ue STEAM essentials

CIBERSEGURIDAD E INFRAESTRUCTURAS CRÍTICAS

LEOPOLDO SANTOS
Escuela de Arquitectura, Ingeniería y Diseño
UNIVERSIDAD EUROPEA DE MADRID

La ciberseguridad es un concepto muy en boga, debido a los continuos incidentes de seguridad que afectan a empresas y organismos del sector público, o incluso infraestructuras críticas. El cambio tecnológico y la adopción de tecnologías que obligan a estar más tiempo conectados, y que forman parte de la transformación digital que se está llevando a cabo por empresas e instituciones de diversa índole provocan una mayor exposición a ciberataques dirigidos en su mayoría a cobrar un rescate por los datos. Es por ello, que tener una visión global de la ciberseguridad y de las buenas prácticas a considerar puede reducir los riesgos y ayudar a entender los retos a los que nos enfrentamos como sociedad.

PALABRAS CLAVE •
Ciberseguridad, infraestructuras críticas, malware, phishing, ransomware

CÓMO CITAR ESTE ARTÍCULO •
Santos, Leopoldo. 2021. **"Ciberseguridad e infraestructuras críticas"** en: UEM STEAM Essentials

INTRODUCCIÓN

Vivimos en un mundo en constante cambio tecnológico y, por tanto, en lo que se refiere a las tecnologías de la información y las comunicaciones, cada vez más interconectados. Esto nos proporciona muchas posibilidades tanto a las empresas como a los ciudadanos para hacer negocios, gestiones con la Administración o disfrutar del ocio, pero por otro lado nos acerca a una gran variedad de amenazas. Es en este espacio donde la ciberseguridad tiene su razón de ser.

La ciberseguridad no tiene una definición acordada entre todos los países, organismos e instituciones que de una u otra manera se dedican a la misma. Lo que sí que está más claro es el propósito de ciberseguridad. No es fácil encontrar una definición que cubra todos los aspectos de la Ciberseguridad, debido a lo amplio que es el término y los dominios de los que se ocupa, Craigen et al (2014) proponen la siguiente definición:

"Ciberseguridad es la organización y agrupación de recursos, procesos, y estructuras para proteger el ciberespacio y los sistemas habilitados para trabajar en el ciberespacio de sucesos que no se alinean con la normativa jurídica vigente (de jure) con los derechos de propiedad obtenidos por la fuerza de los hechos (de facto)."

Posteriormente, Sols (2020), dentro de la serie STEAM Essentials -revista científica editada y publicada por la Universidad Europea de Madrid- proporciona la siguiente definición:

"Es el conjunto de medios y recursos que permiten proteger los activos digitales de una organización. Los principios de la ciberseguridad son la confidencialidad (protección de la información contra el acceso no autorizado), la integridad (protección de la información contra modificaciones no autorizadas) y la disponibilidad (acceso fiable y en el momento requerido a los datos necesitados)."

Aunque se completa y detalla un poco más en la propuesta de Schatz et al. (2017):

"El enfoque y acciones asociadas con los procesos de gestión de riesgos de seguridad seguidos por las organizaciones y estados para proteger la confidencialidad, integridad y disponibilidad de los datos y activos usados en el ciberespacio. El concepto incluye guías, políticas y colecciones de salvaguardas, tecnologías, herramientas y entrenamiento para proporcionar la mejor protección del estado del entorno del ciberespacio y sus usuarios."

Desde el punto de vista nacional no hay una definición oficial, aunque sí que se establece el propósito de la Ciberseguridad en la Estrategia Nacional de Ciberseguridad (2019) donde se indica que la Ciberseguridad es la seguridad del ciberespacio, y más concretamente consiste en *"Garantizar un uso seguro y responsable de las redes y los sistemas de información y comunicaciones a través del fortalecimiento de las capacidades de prevención, detección y respuesta a los ciberataques potenciando y adoptando medidas específicas para contribuir a la promoción de un ciberespacio seguro y fiable".*

Por otro lado, las sociedades modernas son cada vez más dependientes de las infraestructuras, en especial de las críticas. Estas infraestructuras no son independientes sino más bién lo contrario, ya que se necesitan las unas a las otras para producir el rendimiento esperado. Un ejemplo es la red de ferrocarriles, que tiene una dependencia directa de la red eléctrica y de la red de telecomunicaciones para su normal funcionamiento, entendiéndose con tal la gestión de la circulación de trenes, las señales o las comunicaciones.

Por tanto, el funcionamiento de una sociedad, la calidad de vida de los ciudadanos y la economía de una nación depende del funcionamiento continuo y fiable de sus infraestructuras, y por ello los estados establecen cuales son las infraestructuras críticas para el funcionamiento del país. En el caso de España, la Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de infraestructuras críticas (BOE, 2011), establece que es una infraestructura estratégica:

"Las instalaciones, redes, sistemas y equipos físicos y de tecnología de la información sobre las que descansa el funcionamiento de los servicios esenciales."

Y también, que es una infraestructura crítica:

"Las infraestructuras estratégicas cuyo funcionamiento es indispensable y no permite soluciones alternativas, por lo que su perturbación o destrucción tendría un grave impacto sobre los servicios esenciales."

