofisticados, del mismo modo que no todos los ataques selectivos complejos y bien estructurados son una amenaza persistente avanzada. La motivación del adversario, y no tanto el nivel de sofisticación o el impacto, es el principal diferenciador de un ataque APT de otro llevado a cabo por ciberdelincuentes o hacktivistas. *(CCN)*

Análisis de riesgos (Risk analysis)

Utilización sistemática de la información disponible para identificar peligros y estimar los riesgos. *(ENS)*

Aprendizaje automático (Machine Learning)

Es una aplicación de la inteligencia artificial (I.A.) en la que las máquinas pueden “aprender de los resultados”.

Auditoría de la seguridad (Security Audit)

Revisión y examen independientes de los registros y actividades del sistema para verificar la idoneidad de los controles del sistema, asegurar que se cumplen la política de seguridad y los procedimientos operativos establecidos, detectar las infracciones de la seguridad y recomendar modificaciones apropiadas de los controles, de la política y de los procedimientos. *(ENS)*

Autenticación (Authentication)

Procedimiento para comprobar que alguien es quién dice ser cuando accede a un ordenador o a un servicio online. Este proceso constituye una funcionalidad característica para una comunicación segura. *(INCIBE)*

Autenticidad (Authenticity)

Propiedad o característica consistente en que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos. *(ENS)*

Bastionado (System Hardening)

Es el proceso de asegurar un sistema mediante la reducción de vulnerabilidades en el mismo.

Big Data (Big Data)

Big Data es un gran volumen, una alta velocidad y una gran variedad de activos de información que demandan rentabilidad e innovación en el procesamiento de la información para aumentar la comprensión y la toma de decisiones.

Categoría de un sistema (System Classification)

Es un nivel, dentro de la escala Básica-Media-Alta, con el que se adjetiva un sistema a fin de seleccionar las medidas de seguridad necesarias para el mismo. La categoría del sistema recoge la visión holística del conjunto de activos como un todo armónico, orientado a la prestación de unos servicios. *(ENS)*

Ciber-resiliencia (Cyber-resilience)

Ciber-resiliencia se refiere generalmente a las capacidades organizativas y técnicas para absorber impactos externos e internos, y recuperar la normalidad en las operaciones de una forma controlada.

Ciberseguridad (Cybersecurity)

Ver seguridad de las redes y de la información.

Confidencialidad (Confidentiality)

Propiedad o característica consistente en que la información ni se pone a disposición, ni se revela a individuos, entidades o procesos no autorizados. *(ENS)*

Es la propiedad de la información, por la que se garantiza que está accesible únicamente a personal autorizado a acceder a dicha información. *(INCIBE)*

La confidencialidad de la información constituye la piedra angular de la seguridad de la información. Junto con la integridad y la disponibilidad suponen las tres dimensiones de la seguridad de la información. *(INCIBE)*

Cortafuegos (Firewall)

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. *(INCIBE)*

La funcionalidad básica de un cortafuego es asegurar que todas las comunicaciones entre la red e Internet se realicen conforme a las políticas de seguridad de la organización o corporación. *(INCIBE)*

Datos (Data)

Representación de la información usando algún formato que permita su comunicación, interpretación, almacenamiento y procesado automático.

Datos estructurados (Structured Data)

Son datos archivados en tablas o en base de datos relacionales.

Datos no estructurados (Non-Structured Data)

Son datos de muy diversos formatos.

Por ejemplo: fotos, videos, datos de WhatsApp, Facebook, Twiter, datos de diversos sensores, del IoT; datos biométricos, huellas digitales, escáner de retina; emails, registros de voz, historias clínicas, etc.

Los datos no estructurados, generalmente son datos binarios que no tienen estructura interna identificable. Es un conglomerado masivo y desorganizado de varios objetos que no tienen valor hasta que se identifican y almacenan de manera organizada. *(http://smarterworkspaces.kyocera.es/blog/diferencia-datos-estructurados-no-estructurados/)*

Disponibilidad (Availability)

Propiedad o característica de los activos consistente en que las entidades o procesos autorizados tienen acceso a los mismos cuando lo requieren. *(ENS)*

Efecto perturbador significativo (Art 6 DCbs) (Significant Disruptive Effect)

A la hora de determinar la importancia de un efecto perturbador se tendrán en cuenta al menos los siguientes factores intersectoriales:

a) el número de usuarios que confían en los servicios prestados por la entidad de que se trate;

b) la dependencia de otros sectores que figuran en el anexo II sobre el servicio prestado por esa entidad;

c) la repercusión que podrían tener los incidentes, en términos de grado y duración, en las actividades económicas y sociales o en la seguridad pública;

d) la cuota de mercado de la entidad; e) la extensión geográfica con respecto a la zona que podría verse afectada por un incidente;

e) la importancia de la entidad para mantener un nivel suficiente del servicio, teniendo en cuenta la disponibilidad de alternativas para la prestación de ese servicio.

f) también se tendrán en cuenta factores específicos del sector, cuando proceda.

