CURSO *ONLINE* DE CIBERSEGURIDAD_

Unidad 2.
Aspectos básicos de ciberseguridad

GOBIERNO DE ESPAÑA
VICEPRESIDENCIA PRIMERA DEL GOBIERNO
MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL
SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL
incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD
017

Contenidos

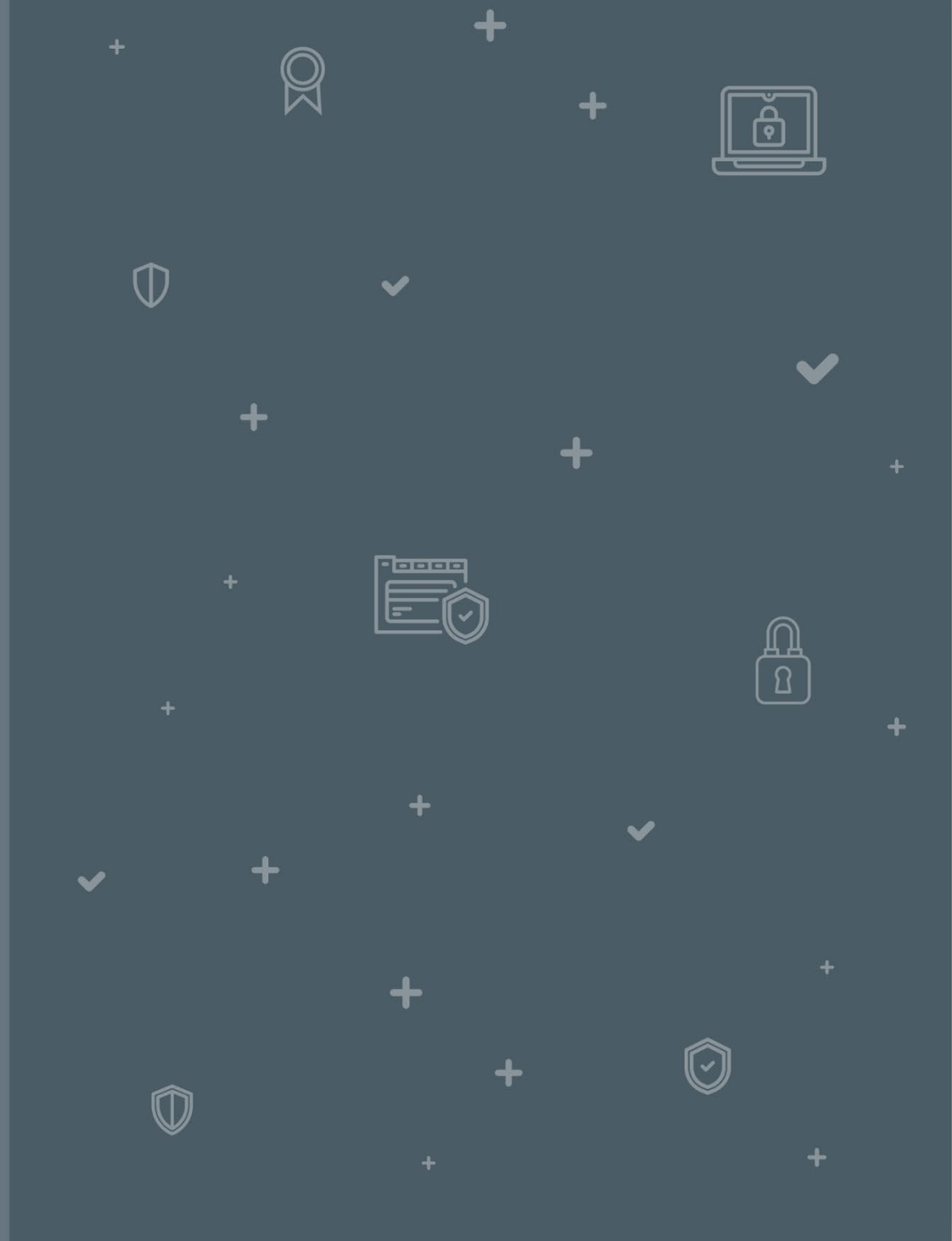
OBJETIVOS

Los principales objetivos de esta unidad son:

- Conocer los conceptos y las diferencias de seguridad de la información, seguridad informática y ciberseguridad; además de los principios básicos de seguridad de la información.
- Comprender los riesgos de los sistemas de información, cuáles son las amenazas más comunes a las que son susceptibles y qué medidas se puede tomar para protegerlos.
- Analizar los tipos de ciberdelincuentes que existen en la actualidad y conocer cuáles son los tipos de ataques más comunes.
- Introducir los conocimientos de la Industria 4.0 y el nacimiento de ciberseguridad industrial, además de entender los elementos principales que la componen. Descubrir las diferencias entre los entornos IT y OT, las principales causas y ataques al entorno OT y analizar qué medidas de seguridad se pueden tomar para proteger este entorno.
- Descubrir los métodos de protección más populares y efectivos para la seguridad de los equipos, activos y sistemas de información.

1

SEGURIDAD DE LA INFORMACIÓN, SEGURIDAD INFORMÁTICA Y CIBERSEGURIDAD



1 SEGURIDAD DE LA INFORMACIÓN, SEGURIDAD INFORMÁTICA Y CIBERSEGURIDAD

Introducción

En la unidad 1, analizamos el concepto de ciberseguridad, pero, para entenderlo correctamente, debemos comprender tres conceptos de seguridad que son claves en este término. Debemos también mencionar que, aunque estos términos puedan parecer sinónimos, tienen sus diferencias, aunque son muy sutiles y con frecuencia se utilizan para referirse a conceptos similares:

Seguridad de la información

Seguridad informática

Ciberseguridad

1 SEGURIDAD DE LA INFORMACIÓN, SEGURIDAD INFORMÁTICA Y CIBERSEGURIDAD

¿Qué es la seguridad de la información?

La «**seguridad de la información**» hace referencia al conjunto de políticas, procedimientos y medidas preventivas y reactivas que afectan a la seguridad del tratamiento de los datos en cualquier formato, ya sea electrónico, en papel, verbal, etc., y en cualquier etapa de su uso, recopilación, almacenamiento, procesamiento, trasmisión y borrado.

Si bien, este cuidado y preservación de la información no se lleva a cabo únicamente de forma técnica, sino que también se realiza a través de políticas y procedimientos que aseguren la confidencialidad, integridad, disponibilidad, autenticidad y no repudio de los sistemas de información.

1 SEGURIDAD DE LA INFORMACIÓN, SEGURIDAD INFORMÁTICA Y CIBERSEGURIDAD

¿Qué es la seguridad de la información?

Por ejemplo, el cifrado de los datos, la creación de copias de seguridad o *backups* o la renovación periódica de contraseñas, son algunas de las medidas de seguridad de la información.

¿Sabías qué?

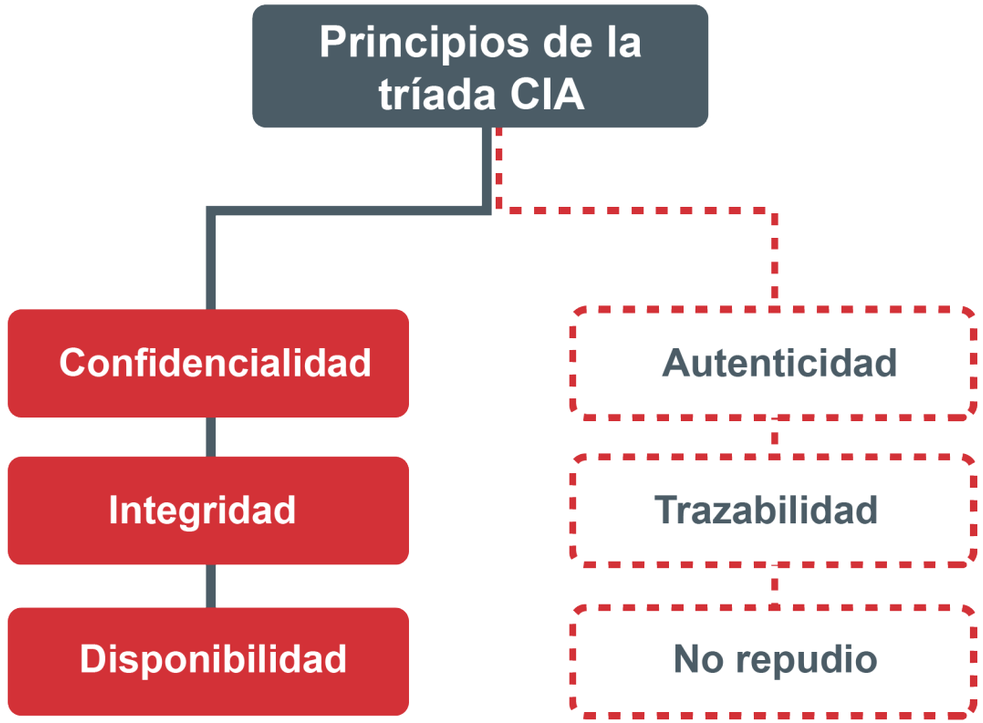
Una aseguradora sufrió un ciberataque *ransomware* en 2020 y, gracias a las medidas técnicas y organizativas de seguridad de las que disponía, el impacto fue prácticamente nulo, ya que los intentos de exfiltración de datos fueron detectados y evitados de forma eficaz. [1]

1 SEGURIDAD DE LA INFORMACIÓN, SEGURIDAD INFORMÁTICA Y CIBERSEGURIDAD

Principios básicos de la seguridad de la información

Como hemos mencionado, el objetivo de la seguridad de la información es tratar de mantener los datos y la información de una organización seguros y, para ello, se hace uso de la tríada CIA, que hace referencia a los tres principios clave en los que se basa la seguridad de la información, como la confidencialidad, la integridad y la disponibilidad.