Los sectores estratégicos que se definen en la Ley 8/2011 son 12, que se identificaron con los distintos Ministerios y organismos competentes son: Administración, espacio, industria nuclear, industria química, instalaciones de investigación, agua, energía, salud, tecnologías de la información y las comunicaciones, transporte, alimentación y sistema financiero y tributario. Es evidente, que un ataque a cualquiera de estas infraestructuras críticas tiene un impacto directo en servicios esenciales para los ciudadanos. Por tanto, la ciberseguridad es una necesidad de nuestra sociedad.

FORMAS DE ABORDAR LA CIBERSEGURIDAD

Se suele articular la ciberseguridad desde una triple vertiente:

- **Estratégica:** Considera el marco regulatorio, la legislación, las políticas de seguridad, los procesos y los sistemas de gestión de la seguridad en su más amplio aspecto. Esta vertiente, que afecta a prácticamente todos los dominios de la ciberseguridad, se ocupa principalmente de establecer el marco de referencia que se va a utilizar para definir los controles, establece el sistema de gestión de la seguridad de la información que se va a aplicar o define, entre otras, la política de concienciación de los empleados de la organización.

- **Táctica:** Se ocupa del análisis de los riesgos, los planes de continuidad de negocio, los planes de seguridad o las auditorías. Define como se va a realizar la gestión de accesos e identidades, si es necesaria una infraestructura de clave pública, o como van a ser los procedimientos de seguridad física a aplicar.

- **Técnica u operativa:** Esta vertiente se centrada en el trabajo más técnico, y por tanto del nivel de detalle de la configuración, parametrización y programación del software necesario para el trabajo habitual en operaciones y que incluye los sistemas operativos, bases de datos, aplicaciones, servidores, comunicaciones o la seguridad física y de las personas. Las actividades que se desarrollan van desde la configuración de un firewall, hasta la administración de seguridad del sistema.

Con el objeto de abordar de una manera integral la ciberseguridad es conveniente identificar y reconocer los dominios sobre los que es necesario actuar y así tener una visión sistémica a la hora de proteger los activos de una organización. En la siguiente figura se identifican los principales dominios en el campo de la ciberseguridad (para ver otro enfoque, Jiang 2021). Con independencia de que se pueda estar de acuerdo o no con la ubicación de determinados dominios o con el nivel de detalle que reflejan, lo que sí es