Gestión de riesgos (Risk management)

Actividades coordinadas para dirigir y controlar una organización con respecto a los riesgos. *(ENS)*

Hallazgo de auditoría (Audit finding)

Resultados de la evaluación de la evidencia de auditoría frente a los criterios de auditoría. Los hallazgos de auditoría pueden indicar conformidad o no conformidad. Pueden conducir a la identificación de oportunidades de mejora o al registro de buenas prácticas. Si los requisitos de auditoría se seleccionan de entre los requisitos legales u otros requisitos, el hallazgo de auditoría se denomina “cumplimiento” o “no cumplimiento”. *(UNE-EN-ISO 19011:2012) (CCN-STIC-802)*

Incidente de seguridad (Security Incident)

Todo hecho que tenga efectos adversos reales en la seguridad de las redes y sistemas de información. *(Art 4 DCbs)*

A fin de determinar la importancia de los efectos de un incidente, se tendrán en cuenta, en particular, los siguientes parámetros: *(Art 14.4 DCbs)*

a) el número de usuarios afectados por la perturbación del servicio esencial;

b) la duración del incidente;

c) la extensión geográfica con respecto a la zona afectada por el incidente.

Cualquier suceso que afecte a la confidencialidad, integridad o disponibilidad de los activos de información de la empresa, por ejemplo: acceso o intento de acceso a los sistemas, uso, divulgación, modificación o destrucción no autorizada de información. *(INCIBE)*

Integridad (en relación con los controles de procesos/aplicación) (completeness)

Completitud. *(En las NIAs y otros documentos técnicos en inglés el término utilizado es “completeness”, que se ha traducido como integridad, lo que puede inducir a confusión con su significado cuando se habla de seguridad de la información).*

Se han registrado todos los hechos y transacciones que tenían que registrarse. (GPF-OCEX 1317).

Integridad (en relación con la seguridad de la información) (Integrity)

Propiedad o característica consistente en que el activo de información no ha sido alterado de manera no autorizada. *(ENS)*

Es la 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)*

Inteligencia artificial (Artificial Intelligence)

Es el concepto de máquinas que pueden realizar tareas de manera tal que podíamos considerar "inteligentes".

Internet de las cosas (Internet of Things)

Este término se encuentra en plena evolución. En esencia, actualmente se refiere a redes de objetos físicos (edificios, marcapasos, biosensores, software, etc.), en definitiva sensores que disponen de conectividad en red que les permiten recolectar información de todo tipo (CCN).

Medidas de seguridad (Security Countermeasures)

Conjunto de disposiciones encaminadas a protegerse de los riesgos posibles sobre el sistema de información, con el fin de asegurar sus objetivos de seguridad. Puede tratarse de medidas de prevención, de disuasión, de protección, de detección y reacción, o de recuperación. *(ENS)*

Metadatos (Metadata)

Los metadatos son el conjunto de datos relacionados con un documento y que recogen información fundamentalmente descriptiva del mismo, así como información de administración y gestión. Los metadatos es una información que enriquece el documento al que está asociado. *(INCIBE)*

No repudio (Non-repudio)

El no repudio en el envío de información a través de las redes es capacidad de demostrar la identidad del emisor de esa información. El objetivo que se pretende es certificar que los datos, o la información, provienen realmente de la fuente que dice ser. *(INCIBE)*

El problema del control de autenticidad dentro de los sistemas de información a través de la Red, en relación tanto de la identidad del sujeto como del contenido de los datos, puede ser resuelto mediante la utilización de la firma electrónica (o digital). *(INCIBE)*

Es sinónimo de autenticidad. *(INCIBE)*

Plan de contingencia (Contigency Plan)

Un Plan de Contingencia de las Tecnologías de la Información y las Comunicaciones (TIC) consiste en una estrategia planificada en fases, constituida por un conjunto de recursos de respaldo, una organización de emergencia y unos procedimientos de actuación, encaminados a conseguir una restauración ordenada, progresiva y ágil de los sistemas de información que soportan la información y los procesos de negocio considerados críticos en el Plan de Continuidad de Negocio de la compañía. *(INCIBE)*

Plan de continuidad (Continuity Plan)

Un Plan de Continuidad de Negocio 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. *(INCIBE)*

Política de seguridad (Security Policy)

Son las decisiones o medidas de seguridad que una empresa ha decidido tomar respecto a la seguridad de sus sistemas de información después de evaluar el valor de sus activos y los riegos a los que están expuestos. *(INCIBE)*

Este término también se refiere al documento de nivel ejecutivo mediante el cual una empresa establece sus directrices de seguridad de la información. *(INCIBE)*

Conjunto de directrices plasmadas en documento escrito, que rigen la forma en que una organización gestiona y protege la información y los servicios que considera críticos. *(ENS)*

Principios básicos de seguridad (Basic Principles of Security)

Fundamentos que deben regir toda acción orientada a asegurar la información y los servicios. *(ENS)*

Proceso (Process)

Conjunto organizado de actividades que se llevan a cabo para producir a un producto o servicio; tiene un principio y fin delimitado, implica recursos y da lugar a un resultado. *(ENS)*