Sin embargo, en los últimos años se han ido incorporando los principios de autenticidad, trazabilidad y no repudio, que han cobrado la misma importancia que la tríada CIA.



1 SEGURIDAD DE LA INFORMACIÓN, SEGURIDAD INFORMÁTICA Y CIBERSEGURIDAD

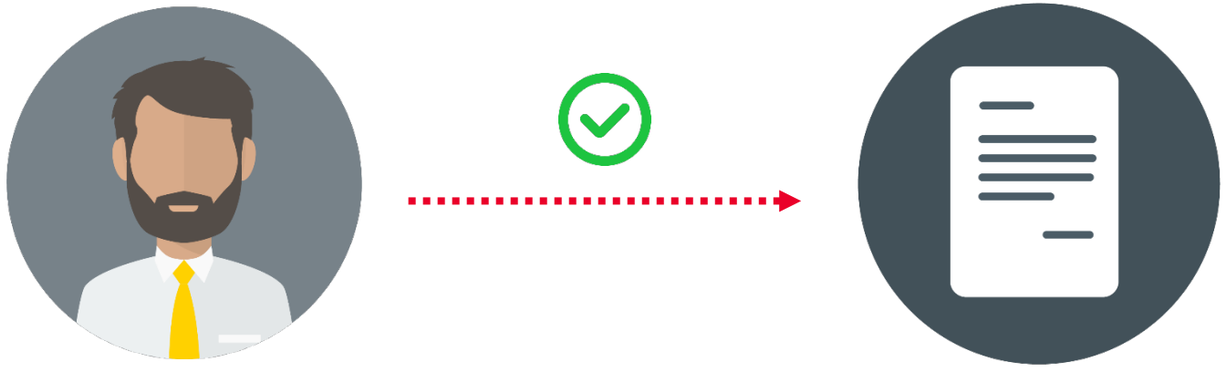
Principios básicos de la seguridad de la información

- **La confidencialidad:** solo los usuarios y procesos autorizados tienen acceso a los datos o la información y, por supuesto, hay que tener en cuenta que, aun cuando se disponga de acceso, esa información no se debe hacer disponible para otros usuarios o procesos. Por ejemplo, debemos establecer un control de acceso hacia la carpeta de información de un proyecto solo a las personas que gestionan un determinado cliente.
- **La integridad:** la información almacenada en un momento dado debe ser inmutable, es decir, nadie debe modificarla de forma incorrecta, ya sea por accidente o de manera maliciosa. Si alguien edita un documento, dicho cambio debe quedar reflejado mediante un registro de modificaciones del archivo.

1 SEGURIDAD DE LA INFORMACIÓN, SEGURIDAD INFORMÁTICA Y CIBERSEGURIDAD

Principios básicos de la seguridad de la información

- **La disponibilidad:** por disponible entendemos aquella información a la que podemos acceder cuando la necesitamos a través de los canales adecuados siguiendo los procesos correctos, es decir, se basa en asegurar que la información esté accesible a los usuarios o procesos que la requieran en el momento en el que la soliciten. Por ejemplo, una caída de los servidores provoca que este principio no se cumpla, ya que no podemos acceder a esa información o servicios.



1 SEGURIDAD DE LA INFORMACIÓN, SEGURIDAD INFORMÁTICA Y CIBERSEGURIDAD

Principios básicos de la seguridad de la información

Es necesario mencionar que, en los últimos años, otros aspectos han ido tomando relevancia en la seguridad de la información. Nos referimos a la autenticidad, la trazabilidad y el no repudio.

- **La autenticidad:** esta propiedad se basa en la garantía de la legitimidad del origen de la transmisión de la información, es decir, validar y verificar que el emisor de la información es quien dice ser. Esta característica está muy vinculada a la integridad, ya que hace referencia a la veracidad total del mensaje. Por ejemplo, en el caso de un correo electrónico, la autenticidad hace referencia a que el emisor de ese correo es verídico y es quien dice ser.

1 SEGURIDAD DE LA INFORMACIÓN, SEGURIDAD INFORMÁTICA Y CIBERSEGURIDAD

Principios básicos de la seguridad de la información

- **La trazabilidad:** esta capacidad permite rastrear un mensaje o contenido hasta su origen. La función principal es certificar que las acciones o información de una entidad u organización se pueden rastrear únicamente hasta esa entidad y ninguna otra. Actualmente, se utilizan los sellos de tiempo, los ID de transacción y los *logs* de eventos.
- **No repudio o la irrenunciabilidad:** esta característica es clave para demostrar la participación de las partes, es decir, garantiza al receptor de una comunicación que el mensaje fue originado por el emisor, además de prevenir que el emisor niegue el envío de esa comunicación. Esta capacidad está facilitada por la firma o el certificado digital.

1 SEGURIDAD DE LA INFORMACIÓN, SEGURIDAD INFORMÁTICA Y CIBERSEGURIDAD

¿Qué es la seguridad informática?

El término «**seguridad informática**» hace referencia a la disciplina que protege la integridad y la privacidad de la información que se almacena en el sistema informático u ordenador, de cualquier posible ataque o acceso no autorizado, a través de los cuales los cibercriminales pretenden obtener beneficios gracias a los datos confidenciales adquiridos.

Por lo tanto, la seguridad informática es la gestión de los riesgos relacionados con la información o los datos del sistema u ordenador, es decir, los riesgos que conlleva su uso, procesamiento, almacenamiento o transmisión, además de los sistemas y procesos que se emplean en el desempeño de estas actividades. La seguridad informática comprende una serie de medidas de seguridad, como, por ejemplo, antivirus, *firewall*, IDS, IPS, etc.

1 SEGURIDAD DE LA INFORMACIÓN, SEGURIDAD INFORMÁTICA Y CIBERSEGURIDAD

¿Qué es la seguridad informática?

Por ejemplo, con la **tecnología SIEM** (que se explicará en detalle en la especialidad de Administración de Sistemas de Ciberseguridad) podemos recopilar información, registrar y correlar *logs* para gestionar las diferentes actividades que hagan los sistemas y, de esta manera, detectar actividades sospechosas como conexiones a una IP maliciosa o que contenga contenido malicioso. Con este tipo de herramientas, centralizamos la información y detectamos las amenazas.

1 SEGURIDAD DE LA INFORMACIÓN, SEGURIDAD INFORMÁTICA Y CIBERSEGURIDAD

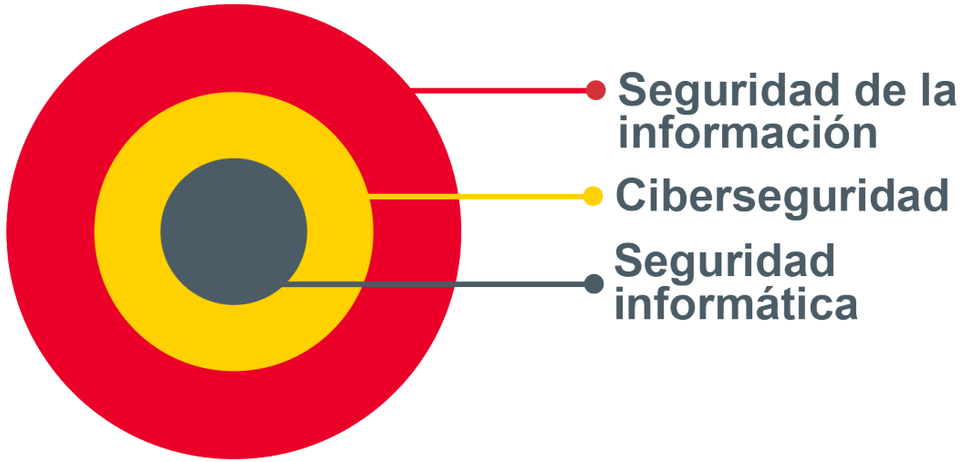
¿Qué es la ciberseguridad?