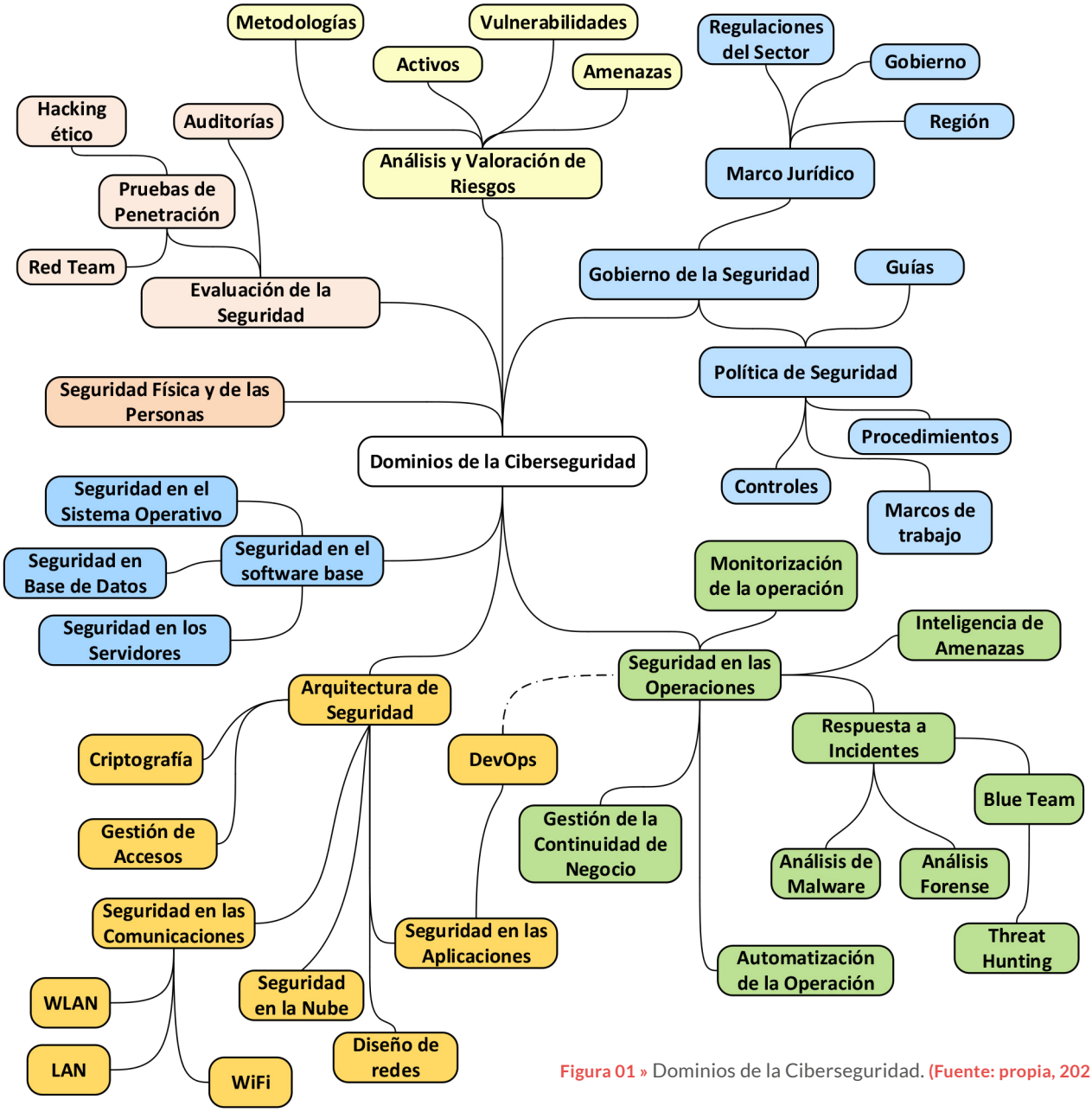


Figura 01 » Dominios de la Ciberseguridad. **(Fuente: propia, 2021)**

evidente es la necesidad de organizar la ciberseguridad teniendo en cuenta a todos ellos, con una visión sistémica y global de la misma para no dejar nada sin cubrir.

El dominio que se ocupara de la **seguridad de las operaciones** es el objetivo principal y para el que toda la organización debe trabajar, para proporcionar productos y servicios de una forma segura, bien sea una industria química, un banco o un hospital. Estamos ocupándonos con este dominio del entorno de producción de la empresa, y por tanto, además de monitorizar y vigilar los servicios o productos que se ofrecen, es importante empezar a recopilar, procesar y analizar información de inteligencia[1] para poder conocer cómo se llevan a cabo los ataques, o incluso reconocer algún patrón antes de que éstos se produzcan. Esta inteligencia de amenazas debe facilitar el camino a la caza de esas amenazas (threat hunting) que busca de forma proactiva anticiparse a las amenazas internas y externas a nuestra organización. A esto hay que unirle la monitorización de las operaciones mediante un sistema que permite la gestión de eventos y la información de seguridad (SIEM, Security Information and Event Management) con el objeto de bloquear las amenazas y en su caso neutralizarla y/o responder. Un SIEM se puede complementar con otros sistemas de respuesta, automatización y orquestación de la seguridad (SOAR, Security Orchestration, Automation and Response) que tiene su aplicación cuando los procesos están perfectamente establecidos y se necesita una respuesta automática y sin intervención humana, precisándose al humano para programarla con la información que les proporcionen los especialistas de seguridad del centro de operaciones. A estas capacidades anteriores hay que añadir la necesidad de definir planes de contingencia, para construir de una forma integral la gestión de la continuidad de negocio, así como los planes de recuperación y respuesta, incluyendo

1 » Entiéndase por información de inteligencia, aquella que se obtiene tras valorar, analizar, integrar e interpretar la información.

también los planes de retorno a la actividad después de un evento crítico. Es necesario destacar que hay sectores que cuentan con requisitos específicos en materia de continuidad de negocio, que hay que aplicar, como por ejemplo el sector aeroportuario que debe cumplir con los requisitos que le impone en esta materia la Organización de Aviación Civil Internacional, la Ley de Seguridad Aérea, o los planes de seguridad y de emergencia de cada aeropuerto.

Se ha incluido el concepto de **DevOps**, acrónimo procedente de las palabras desarrollo y operaciones, uniendo los dominios de la seguridad en las aplicaciones con la seguridad en las operaciones. La meta es mejorar la comunicación y la integración de ambos dominios con el objetivo de conseguir todo el beneficio posible de los enfoques que aporta el desarrollo de software moderno. Este enfoque genera versiones con nuevas características de una forma muy ágil, a la vez que permite aprender de la forma de usar el software por parte del usuario final, y de esta forma lo implica en el proceso de desarrollo de software con el objetivo de que no vea como un riesgo inabordable la subida a producción de las distintas versiones de software. Este concepto implica la utilización de herramientas de implementación, integración continua, monitorización y contenedores[2], por citar algunas.

A partir de las operaciones o negocio que se quiere llevar a cabo, se deben de comenzar a estudiar los riesgos, utilizando alguna de las metodologías existentes como MAGERIT[3] o CRAMM[4] por citar algunas, con el objetivo de identificar los activos de la organización, conocer las vulnerabilidades y así poder prevenir las amenazas. De alguna forma se trata de conocer si es aceptable el nivel de riesgos que asume la empresa u organización, que ayudará a tomar decisiones al dominio del Gobierno de la Seguridad.