Redes y sistemas de información (Art 4 DCbs) (Network and Information Systems)

a) una red de comunicaciones electrónicas;

b) todo dispositivo o grupo de dispositivos interconectados o relacionados entre sí en el que uno o varios de ellos realizan, mediante un programa, el tratamiento automático de datos digitales, o

c) los datos digitales almacenados, tratados, recuperados o transmitidos mediante elementos contemplados en las letras a) y b) para su funcionamiento, utilización, protección y mantenimiento;

Requisitos mínimos de seguridad (Minimum Security Requirements)

Exigencias necesarias para asegurar la información y los servicios. *(ENS)*

Riesgo (Risk)

Toda circunstancia o hecho razonablemente identificable que tenga un posible efecto adverso en la seguridad de las redes y sistemas de información. *(Art 4 DCbs)*

Estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la organización. *(ENS)*

Router (Router)

Es un dispositivo que distribuye tráfico de red entre dos o más diferentes redes. Un router está conectado al menos a dos redes, generalmente LAN o WAN y el tráfico que recibe procedente de una red lo redirige hacia la(s) otra(s) red(es). *(INCIBE)*

En términos domésticos un router es el dispositivo que proporciona el proveedor de servicios de telefonía (o ISP) y que permite conectar nuestra LAN doméstica con la red del IS. *(INCIBE)*

El router comprueba las direcciones de destino de los paquetes de información y decide por qué ruta serán enviados, para determinar el mejor camino emplean cabeceras y tablas de comparación. *(INCIBE)*

Seguridad de la información (Information Security)

Garantiza que dentro de la entidad, la información está protegida frente a divulgación no autorizada (confidencialidad), modificación indebida (integridad), y que está accesible cuando se solicita (disponibilidad). (ISACA)

Seguridad de las redes y de la información (Network and Information Security)

Es la capacidad de las redes o de los sistemas de información de resistir, con un determinado nivel de confianza, los accidentes o acciones ilícitas o malintencionadas que comprometan la disponibilidad, autenticidad, integridad y confidencialidad de los datos almacenados o transmitidos y de los servicios que dichas redes y sistemas ofrecen o hacen accesibles. *(ENS)*

La capacidad de las redes y sistemas de información de resistir, con un nivel determinado de fiabilidad, toda acción que comprometa la disponibilidad, autenticidad, integridad o confidencialidad de los datos almacenados, transmitidos o tratados, o los servicios correspondientes ofrecidos por tales redes y sistemas de información o accesibles a través de ellos. *(Art 4 DCbs)*

La ciberseguridad trata de la protección de los activos de información frente a las amenazas a la información procesada, almacenada y transportada por sistemas de información interconectados. (ISACA)

Sistema de gestión de la seguridad de la información (SGSI) (Information Security Management System)

Sistema de gestión que, basado en el estudio de los riesgos, se establece para crear, implementar, hacer funcionar, supervisar, revisar, mantener y mejorar la seguridad de la información. El sistema de gestión incluye la estructura organizativa, las políticas, las actividades de planificación, las responsabilidades, las prácticas, los procedimientos, los procesos y los recursos. *(ENS)*

Sistema de información (Information System)

Conjunto organizado de recursos para que la información se pueda recoger, almacenar, procesar o tratar, mantener, usar, compartir, distribuir, poner a disposición, presentar o transmitir. *(ENS)*

Los elementos de un sistema de información son: hardware, software, soportes de información, comunicaciones, instalaciones, personal y servicios provisionados por terceros.

Conjunto de aplicaciones, servicios, activos relacionados con tecnologías de la información y otros componentes para manejar información. *(UNE-ISO/IEC 27000:2014; CCN-STIC-830)*

Tecnologías cognitivas (Cognitive Technologies)

Las tecnologías cognitivas utilizan los principios de inteligencia artificial y del aprendizaje automático pero necesitan algunos elementos de criterio humano de interpretación para actuar a partir de la información y alcanzar un resultado.

Las personas participan en las actividades de la I.A./A.A. para alcanzar la decisión final. Esto lleva a algunos a denominar los sistemas de tecnologías cognitiva como “inteligencia aumentada” (máquina + persona) en lugar de simplemente I.A.

Trazabilidad (Traceability)

Propiedad o característica consistente en que las actuaciones de una entidad pueden ser imputadas exclusivamente a dicha entidad. *(ENS)*

Vulnerabilidad (Vulnerability)

Una debilidad que puede ser aprovechada por una amenaza. *(ENS)*

Fallos o deficiencias de un programa que pueden permitir que un usuario no legítimo acceda a la información o lleve a cabo operaciones no permitidas de manera remota. *(INCIBE)*

Los agujeros de seguridad pueden ser aprovechadas por atacantes mediante *exploits*, para acceder a los sistemas con fines maliciosos. Las empresas deben ser conscientes de estos riesgos y mantener una actitud preventiva, así como llevar un control de sus sistemas mediante actualizaciones periódicas. *(INCIBE)*