Como vimos en la unidad 1, la «**ciberseguridad**» es el conjunto de prácticas que tratan de proteger los ordenadores, los servidores, los dispositivos móviles, los sistemas electrónicos, las redes y los datos, de ataques maliciosos, es decir, tiene por objetivo proteger los sistemas y equipos y la información almacenada en ellos de cualquier ciberataque cuyo fin sea acceder, modificar o destruir la información confidencial, extorsionar a los usuarios o interrumpir la continuidad de un negocio.

1 SEGURIDAD DE LA INFORMACIÓN, SEGURIDAD INFORMÁTICA Y CIBERSEGURIDAD

¿Qué es la ciberseguridad?

Por lo tanto, aunque los términos «seguridad informática» y «ciberseguridad» se utilizan con frecuencia para referirse a lo mismo, la diferencia es muy sutil ya que, mientras la **seguridad informática** hace referencia a la protección de un único ordenador o sistema; la **ciberseguridad** protege a toda la infraestructura, sistemas, redes y ordenadores. Si bien no son definiciones cerradas, ya que sigue existiendo un debate sobre ellas, no obstante, estas son las más extendidas.



Fuente: *Diferencia entre Ciberseguridad, Seguridad Informática y Seguridad de la Información* [Gráfico] Elaborado a partir de https://www.lisainstitute.com

1 SEGURIDAD DE LA INFORMACIÓN, SEGURIDAD INFORMÁTICA Y CIBERSEGURIDAD

¿Qué es la ciberseguridad?

En las empresas u organizaciones, tanto las personas como los procesos y la tecnología deben complementarse para crear una defensa óptima y eficaz contra los posibles ciberataques u accesos no autorizados. Por ello, contamos con cinco funciones de operaciones de seguridad, que son claves para su éxito, como la concienciación, prevención, detección, investigación y corrección.

Funciones de operaciones de seguridad

- **Concienciación**
- **Prevención**
- **Detección**
- **Investigación y corrección**

1 SEGURIDAD DE LA INFORMACIÓN, SEGURIDAD INFORMÁTICA Y CIBERSEGURIDAD

¿Qué es la ciberseguridad?

- **Concienciación:** todo el personal de la empresa debería conocer los riesgos y las medidas de seguridad y actuar conforme a estas últimas. Por ejemplo, recibiendo formación en ciberseguridad y carteles informativos en la organización.
- **Prevención:** un factor clave es tomar medidas y estrategias que protejan los sistemas como tener el equipo actualizado con antivirus, parches, etc.
- **Detección:** una detección temprana comienza con un análisis y monitorización de los sistemas. Así, por ejemplo, al implantar un antivirus en nuestro equipo, podemos detectar y prevenir ataques.
- **Investigación y corrección:** al mismo tiempo que estudiamos el ataque o la intrusión para poder corregirlo, podemos tomar las medidas y acciones necesarias para su recuperación y así asegurar que no ocurra de nuevo. Así, generamos un historial de aprendizaje e implementar acciones de mejora.

1 SEGURIDAD DE LA INFORMACIÓN, SEGURIDAD INFORMÁTICA Y CIBERSEGURIDAD

Más conceptos básicos de ciberseguridad

Si quieres conocer más conceptos básicos del ámbito de la ciberseguridad, estas imágenes te dirigen a los glosarios más relevantes, donde podrás descubrir el significado de los términos clave y más utilizados en este campo.

incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

Enlace [2]

OSI Oficina de Seguridad del Internauta

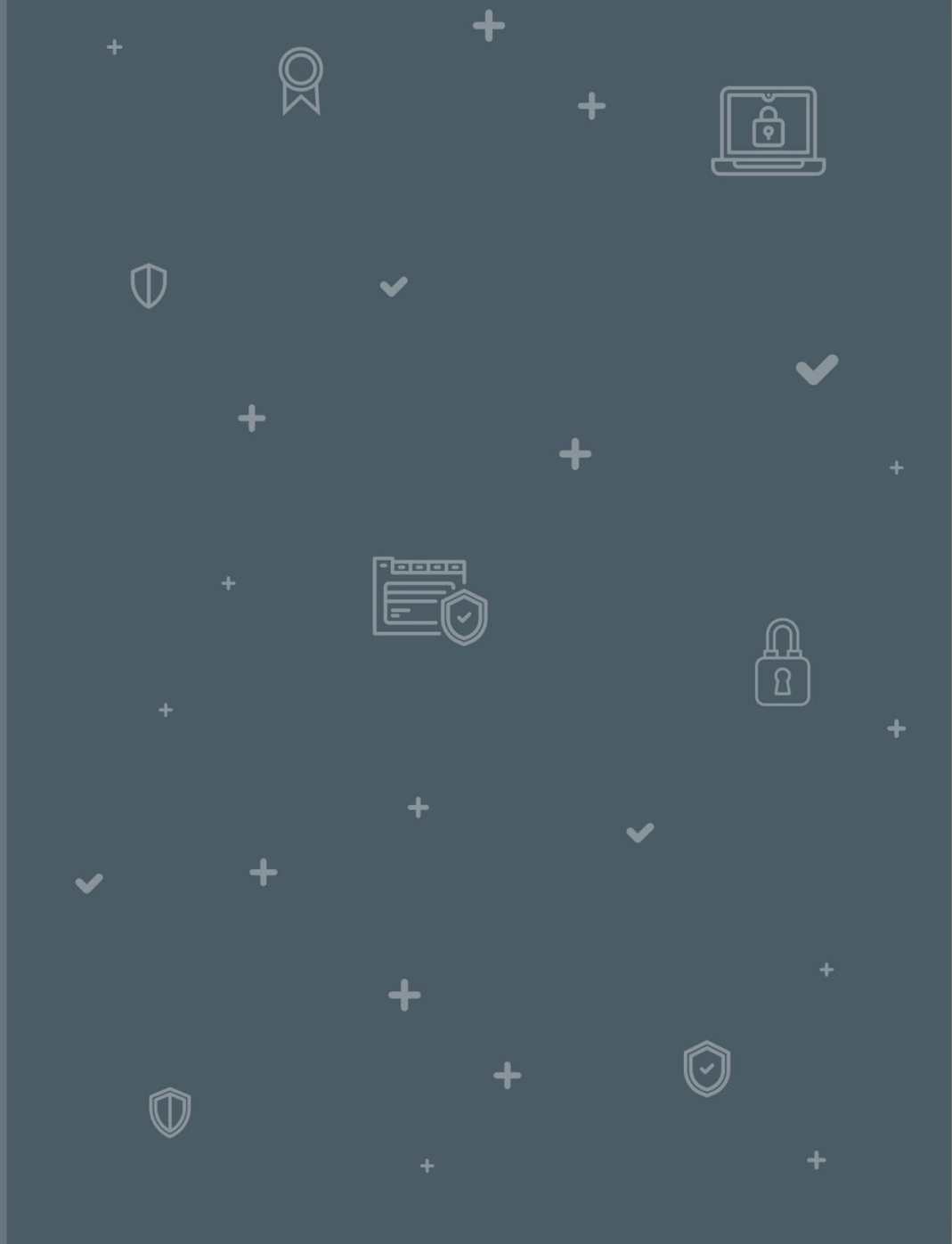
Enlace [3]

protege tu empresa

Enlace [4]

2

RIESGOS PARA LOS SISTEMAS DE INFORMACIÓN

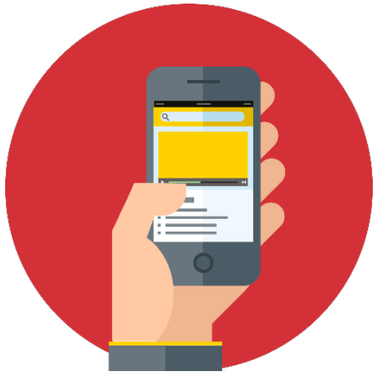


2 RIESGOS PARA LOS SISTEMAS DE INFORMACIÓN

Conceptos básicos

Para conocer los riesgos a los que son susceptibles los sistemas de información, debemos conocer primero cuáles son sus activos. Un **activo** es todo aquello que tenga valor para la empresa, siendo la información uno de los más valiosos y, aunque hoy en día una gran cantidad de la misma está en formato digital, haciéndola más accesible y manejable, también la hace más vulnerable.

Los **activos de información** también son todos aquellos recursos que se utilizan para generar, procesar, almacenar o transmitir la información, como las aplicaciones, ordenadores o dispositivos móviles, a parte del gran volumen de datos que generamos.