Por tanto, el dominio que tiene que ver con la forma de **gobierno de la seguridad**, en primer lugar, pasa por identificar y aplicar el marco jurídico que debe tener en cuenta por parte del país, y/o región en la que realiza sus operaciones, junto con el marco regulatorio del sector en concreto en el que ejerce su actividad de producción, que no es el mismo para la banca que, para el sector de la alimentación, o el de la industria. En España, el RD 43/2021 es la principal norma en cuestiones de ciberseguridad y alinea el derecho español con el marco armonizado europeo conforme a la Directiva 2016/1148, más conocida como Directiva NIS[5]. En segundo lugar, le corresponde a este dominio definir las políticas de seguridad en la empresa, y para ello puede basarse en algún marco de trabajo de referencia (NIST[6], COBIT[7] o ISO 27000) para definir los controles críticos a establecer enlazándolos con las amenazas de seguridad, como por ejemplo las denominadas Amenazas Persistentes Avanzadas[8] (APT), así como los procedimientos y guías a seguir.

La **arquitectura de seguridad** es el dominio que da soporte al de seguridad en las operaciones. El entorno en el que actualmente se trabaja puede ser muy variado y complejo manteniendo distintas tipologías de medios, que van desde el centro de datos propio a usar entornos Cloud multiplataforma. Por ello, la Seguridad en las Comunicaciones, bien sea la conexión inalámbrica de los ordenadores con los que se trabaja en la organización, en una red de área local o en una red de área extendida, es necesario tenerla en cuenta y sabiendo que los datos pasan a través de dispositivos de red que en muchos casos se escapan de nuestro control. En cualquier caso, el diseño de la red y su segmentación, así como los distintos dispositivos como cortafuegos[9] (FW, firewall), los Sistemas de Prevención de Intrusiones (IPS, Intrusion Prevention System) o los Sistemas de Detección de Intrusos (IDS deben configurarse adecuadamente. Los IPS evitan los ataques cuando detectan software de tipo malicioso bloqueando las direcciones IP de los atacantes y avisan al personal de seguridad de posibles amenazas. Estos IPS complementan a los IDS (Intrusion Detection System) siendo éstos últimos los que detectan y analizan el tráfico de red buscando actividades anómalas. También es importante considerar los cortafuegos o firewall de aplicación web denominados WAF (Web Application Firewall), y que consisten en una solución hardware y software que se coloca entre las aplicaciones web y los usuarios. De alguna forma no podemos olvidar que muchos ataques se producen en distintos niveles de los protocolos de red, y esto implica sistemas de defensa diferentes para cada tipo de tráfico, siendo necesario que se analicen todas las conexiones http[10] por el WAF, complementándose, a su vez con el IPS que analiza otro tipo de tráfico más amplio.

Junto con la seguridad en las comunicaciones y todavía dentro del dominio de la arquitectura de seguridad, nos encontramos la seguridad en la nube (o cloud), que tiene por objetivo asegurar los sistemas informáticos en la nube,

2 » Los contenedores permiten compartir software y sus dependencias entre los entornos de producción y los de desarrollo. Ejemplo de éstos son Kubernetes y Docker.

3 » MAGERIT: Metodología de análisis de Riesgos de los Sistemas de Información.

4 » CRAMM: CCTA Risk Analysis and Management Method

5 » NIS es el acrónimo de Redes y Sistemas de Información

6 » NIST: National Institute of Standards and Technology. Marco de trabajo de Ciberseguridad emitido por este organismo de los Estados Unidos, para entender, gestionar y reducir los riesgos.

7 » COBIT: Acrónimo del inglés Control Objectives for Information and related Technology. es una guía de mejores prácticas presentada como framework, dirigida al control y supervisión de tecnología de la información (TI)

8 » APT: que son un tipo de amenazas que utilizan técnicas , como su nombre indica, avanzadas y sigilosas utilizando múltiples formas de ataque continuadas en el tiempo

9 » Un cortafuegos es un dispositivo de seguridad que permite bloquear accesos no autorizados. Puede ser una herramienta hardware o software.

10 » http es el protocolo de transferencia de hipertexto (Hypertext Transfer Protocolo, HTTP) que permite las transferencias de información a través de archivos con (con extensión html, shml, etc.) en la Web.

las aplicaciones que se ejecutan en esos sistemas informáticos, y los datos almacenados en la nube.

En cuanto a la seguridad en las aplicaciones, tenemos que entender cómo han evolucionado éstas, que empezaron siendo monolíticas[11], más tarde se optó por arquitecturas de tres capas (presentación, reglas de negocio y persistencia de datos), seguidas de las arquitecturas orientadas a servicios (SOA -Service-Oriented Architecture), a las que a su vez siguieron las arquitecturas dirigidas por eventos (EDA, Event-Drive Architecture), para continuar con las aplicaciones que se ejecutan en la nube, y finalizando por las arquitecturas de microservicios. Es importante destacar que la aparición de un modelo de arquitectura de aplicaciones, como los microservicios no implica la desaparición del SOA o la EDA, es decir, coexisten aplicaciones con distintas arquitecturas puesto que cada una de ellas es aplicable a casos de negocio con los que encaja perfectamente. Esto, además de aumentar la complejidad del sistema en producción, hace que no pueda mantener la seguridad aislada de los desarrolladores. Por otro lado, no podemos olvidar la gestión de accesos e identidades (IAM, Identity and Access Management), que tiene por objeto gestionar identidades de los distintos usuarios, además de registrar a los mismos junto con sus permisos de acceso, para poder autenticarlos, y auditarlos llegado el caso.

Otro aspecto por considerar en la arquitectura del sistema es la criptografía[12], teniendo en cuenta la robustez de los algoritmos de encriptación a utilizar, las técnicas de ocultación de la información, o la gestión de las claves dependiendo de la gestión de accesos que vayamos a realizar. También pude ser necesario contar con una infraestructura de clave pública (PKI, Public Key Infrastructure), para, poder ofrecer servicios de firma electrónica o de sellado de tiempo certificando que una actividad se hizo a una hora concreta.

Con el dominio que se ocupa de la **seguridad en el software base**, se identifican actividades que tienen que ver con eliminar vulnerabilidades de los sistemas operativos, los sistemas gestores de bases de datos, así como otros servidores imprescindibles para el funcionamiento de una empresa como puede ser el de correo, o aquellos que alojan aplicaciones específicas del negocio.

Otro dominio importante, es el que tiene que ver con la **seguridad física** de la empresa y de su Centro de Proceso de Datos (CPD), analizando e implementando controles y procedimientos de seguridad, como por ejemplo los relacionados con las copias de seguridad, teniendo en cuenta los puntos de vista internos y externos o de perímetro. De la misma forma, hay que aplicar conceptos y fundamentos de **seguridad de las personas** desde la óptica que proporcionan marcos de trabajo de referencia como el COBIT o la ISO 27000 con el objeto de reducir la amenaza interna intencionada o no, comenzando por procesos como el relacionado con las debidas comprobaciones (due diligence) a la hora de contratar personal para determinados puestos o establecer procedimientos de clasificación de la información asociados a las necesidades de conocer de distintas personas.

En definitiva, se tienen sistemas en producción, con un software base al que se han reducido las vulnerabilidades, al menos de las conocidas hasta ese momento, se ha definido una arquitectura de seguridad para el hardware incluyendo los sistemas de comunicaciones necesarios, se ha construido aplicaciones seguras siguiendo los modelos que indican las arquitecturas de seguridad software, se han establecido roles de usuario, procedimientos y controles. ¿Nos quedamos tranquilos? Quizás si se hiciera una **evaluación de la seguridad** de una forma metódica, mediante auditorías y/o o pruebas de penetración para poder estar seguro de que los riesgos que se asumen son aceptables y/o corregir aquellas deficiencias que puedan llegar a ser críticas, nos podríamos quedar más tranquilos.

Por último, hay un dominio que no aparece en la figura y que subyace en todos los dominios es el que tiene que ver con la formación, en su más amplio sentido, puesto que el talento en ciberseguridad es necesario y muy especializado. Para cubrir determinados puestos relacionados con la gestión de la ciberseguridad, es necesario contar con una visión global de todos los dominios, complementada con formación específica en algunos de ellos, y me refiero a puestos como el de CISO (Chief Information Security Officer), CSO (Chief Security Officer), CTO (Chief Technology Officer), DPO (Data Protection Officer) o el Arquitecto de Seguridad, a los que hay que añadir los administradores de seguridad, desarrolladores de aplicaciones seguras, expertos en criptoanálisis, consultores de seguridad, y un largo etcétera de puestos de trabajo que precisan de la definición de un itinerario para recibir una formación especializada en seguridad.

ATAQUES A LAS INFRAESTRUCTURAS CRÍTICAS

Las características de los ataques, como indica la Estrategia Nacional de Seguridad (2013) son las siguientes: bajo coste, ubicuidad y fácil ejecución, efectividad e impacto y reducido riesgo para el atacante. Esto hace que la cantidad de potenciales atacantes aumente los riesgos y amenazas que pueden poner en graves dificultades los servicios prestados por empresas y administraciones.

11 » Aplicación monolítica es aquella que combina en una sola aplicación la interfaz de usuario, las reglas de negocio y la capa de datos, constituyendo un único programa.

12 » Criptografía: Ciencia que desarrolla algoritmos y sistemas para cifrar la información con el objetivo de ocultarla.

Por otro lado, y centrándonos en los entornos industriales, denominados sistemas OT (Operation Technology), tal y como indica la Guía OT (Ministerio del Interior, 2021) hasta hace poco tiempo se tenía una falsa sensación de seguridad debido a la creencia de no existencia de riesgos, debido a cinco ideas preconcebidas:

- La planta está aislada, no está conectada a internet.
- Tenemos un firewall que nos protege.
- Los hackers no saben de sistemas/procesos industriales.
- Mi planta no es objetivo de nadie.
- Los sistemas de seguridad física de la planta nos protegen de los ciberataques.

El principal objetivo de los hackers son los entornos industriales, tales como sistemas de agua, plantas de energía, transporte, comunicaciones, en definitiva, cualquier tipo de infraestructura crítica. A ésto hay que sumar, que cada vez es más difícil mantenerse aislado. Los sistemas de automatización y control industrial (ICS, Industrial Control Systems) y los sistemas SCADA (Supervisor Control and Data Acquisition), están evolucionando de protocolos propietarios y cerrados, a protocolos de red abiertos para reducir costes en su programación y gestión, con las consecuencias que esto tiene desde el punto de vista de la seguridad. En cualquier caso, y aunque se consiga mantener el aislamiento, los dispositivos que se utilizan para configurar estos sistemas son ordenadores portátiles, pendrives, tabletas y smartphones, que han tenido contacto previo con internet o con otros ordenadores que pueden haber sufrido algún ataque o estar infectados con malware[13]. Por tanto, la única manera de mitigar el riesgo es siendo conscientes de las amenazas y vulnerabilidades y aplicando políticas de seguridad adecuadas.