Así, los ejemplos más destacados son las bases de datos de nuestros clientes o proveedores, en el ámbito organizativo, o la agenda de contactos de nuestros dispositivos móviles o correo electrónico.

2 RIESGOS PARA LOS SISTEMAS DE INFORMACIÓN

Conceptos básicos

También es importante comprender el significado de los términos vulnerabilidad y amenaza y la diferencia que existe entre ellos:

- **Vulnerabilidad**: este concepto hace referencia a una debilidad o fallo en un activo. Por ejemplo, un fallo en el diseño o un error de configuración en un sistema o dispositivo.

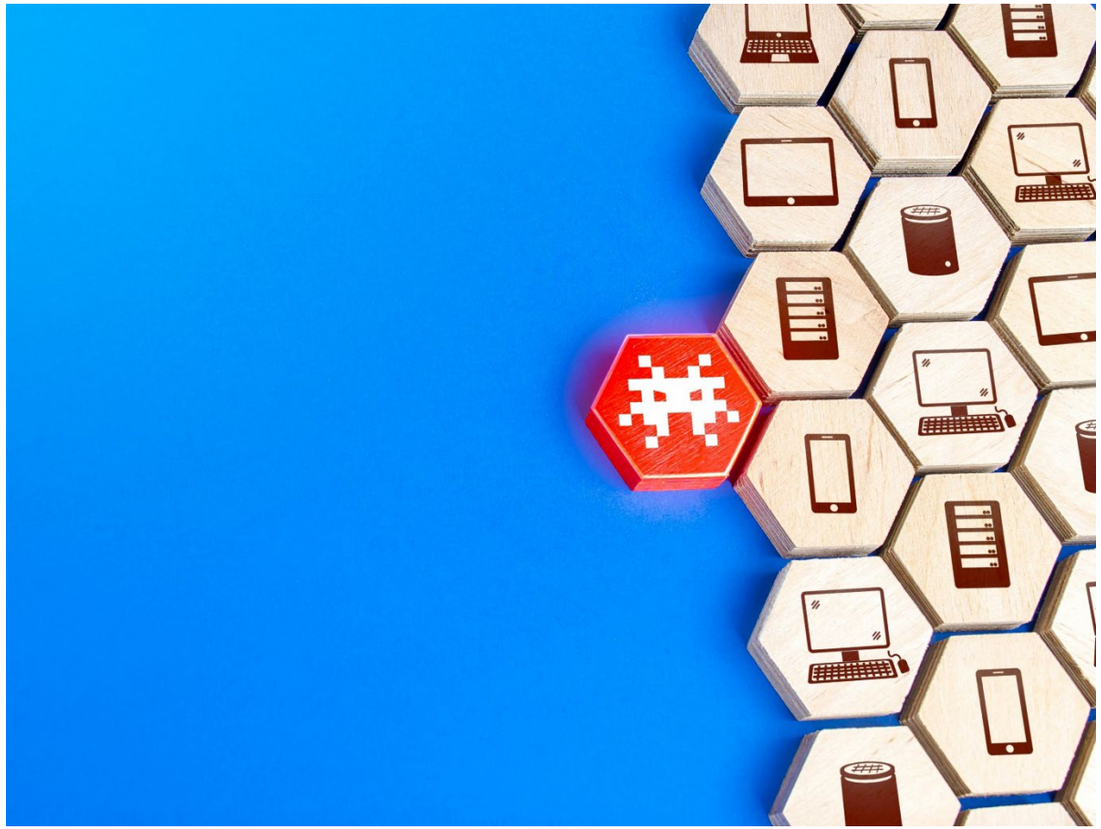
- **Amenaza:** circunstancia desfavorable que puede ocurrir y que cuando sucede tiene consecuencias negativas sobre los activos provocando su indisponibilidad, funcionamiento incorrecto o pérdida de valor. Las amenazas pueden proceder de ataques (como un virus), de sucesos físicos (como un incendio) o por negligencia (como un mal uso de las contraseñas).

La vulnerabilidad existe independientemente de que se explote o no, es decir, forma parte del activo, mientras que la amenaza es algo externo al activo.

2 RIESGOS PARA LOS SISTEMAS DE INFORMACIÓN

Conceptos básicos

Cuando una amenaza, aprovecha una debilidad o vulnerabilidad de un sistema de información, estamos ante un incidente de seguridad. Los incidentes de seguridad de la información implican la explotación de una o varias vulnerabilidades que afecten a alguno de los principios de ciberseguridad: confidencialidad, integridad y disponibilidad de los recursos de dicho sistema.

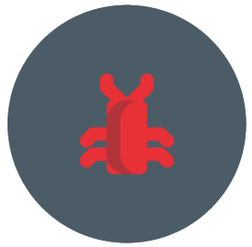


2 RIESGOS PARA LOS SISTEMAS DE INFORMACIÓN

Conceptos básicos

- **Confidencialidad**: si la explotación de la vulnerabilidad permite el acceso a información que no sea pública.
- **Integridad**: si la explotación de la vulnerabilidad permite alterar información que no esté configurada para ser modificada de dicha forma.
- **Disponibilidad**: si la explotación de la vulnerabilidad impide o dificulta el acceso a los recursos del sistema por parte de usuarios legítimos. Por ejemplo, el borrado de información o una denegación de servicio.

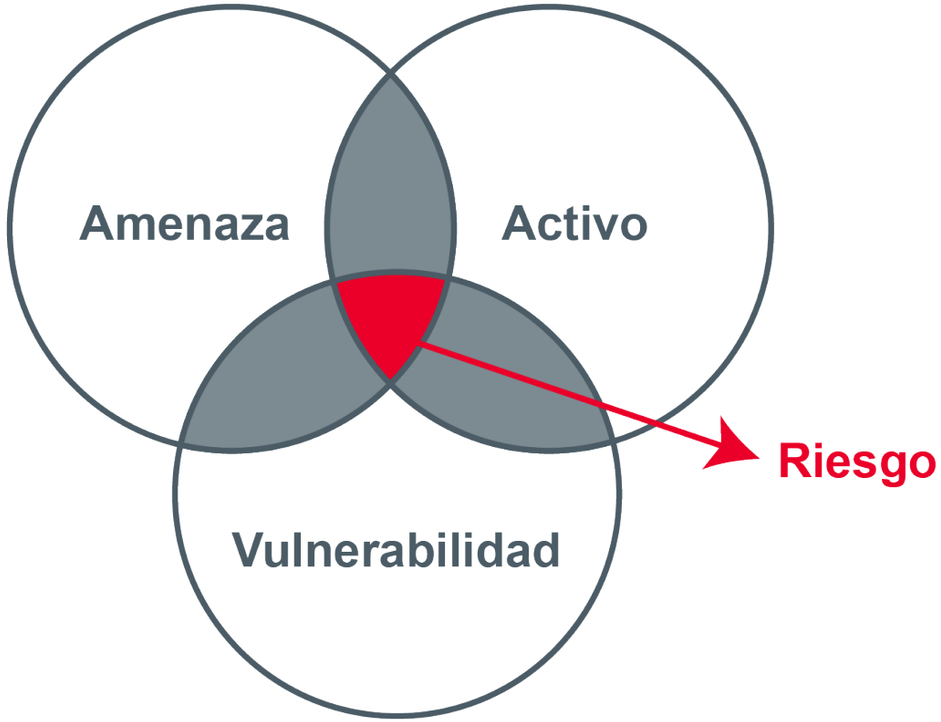
Un incidente puede afectar a varios principios de ciberseguridad simultáneamente, por ejemplo, un programa malicioso de tipo *ransomware* que cifra los archivos del ordenador afecta, tanto a la integridad como a la disponibilidad de la información.



2 RIESGOS PARA LOS SISTEMAS DE INFORMACIÓN

Conceptos básicos

Ahora vamos a conocer el concepto de riesgo. Un **riesgo** se define como la probabilidad de que se produzca un incidente de seguridad, materializándose una amenaza y causando pérdidas o daños. Este término suele considerarse como la combinación de la probabilidad de que se produzca un suceso y sus consecuencias.