El primer ataque a un sistema de producción de energía que cortó la electricidad a 225.000 mil personas durante unas ocho horas se produjo en Ucrania en diciembre de 2015 y fue realizado por grupo de hacktivistas[14] con un malware denominado BlackEnergy. Este ataque tuvo por objetivo, dañar los sistemas SCADA de tres empresas de distribución de electricidad y empezó con un ataque de phishing, es decir, mediante correos suplantando personas u organizaciones de confianza, lo que les permitió obtener las claves de acceso de algunos usuarios. Como se puede observar, y de acuerdo con Ahola (2019), el 95% de las brechas de ciberseguridad, la causa es debida al factor humano, bien sean errores sin intención como fallos al realizar una acción adecuada, o totalmente intencionados. Se puede ver un esquema de ataque en la fig. 02.

De acuerdo con Ginter (2019) de los 20 ciberataques principales a los sistemas de control industrial, el primero es el que denomina "empleados del ICS", y el segundo es "empleados de IT", es decir, en ambos casos técnicos y empleados de la empresa que facilitan el acceso a los hackers, a partir de las contraseñas que han obtenido espiando a sus compañeros. Este es un claro ejemplo de ciberataque que entra dentro del dominio de la seguridad física y de las personas denominado como amenaza interna (insider threat).

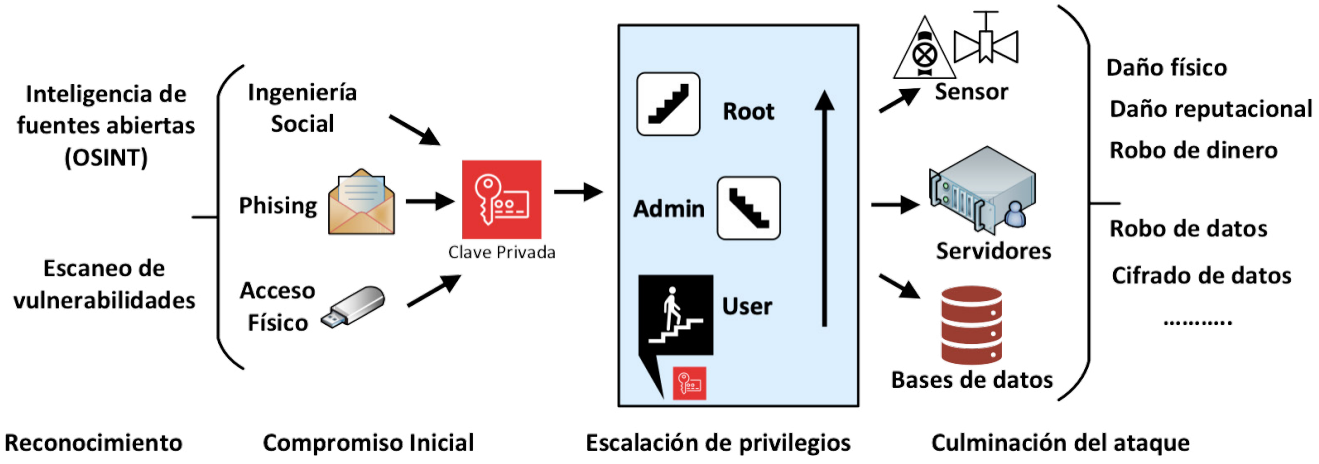
Otro ejemplo de ciberataque a una infraestructura crítica relacionada con la energía es el sufrido por Colonial Pipeline, la principal distribuidora de combustible de Estados Unidos, el 7 de mayo de este año, y que debido a un ataque de ransomware por un grupo de hackers denominado Dark Side tuvo que parar todas sus operaciones. El ransomware es un tipo de ataque que consiste la infección de los servidores por un software malicioso (malware) que encripta los datos y deja a los servidores bloqueados hasta que la víctima paga el rescate.

Con la pandemia, han aumentado de forma significativa los

13 » Software malicioso

14 » Engloba en un mismo término las palabras hacker y activista. Utilizan la tecnología para reivindicar posiciones políticas o sociales

Figura 02 » Fases y esquema del proceso de un ataque de ciberseguridad (Fuente: propia, 2021)



ataques a hospitales, infraestructura crítica vital durante esta situación provocada por el COVID-19. Como indica Harán (2021), el sector de la salud se ha convertido en un blanco perfecto para la extorsión mediante ransomware, ya que la interrupción del servicio tiene un impacto significativo en la salud de las personas, y esto provoca que se quiera resolver el ataque con urgencia favoreciendo en la negociación al cibercriminal. Uno de los primeros ataques de ransomware a hospitales se llevó a cabo en Reino Unido en 2017 mediante WannaCry infectando a 16 hospitales y centros de salud, desde entonces el crecimiento ha sido exponencial.

Tampoco se libra el sector público de los ataques, y no sucede sólo en España, que son el objetivo de los ataques más destructivos de sus infraestructuras digitales (Wirtz & Weyerer, 2017). El último ataque, en junio de 2021, se ha producido al Ministerio de Trabajo y Economía Social, tres meses después del que el Servicio Público de Empleo Estatal (SEPE), siendo este ataque un ransomware. Algunas fuentes indican que más de un 75% de las organizaciones del sector público ha sido víctimas de un ciberataque.

Estos incidentes además de seguir un patrón muy parecido en todos ellos, no se producen de un día para otro. Se producen incidentes previos menores que pasan desapercibidos por motivos que van desde la falta de concienciación, de conocimientos, de políticas de seguridad, o incluso de recursos humanos y técnicos. En la mayoría de los casos, los hackers llevan mucho tiempo dentro de la organización recabando información sobre la misma.

BUENAS PRÁCTICAS EN CIBERSEGURIDAD

Debemos tener en cuenta que el principal activo de nuestra organización es la información, la cual gestionamos por medio de una variedad de recursos tecnológicos. Por tanto, y siguiendo el orden establecido al explicar los dominios a considerar, se proponen las siguientes buenas prácticas:

1 » **Analizar los riesgos:** Para ello es necesario establecer un inventario de activos de la organización que recoja tanto el hardware como el software, así como la información y su soporte. A partir de aquí, se identificarán las distintas amenazas que les pueden afectar y ésto implica considerar tanto las amenazas internas como las externas, y dentro de éstas las que pueden ser intencionadas o accidentales. A la vista de esas amenazas, veremos que vulnerabilidades[15] de los activos pueden ser explotadas. Con todo ello, se identificará el riesgo, entendido como la estimación de que una amenaza se materialice sobre uno o mas activos causando daños o perjuicios a la Organización. Este riesgo lo reduciremos a través de salvaguardas o controles y medidas de seguridad.

15 » Entiéndase vulnerabilidad como cualquier debilidad en los activos que pueda ser explotada por una amenaza

2 » **Establecer un gobierno de la seguridad:** Los recursos tecnológicos deben estar alineados con el negocio de la organización, y para ello lo mas idóneo es establecer un marco de trabajo para el gobierno de las tecnologías de la información que nos permita diseñar la estrategia y la planificación de estas tecnologías teniendo en cuenta la seguridad de la información, gestionando los riesgos de una forma adecuada y controlando el éxito o fracaso de los proyectos de seguridad dentro de la organización. En definitiva, se trata de diseñar un sistema de gestión de seguridad de la Información (SGSI) alineado con el negocio.

3 » **Diseñar de forma integral la seguridad de las operaciones:** Identificar las operaciones necesarias para el negocio, su automatización y monitorización, la forma de responder a los incidentes y de recuperarse ante los desastres, como vamos a actualizar las aplicaciones (DevOps) y el software necesario (antivirus, sistema operativo, bases de datos, etc.), y sobre todo como vamos a garantizar la continuidad de negocio. Para esto último, el contar con copias de seguridad en otras ubicaciones seguras con control de acceso a las mismas es fundamental, además de realizar pruebas de restauración de estas copias de una forma periódica.

4 » **Definir la arquitectura de seguridad adecuada a las operaciones:** Diseñar la red, junto con los dispositivos de protección de perímetro necesarios, definir la gestión de accesos e identidades de acuerdo con las operaciones a realizar garantizando la seguridad de las comunicaciones.

5 » **Garantizar la seguridad del software base:** Estableciendo los procedimientos y mecanismos necesarios para mantener actualizados tanto los antivirus como los distintos servidores de aplicaciones, correo, web, sus sistemas operativos y sus sistemas gestores de bases de datos.

6 » **Controlar adecuadamente el acceso a los sistemas:** La seguridad física de los diferentes activos, tanto desde el exterior de las instalaciones como desde el interior de las mismas, teniendo en cuenta los objetivos de protección es de vital importancia. Además, saber cómo gestionar la seguridad de las personas como uno de los principales activos de una organización, su contratación, el cambio de puesto de trabajo o la extinción de los contratos, exige definir procedimientos adecuados.

7 » **Medir la seguridad de forma continua:** Se trata de evaluar permanentemente que los controles y los procedimientos funcionan de acuerdo con las necesidades de la organización y las operaciones que se llevan a cabo.

8 » **Formación y concienciación:** el dominar por parte de todos los usuarios las técnicas que nos pueden aplicar de ingeniería social, de phising, de errores comunes, y el contar con personal técnico cualificado para detectar y responder ante los incidentes es crucial.