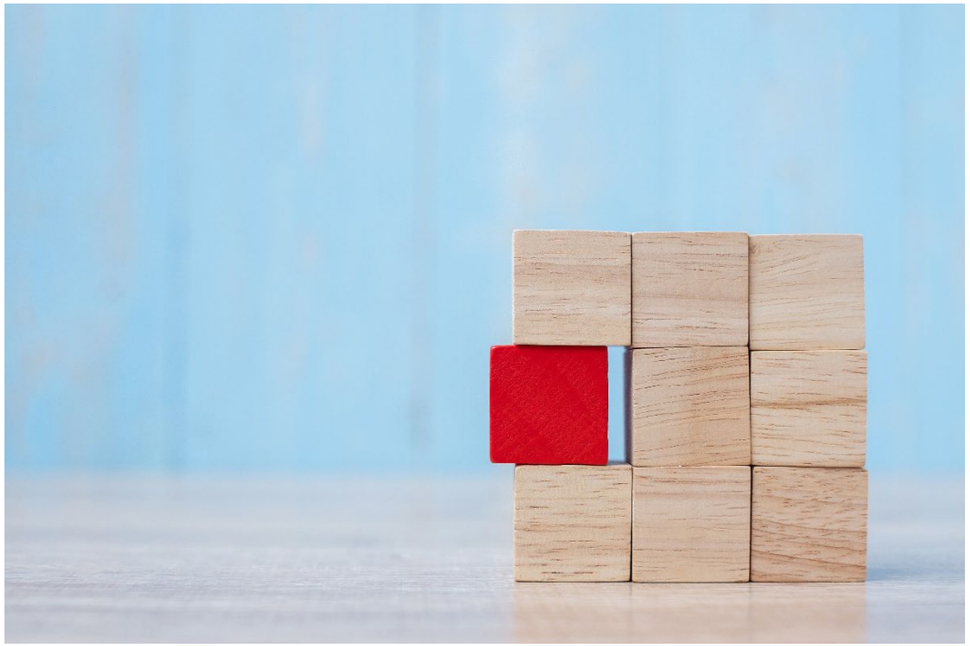


Fuente: *Amenaza vs Vulnerabilidad, ¿sabes en qué se diferencian?* [Gráfico] Extraído de https://www.incibe.es

2 RIESGOS PARA LOS SISTEMAS DE INFORMACIÓN

Conceptos básicos

- El **impacto** hace referencia a las consecuencias de la materialización de una amenaza sobre un activo aprovechando una vulnerabilidad. Se suele estimar en un porcentaje, donde el 100 % sería la pérdida total.
- La **probabilidad** es la posibilidad de que ocurra un hecho, suceso o acontecimiento.
- El **riesgo** se suele representar en forma de tabla como la que podemos ver en la siguiente diapositiva:



RIESGOS PARA LOS SISTEMAS DE INFORMACIÓN

Conceptos básicos

Riesgo dinámico (indicadores generales CVSS)	Probabilidad según el ciclo de vida de una vulnerabilidad			
	Raro	Poco probable	Probable	Muy alto
Bajo	Bajo	Bajo	Medio	Medio
Medio	Bajo	Medio	Medio	Alto
Alto	Medio	Medio	Alto	Muy alto
Muy alto	Medio	Alto	Muy alto	Muy alto

Fuente: *Valoración del riesgo dinámico de ciberseguridad* [Tabla] Extraído de https://www.tarlogic.com

RIESGO = PROBABILIDAD (de que se materialice una amenaza) **x IMPACTO**

2 RIESGOS PARA LOS SISTEMAS DE INFORMACIÓN

¿Qué riesgos existen?

Vamos a analizar los riesgos a los que están expuestos los activos y los sistemas de información:

- **Los ataques**: los ciberdelincuentes tienen como objetivo robar información, inutilizar los sistemas o usar los recursos existentes. Pueden ser externos o internos (como en el caso de un sabotaje).

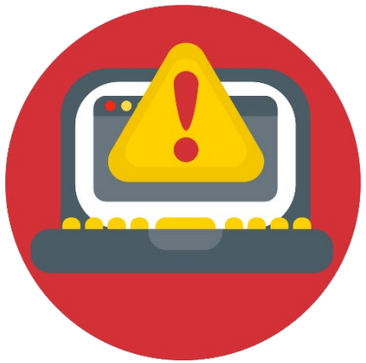
¿Sabías qué?
Una organización sufrió un ciberataque y los datos de más de 530 millones de cuentas de 108 países han sido publicados en Internet. [5]

- **Los errores humanos**: la intervención humana está en constante exposición a cometer errores, pudiendo provocar acciones que comprometan los datos o un mal funcionamiento de los sistemas. Por ejemplo, conectar un USB sin conocer su procedencia o si esconde contenido malicioso.

2 RIESGOS PARA LOS SISTEMAS DE INFORMACIÓN

¿Qué riesgos existen?

- **Los desastres naturales**: algunas situaciones pueden comprometer los equipos o sistemas, como es el caso de sufrir una inundación o un incendio. Por ejemplo, la erupción del volcán de la Palma dejó sepultados varios polígonos industriales bajo la lava, con la consecuente pérdida de infraestructuras, sistemas e información. [6]
- **Las situaciones extraordinarias**: ataques terroristas como el provocado en el 11-S en EE.UU. a las torres gemelas o los atentados del 11M de Madrid, las caídas o picos de tensión extremos, etc., que pueden suponer una amenaza a los sistemas de información.



2 RIESGOS PARA LOS SISTEMAS DE INFORMACIÓN

¿Qué amenazas y fuentes de amenazas existen?

Los activos y los sistemas de información son vulnerables a las amenazas. Así, las amenazas y fuentes de las mismas más comunes son:

- **El *malware***: este código malicioso permite a los atacantes realizar diferentes acciones como un ataque dirigido, es decir, hacia un objetivo específico, diseñado para atacar un componente específico de la Red, una configuración, etc.; o un ataque genérico, que no hace ese tipo de distinciones. **[7]**
- **La ingeniería social**: a través de técnicas de persuasión, los atacantes se aprovechan de la víctima y de su falta de concienciación en seguridad para obtener información y datos confidenciales. Suelen hacerse pasar por algún responsable o empresa conocida y legítima para ganarse la confianza de las víctimas y obtener así datos personales. Un ataque de *phishing* es un ejemplo de ingeniería social. **[8]**

2 RIESGOS PARA LOS SISTEMAS DE INFORMACIÓN

¿Qué amenazas y fuentes de amenazas existen?

- **Las Amenazas Persistentes Avanzadas o APT (*Advanced Persistent Threats*)**: estas amenazas hacen referencia a los ataques coordinados y dirigidos contra una empresa, con el objetivo de robar o filtrar información o datos sensibles. [9]

- **Las *botnets***: estas amenazas son redes de equipos infectados que ejecutan programas de forma automática y autónoma, es decir, sin el conocimiento ni el consentimiento del propietario del ordenador, donde el creador de la *botnet* puede controlarlos en remoto para realizar otro tipo de ataques más sofisticados. [10]

2 RIESGOS PARA LOS SISTEMAS DE INFORMACIÓN

¿Qué amenazas y fuentes de amenazas existen?

- **Las redes sociales y páginas web**: la falta de control de las redes sociales, las publicaciones en Internet o incluso un ataque a la página web propia de la organización puede poner en riesgo la reputación de una empresa.

¿Sabías qué?
Estas fueron las reacciones de las grandes empresas a sus crisis reputacionales. [11]

- **Los servicios en la nube**: otra de las fuentes de amenazas desde la que se puede producir un ataque son los servicios en la nube; por lo que se deben exigir a los proveedores los mismos criterios de seguridad que se tiene en los sistemas de una organización. Por ejemplo, si la compañía tiene unos criterios específicos de acceso a ciertos servicios o información, este mismo acceso en la nube tiene que ser igual o más restrictivo.

2 RIESGOS PARA LOS SISTEMAS DE INFORMACIÓN

¿Qué medidas podemos implementar?

Los incidentes de seguridad que pueden surgir en una organización pueden implicar diversos problemas, ya sean pérdida de información, sanciones económicas o daños a la imagen y reputación de la empresa, entre otros; por lo que resulta esencial conocer qué riesgos existen y evaluarlos para poder tomar las medidas de seguridad adecuadas.

El primer paso será conocer el nivel de riesgo de nuestra organización. Este proceso de detección se puede realizar a través de un **análisis de riesgos,** que se compone de seis fases:

Fase 1 **Fase 2** **Fase 3** **Fase 4** **Fase 5** **Fase 6**

RIESGOS PARA LOS SISTEMAS DE INFORMACIÓN

¿Qué medidas podemos implementar?

Fase 1

Definir el alcance del análisis de riesgos, es decir, dónde vamos a analizar los riesgos. Pueden ser todos los servicios, departamentos y actividades o centrarse en algunos en concreto.

Fase 2

Identificar y valorar los activos de información del departamento, proceso o sistema objeto del estudio.

Fase 3

Identificar las **amenazas** a las que están expuestos estos activos.

2 RIESGOS PARA LOS SISTEMAS DE INFORMACIÓN

¿Qué medidas podemos implementar?

Fase 4

Estudiar y analizar las características de nuestros activos para identificar **los puntos débiles o vulnerabilidades y las salvaguardas existentes.**

Fase 5

Para cada par activo-amenaza, estimar la **probabilidad** de que la amenaza se materialice y el **impacto** sobre el negocio que esto produciría.

Fase 6

Una vez calculado el riesgo, **tratar aquellos riesgos que superen un límite** que nosotros mismos hayamos establecido.

2 RIESGOS PARA LOS SISTEMAS DE INFORMACIÓN

¿Qué medidas podemos implementar?

El análisis de riesgos nos ayudará a conocer la importancia y la gravedad que supondría la materialización de una amenaza y, así, poder gestionar los riesgos de forma adecuada.

El primer paso será definir un umbral de riesgo, lo que se conoce como apetito de riesgo, para determinar qué riesgos son asumibles y cuáles no. Una vez que tengamos esto definido, las posibles acciones a seguir para cada riesgo identificado son:

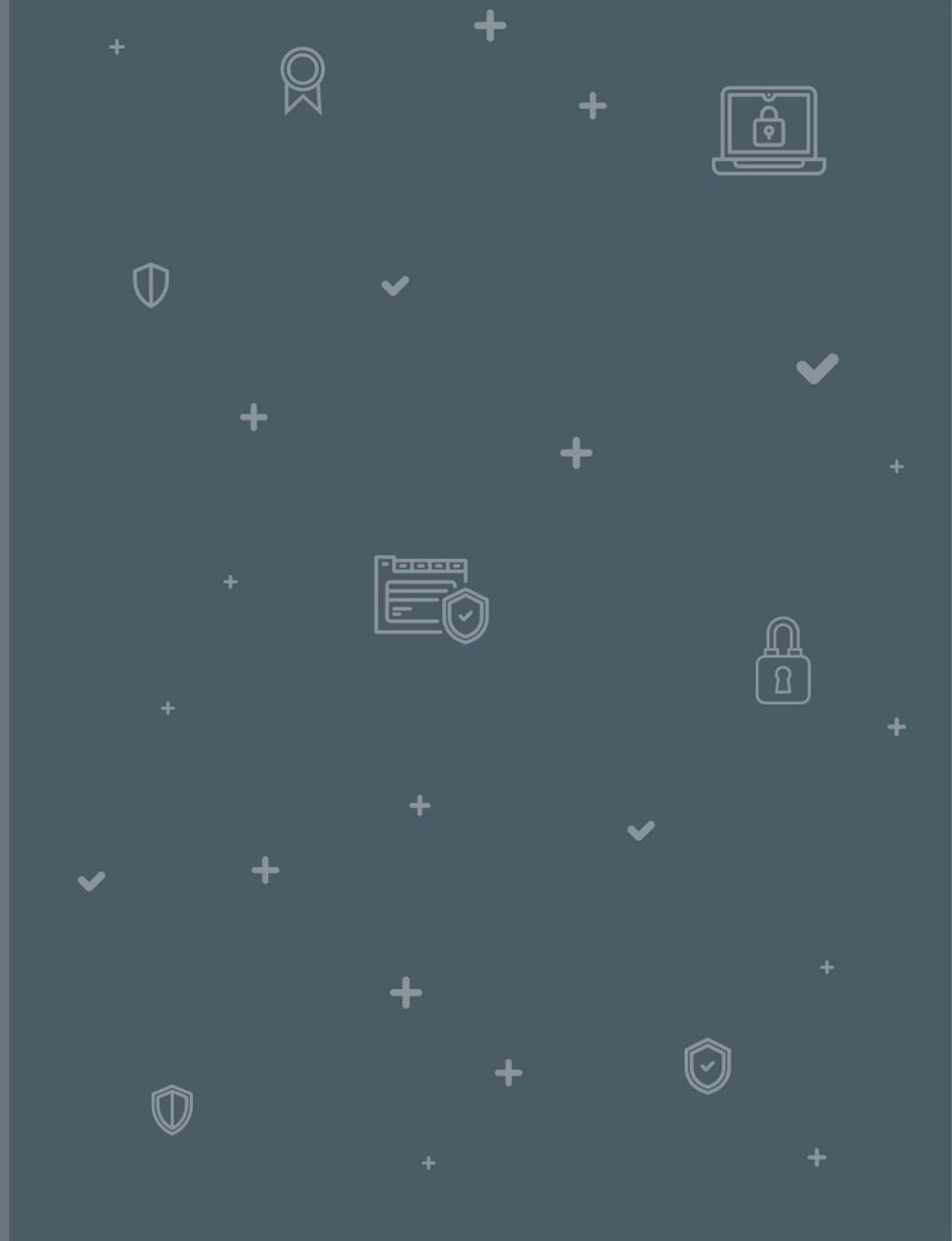
- **Evitar el riesgo**, eliminando la causa que lo provoca.
- **Mitigar el impacto o la probabilidad del riesgo**, adoptando las medidas necesarias. Por ejemplo, la instalación de un sistema antincendios en la sala de los servidores puede reducir el impacto.
- **Transferir el riesgo a un tercero**, por ejemplo, a través de contratos de seguros.
- **Aceptar la existencia del riesgo y monitorizarlo**.

¿Sabías qué?

El sector sanitario es uno de los más vulnerables a la hora de asegurar la privacidad de los datos de sus pacientes. [12]

3

TIPOS DE CIBERDELINCUENTES Y ATAQUES MÁS COMUNES



3 TIPOS DE CIBERDELINCUENTES Y ATAQUES MÁS COMUNES

¿Qué es un ciberdelincuente?

Primero debemos comprender la diferencia entre *hacker* y ciberdelincuente.

- ***Hacker***: es aquella persona que trata de solventar, paliar o informar sobre los problemas de seguridad encontrados en programas, servicios, plataformas o herramientas. La RAE lo define como «*aquella persona con grandes habilidades en el manejo de equipos que investiga un sistema informático para avisar de los fallos y desarrollar técnicas de mejora*».
- **Ciberdelincuente**: es la persona que buscará sacar beneficio de estos problemas o fallos de seguridad utilizando para ello distintas técnicas como es la ingeniería social o el malware. La RAE aporta también el término de «pirata informático», siendo este la «*persona que accede ilegalmente a sistemas informáticos ajenos para apropiárselos u obtener información secreta*». Muchas veces también encontramos que a los ciberdelincuentes se les denomina cibercriminales, por la traducción del inglés «*cybercriminal*».

3 TIPOS DE CIBERDELINCUENTES Y ATAQUES MÁS COMUNES

¿Qué es un ciberdelincuente?

¿Sabías qué?

A raíz de la pandemia COVID-19 y del aumento del uso de códigos QR, en detrimento del uso de documentos en papel para reducir el riesgo de contagio, los ciberdelincuentes han aprovechado esta tecnología para llevar a cabo fraudes y robos de datos. [13]

3 TIPOS DE CIBERDELINCUENTES Y ATAQUES MÁS COMUNES

Tipos de ciberdelincuentes

Tras conocer el significado de *hacker* y de ciberdelincuente, ahora vamos a entender que este puede tener diferentes motivaciones u objetivos. Los *hackers* se dedican a detectar problemas o brechas del sistema, mientras que los ciberdelincuentes tienen como objetivo lucrarse o realizar algún tipo de reivindicación. Por ello, existen diferentes tipos, siendo los *White Hat*, los *Black Hat* y los *Grey Hat* los principales, y el resto subtipos de ellos:

3 TIPOS DE CIBERDELINCUENTES Y ATAQUES MÁS COMUNES

Tipos de ciberdelincuentes

White Hat: este tipo hace referencia a aquellos *hackers* éticos que trabajan protegiendo los sistemas, investigando y buscando las brechas de seguridad existentes.

Black Hat: a estos ciberdelincuentes también se les conoce bajo el nombre de *crackers,* ya que utilizan sus habilidades informáticas para irrumpir en los sistemas de seguridad, infectar las redes, suplantar identidades, etc., es decir, cometen actos ilícitos y con ellos obtienen un beneficio personal que, en la mayoría de los casos, es lucrativo.

Grey Hat: este tipo es una mezcla de *White Hat* y *Black Hat*, pudiendo posicionarse en cualquiera de ellos. Estos ciberdelincuentes son capaces de infiltrarse ilegalmente en los sistemas informáticos, pero lo hacen siguiendo su propia ética. También se dedican a obtener información de gran relevancia de forma ilegal para hacerla llegar a la opinión pública.

3 TIPOS DE CIBERDELINCUENTES Y ATAQUES MÁS COMUNES

Tipos de ciberdelincuentes

Blue Hat: vengadores: son un subtipo de *Black Hat*. A este tipo de ciberdelincuentes no les importa necesariamente el dinero o la fama, si no que realizan ciberataques para vengarse personalmente de una persona, empleador, institución o gobierno. Hacen uso de *malware* y despliegan ataques en los servidores/redes de sus enemigos para causar daños.