CONCLUSIÓN

A la vista de los dominios, la superficie de ataque es muy amplia y cualquier empresa u organismo público es propensa de ser atacada, si no lo ha sido ya. Se observa un patrón muy similar en todos los ataques: se aprovechan las vulnerabilidades vía, amenaza interna, phishing o ingeniería social, se compromete una cuenta de usuario, se escalan privilegios para llegar a ser administrador, se consigue llegar a los servidores de producción una vez se ha explorado la red, se cifra la información relevante y se pide un rescate. Esto no sucede de un día para otro. En cualquier caso, cuando se producen estos ataques a la infraestructura crítica o el propio organismo que la gestiona, si es él el atacado, se sufren una serie de consecuencias relacionadas con el perjuicio que se produce a los ciudadanos por el servicio o producto que dejan de recibir, con los costes que hay que asumir para volver a la situación previa al incidente que pueden llegar a ser muy altos, y además tiene repercusión en la imagen del servicio público que se prestaba. En el caso de las empresas, un alto porcentaje de ellas llega a desaparecer.

No hay una receta mágica que resuelva estas situaciones, pero aplicar unas buenas prácticas combinadas con una visión global de la seguridad tratándola como un sistema que cubra todos los dominios, que gestione mejor sus datos, el contar con personal formado en ciberseguridad, y trabajar desde el gobierno de la seguridad con una visión estratégica muy bien definida y coherente con los servicios y productos que se tienen que salvaguardar, reducirá mucho las posibilidades de sufrir un incidente, y si éste se materializa, se contará con los medios técnicos y humanos con el talento suficiente para resolverlo adecuadamente.

REFERENCIAS BIBLIOGRÁFICAS

Ahola, M. (2019, October 18). ***The Role of Human Error in Successful Cyber Security Breaches.*** Recuperado de: https://blog.getusecure.com/post/the-role-of-human-error-in-successful-cyber-security-breaches. Último acceso el 5 junio de 2021.

BOE. (2011). Ley 8 / 2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas. Agencia Estatal Boletín Oficial Del Estado, 1(11), 1–11.

Craigen, D., Diakun-Thibault, N., & Purse, R. (2014). ***Defining cybersecurity. Technology Innovation Management Review.*** 4(10).

de España, G. (2013). ***Estrategia de ciberseguridad nacional.*** Recuperado de https://www.ccn-cert. cni. es/publico/dmpublido-cuments/EstrategiaNacionalCiberseguridad. pdf. último acceso el 6 de junio de 2021.

Ginter, A. (2019). ***The top 20 cyberattacks on Industrial Control Systems.*** Recuperado de: https://www.fireeye.com/content/dam/fireeye-www/products/pdfs/wp-top-20-cyberattacks.pdf. Último acceso el 5 de junio de 2021.

Harán J.M. (2020). ***Hospitales: Uno de los principales blancos de los ciberataques.*** Recuperado de: https://www.welivesecurity.com/la-es/2020/04/22/por-que-hospitales-blanco-atractivo-cibercriminales/. Último acceso el 15 de junio de 2021.

Jiang H. (2021). ***The Map of Cybersecurity Domains rev 3.0.*** Mapa de todos los dominios de la Ciberseguridad (derechodelared.com). Último acceso el 4 de junio de 2021.

Ministerio del Interior (2021). ***Guía sobre controles de seguridad en sistemas OT.*** Recuperado de https://www.ismsforum.es/ficheros/descargas/Gu%C3%ADa%20OT.pdf. Último acceso el 6 de junio de 2021.

Plėta, T., Tvaronavičienė, M., Della Casa, S., Agafonov, K. 2020. ***Cyber-attacks to critical energy infrastructure and management issues: overview of selected cases.*** Insights into Regional Development, 2(3), 703-715. https://doi.org/10.9770/IRD.2020.2.3(7).

Schatz, D., Bashroush, R., & Wall, J. (2017). ***Towards a more representative definition of cyber security.*** Journal of Digital Forensics, Security and Law, 12(2), 53-74.

Sols, Alberto. (2020). ***Industria 4.0: La cuarta revolución industrial*** en UEM STEAM Essentials.

Terrón Santos, D. (2019). Orden PCI/487/2019, de 26 de abril, por la que se publica la Estrategia Nacional de Ciberseguridad 2019, aprobada por el Consejo de Seguridad Nacional [BOE n. º 103, 30/IV/2019].

Wirtz, B. W., & Weyerer, J. C. (2017). ***Cyberterrorism and cyber attacks in the public sector: How public administration copes with digital threats.*** International Journal of Public Administration, 40(13), 1085-1100.

BIOGRAFÍA

Leopoldo Santos es Ingeniero Informático y actualmente está realizando el doctorado en la Universidad de Alcalá de Henares, desde el año 2017 dirige el Master Universitario en Seguridad de las TIC en la modalidad Online. Ha sido miembro como User Advisory Board de varios proyectos de investigación europeos FP-7 como "Alert for All" e "INDECT".

Como profesor asociado tiene más de doce años de experiencia en la Universidad Carlos III de Madrid y en la Universidad Europea de Madrid impartiendo distintas asignaturas. Es autor de varios artículos de investigación.

Ha sido Administrador de Sistemas durante tres años en OTAN donde recibió formación en distintas herramientas software y sistemas operativos. Ha participado durante más de quince años como Ingeniero de Sistemas y como Director Técnico de distintos sistemas de Comunicaciones y Mando y Control donde la seguridad es un aspecto de vital importancia.