Hacktivista: son un subtipo de *Grey Hat*. Se trata de un ciberdelincuente que utiliza la tecnología y sus conocimientos acerca de ella para su activismo, es decir, para atacar los sistemas con fines políticos, ideológicos o éticos.

El famoso grupo Anonymous es un ejemplo de *hacktivista*.

3 TIPOS DE CIBERDELINCUENTES Y ATAQUES MÁS COMUNES

Tipos de ciberdelincuentes

¿Sabías qué?

El término *hacktivismo* surge de la unión de la palabra «*hacker*» y «activismo», y hace referencia a la realización de actos maliciosos, en Internet, con el fin de promover ideas políticas, religiosas, sociales, ideológicas o éticas. Además, existe un subtipo de *hacker*, llamado *Green Hat* o «*newbies*», que hace referencia a los ciberdelincuentes novatos, es decir, aquellos que no tienen habilidades técnicas, pero utilizan las herramientas maliciosas para causar daños, por mera curiosidad o para beneficiarse de los ciberataques, sin tener ningún conocimiento sobre cómo hacerlo. [14]

3 TIPOS DE CIBERDELINCUENTES Y ATAQUES MÁS COMUNES

Conceptos básicos

A continuación, vamos a comprender los términos de ciberdelito y ciberataque:

- «**Ciberdelito**» **o delito informático** es un concepto que hace referencia a la actividad ilícita que se realiza a través de Internet o mediante el uso de herramientas tecnológicas, ya sean ordenadores, teléfonos móviles, etc.
- El término «**ciberataque**» hace referencia a aquellas acciones que están dirigidas contra los sistemas de información digitales, con la finalidad y objetivo de perjudicar a personas, instituciones u organizaciones, robar información u obtener un beneficio económico. La palabra «ciberataque» viene de la fusión de los conceptos «ataque» y «cibernético». Así, un ciberataque puede realizarse contra los equipos y sistemas de la Red, ya sea anulando sus servicios o impidiendo su acceso o, por ejemplo, contra las bases de datos que almacenan información sensible, espiándola, robándola o utilizándola para la extorsión de los usuarios y/o de la organización.

3 TIPOS DE CIBERDELINCUENTES Y ATAQUES MÁS COMUNES

Los ciberataques actuales

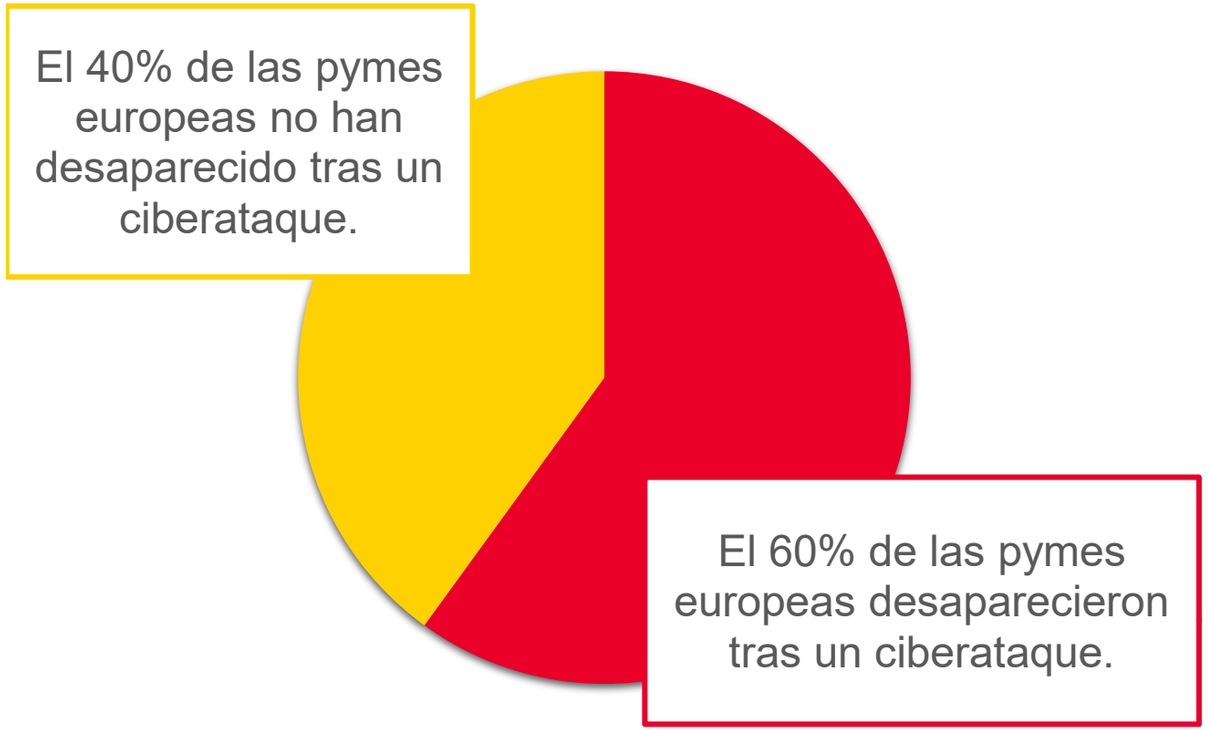
En la actualidad, las organizaciones criminales cada vez abogan más por los ataques cibernéticos, dada su gran rentabilidad y su difícil rastreo.

La principal diferencia entre estos conceptos reside en que los ciberdelitos no siempre persiguen un beneficio económico, como es el caso, por ejemplo, del acoso a través de la Red; y, sin embargo, para su realización se utilizan dispositivos tecnológicos, aunque no se requieren conocimientos técnicos avanzados. Por otro lado, en los ciberataques sí se requieren de conocimientos informáticos avanzados para que estos puedan ser ejecutados.

3 TIPOS DE CIBERDELINCUENTES Y ATAQUES MÁS COMUNES

Los ciberataques actuales

El 60% de las pymes europeas que son víctimas de ciberataques desaparece en los seis meses siguientes al incidente, muchas veces lastradas por el coste medio del ataque, que suele ser aproximadamente 35.000 euros.



Informe: Panorama actual de la Ciberseguridad en España.

3 TIPOS DE CIBERDELINCUENTES Y ATAQUES MÁS COMUNES

El ciclo de vida de un ciberataque

Aunque cada vez es mayor el número de empresas que toman las medidas necesarias para prevenir, protegerse y reaccionar ante cualquier incidente de seguridad, hay ocasiones en las que estas medidas previas no son suficientes para detener un ciberataque desconocido. Por ello, es necesario comprender cuál es el ciclo de vida de un ciberataque, para poder anticiparse a él y tomar las medidas y acciones necesarias que garanticen una mayor seguridad y protección de los activos.

Al ciclo de vida de un ciberataque también se le conoce como «*Cyber Kill Chain*», y está formado por siete fases que veremos a continuación.

Veamos cómo se desarrolla cada fase a través de un ejemplo de ataque de *phishing*.

Fuente: *Las 7 fases de un ciberataque. ¿Las conoces?* [Gráfico] Elaborado a partir de https://www.incibe.es

TIPOS DE CIBERDELINCUENTES Y ATAQUES MÁS COMUNES

El ciclo de vida de un ciberataque

Fase 1: reconocimiento

En esta fase, el ciberdelincuente recopila toda la información posible de su objetivo o víctima, ya sea sobre la tecnología que utiliza, como datos e información que pueda obtener publicada en la Red. Así, el atacante valorará los métodos de ataque que podrían funcionar y la probabilidad de éxito de los mismos. Dos métodos muy utilizados para la recopilación de información son las técnicas de ***footprinting*** y ***fingerprinting***:

- ***Footprinting***: este concepto hace referencia a la recopilación de información a través de canales de acceso público, generalmente, como buscadores de Internet.
- ***Fingerprinting***: se trata de una técnica intrusiva en la que los atacantes buscan, de manera activa, los puertos y servicios que pudieran estar a la escucha (abiertos), con el objetivo de encontrar vulnerabilidades que explotar.

3 TIPOS DE CIBERDELINCUENTES Y ATAQUES MÁS COMUNES

El ciclo de vida de un ciberataque

Fase 1: reconocimiento

Por ejemplo, los atacantes podrían recabar información acerca de la organización a la que van a realizar el ataque de *phishing,* ya sea a través de las **publicaciones** encontradas en Internet tanto en su página web como en redes sociales, al igual que en noticias de diversos medios sobre la organización. El atacante intentará deducir posibles **puntos débiles**, por ejemplo, si es una empresa que gestiona muchas facturas, podrá intentar generar un ataque de *phishing* incluyendo un *malware* en un archivo adjunto que simule ser una factura.

Las **medidas** que se pueden llevar a cabo para proteger la organización de un posible ciberataque, en esta primera fase, son:

- Restringir la información ofrecida en Internet de la empresa.
- Realizar un análisis completo de los posibles vectores de ataque.

3 TIPOS DE CIBERDELINCUENTES Y ATAQUES MÁS COMUNES

El ciclo de vida de un ciberataque

Fase 2: preparación

Esta fase hace referencia a la preparación específica del ataque sobre un **objetivo**, que puede ser **genérico**, es decir, aquel donde no importa quién sea la víctima; o **focalizado**, esto es, busca atacar a alguien en concreto, un componente, dispositivo o configuración de la Red específicos, como puede ser un ataque de *phishing,* donde se logra obtener la dirección de correo de la víctima, siendo un tipo de *phishing* denominado *spear phishing.* Sin embargo, se podría realizar un ataque de *phishing* genérico, donde los ciberdelincuentes se inventan direcciones de correo para comprobar así direcciones existentes en la organización.

Esta fase se centra en establecer o **determinar el rango de objetivo**, qué **alcance** tendrá el ataque, qué **herramientas** se utilizarán para realizarlo, incluso concretar **la hora y fecha** de realización del ataque, es decir, el ciberdelincuente prepara minuciosa y detalladamente el ataque.

TIPOS DE CIBERDELINCUENTES Y ATAQUES MÁS COMUNES

El ciclo de vida de un ciberataque

Fase 2: preparación

Siguiendo con el ejemplo de un ataque *phishing*, la fase de preparación consistiría en elaborar un **correo electrónico** o, si en el ataque se quiere redirigir a las víctimas a una **página falsa**, en este momento también se generaría dicha página. También se establecería la hora y la fecha a la que se lanzará el ataque y el alcance del mismo, por ejemplo, si se lanzará a toda una organización, a qué sector determinado, etc.

Como **estrategia de defensa** en esta fase, se recomienda contrastar los archivos sospechosos con algún escáner de *malware*, por ejemplo, se puede emplear herramientas de análisis como VirusTotal o urlscan.io que analizan un fichero contra gran cantidad de motores antivirus, lo que facilita la detección de posibles ataques.

TIPOS DE CIBERDELINCUENTES Y ATAQUES MÁS COMUNES

El ciclo de vida de un ciberataque

Fase 3: distribución

En esta fase se ejecuta la transmisión del ataque, es decir, el ciberdelincuente establece el medio para realizar su ataque **en base a la información recopilada** en las fases previas, pudiendo utilizar, por ejemplo, una memoria USB o un correo electrónico, siendo en estos casos la acción del usuario necesaria para que se lleve a cabo el ataque; o **explotando una vulnerabilidad** del ordenador en la que el usuario no interviene para que dicho ataque se lleve a cabo.

El éxito de esta fase dependerá de la información recogida en la fase de reconocimiento de la víctima y del nivel de preparación que tenga el atacante.

TIPOS DE CIBERDELINCUENTES Y ATAQUES MÁS COMUNES

El ciclo de vida de un ciberataque

Fase 3: distribución

Así, en esta fase, el atacante distribuiría la campaña de *phishing* a través del correo electrónico a los **usuarios** u **organizaciones** que haya seleccionado en el alcance de la fase de preparación anterior.

En este caso, la mejor **estrategia de defensa** sería la monitorización constante por parte de la organización, permitiendo así el descubrimiento o detección de los posibles ataques y, como en la fase anterior, permitiendo su análisis para conocer los efectos que el ataque tendría sobre los sistemas o dispositivos de la organización.

TIPOS DE CIBERDELINCUENTES Y ATAQUES MÁS COMUNES

El ciclo de vida de un ciberataque

Fase 4: explotación

En esta fase se explota el ataque y, en función del objetivo que se haya fijado el atacante, quedará **comprometido** el equipo infectado, la Red a la que pertenece o expuesta información confidencial. Para tener éxito se deberá explotar alguna vulnerabilidad a través de un ***exploit*** ya existente o creando uno nuevo.

Teniendo como referencia el ejemplo anterior, si un usuario que haya recibido un ataque de *phishing* a través del correo electrónico sigue y realiza las indicaciones del correo, facilitará información confidencial al atacante. Otro caso podría ser que en el correo electrónico hubiera un archivo adjunto, aparentemente legítimo pero que, al descargarlo, dicho archivo contenga un *malware* que aproveche una vulnerabilidad del sistema.

TIPOS DE CIBERDELINCUENTES Y ATAQUES MÁS COMUNES

El ciclo de vida de un ciberataque

Fase 4: explotación

Como **estrategia de defensa**, las organizaciones deben centrarse en vectores de ataque abiertos, es decir, en los métodos o entradas o vulnerabilidades que los ciberdelincuentes puedan utilizar para realizar el ataque. Un método muy eficaz es realizar pruebas de penetración (*pentesting*), ya que permiten descubrir posibles vulnerabilidades y tomar medidas de protección, reduciendo o suprimiendo así el riesgo de que un atacante las explote. También, aunque es aplicable a todas las fases, la formación y concienciación de los empleados es crucial para que los trabajadores sepan cómo actuar en caso de que detecten algo sospechoso o se produzca un incidente.

El ciclo de vida de un ciberataque

Fase 5: instalación

En esta fase, si bien no se produce en todos los casos, está pensada para que los atacantes puedan acceder de forma **persistente** a los ordenadores. Por ello, suelen instalar puertas traseras o integran el ordenador víctima una ***botnet***, por ejemplo.

El ciberdelincuente puede decidir instalar el *malware* en la víctima objetivo, ejecutar un *script* que cargue un *payload* malicioso en el sistema, robar credenciales, etc.

Un ***script*** es una secuencia de comandos, fragmentos de código con el objetivo de realizar o añadir funciones dentro de un dispositivo o servicio. Un ***payload*** es la parte del código del *malware* que realiza la acción maliciosa en el sistema, mientras que el ***exploit***, es la parte encargada de aprovechar una vulnerabilidad que permita ejecutar el *payload*.

TIPOS DE CIBERDELINCUENTES Y ATAQUES MÁS COMUNES

El ciclo de vida de un ciberataque

Fase 5: instalación

Por ejemplo, si el ataque de *phishing* tiene adjunto un archivo malicioso que instala un ***malware***, esta fase sí se producirá; sin embargo, si lo que encontramos es un enlace a una página fraudulenta para obtener información confidencial o nuestras credenciales personales, no se produce instalación alguna y esta fase no existiría.

En este caso, las **medidas de protección o defensa** consisten en impedir que el atacante pueda realizar estas acciones de instalación. Por ello, es importante disponer de soluciones de seguridad y mantener los sistemas actualizados, en especial los antivirus.

TIPOS DE CIBERDELINCUENTES Y ATAQUES MÁS COMUNES

El ciclo de vida de un ciberataque

Fase 6: comando y control

En esta fase, el atacante adquiere el **control del sistema o del equipo de la víctima**, en el que podrá realizar o lanzar **acciones maliciosas**, como robar información confidencial, extraer datos de acceso, instalar programas, conocer la Red del usuario, etc.

Siguiendo con el ejemplo del *phishing*, en caso de que la víctima se hubiera descargado un **archivo malicioso** de dicho correo electrónico, el atacante, en función de cómo esté configurado el *malware*, podría realizar acciones como obtener el control del equipo de la víctima, **robar información confidencial**, instalar programas o lanzar ataques contra otros equipos. Asimismo, si el *phishing* redirigiese a una página fraudulenta, en esta fase el atacante accedería a la página falsa para ver cuánta gente ha facilitado su información confidencial.

3 TIPOS DE CIBERDELINCUENTES Y ATAQUES MÁS COMUNES

El ciclo de vida de un ciberataque

Fase 6: comando y control

Como **estrategia de defensa**, a partir del análisis de los vectores de ataque que se ha realizado anteriormente, se pueden tomar y establecer las medidas necesarias y adecuadas para proteger a los sistemas y equipos. Por ejemplo, se pueden cerrar todos los puertos que no sean necesarios, establecer medidas más restrictivas en la configuración de los *firewalls*, etc.

TIPOS DE CIBERDELINCUENTES Y ATAQUES MÁS COMUNES

El ciclo de vida de un ciberataque

Fase 7: acciones sobre los objetivos

En esta última fase, el ciberdelincuente trata de cumplir el **objetivo** de su ataque, ya sea **espionaje, sabotaje, robo de datos, realizar nuevos ataques, etc.** También cabe la posibilidad de que el ciberdelincuente trate de expandir sus acciones hacia más objetivos, en cuyo caso suele hacerlo hacia el exterior, es decir, hacia los clientes, proveedores y/o colaboradores de la organización.

Por ejemplo, si con el ataque de *phishing* se han recopilado **datos de acceso** a los bancos de las víctimas del ataque, en esta fase, el atacante accedería a esos bancos y vaciaría las cuentas bancarias de las víctimas, gracias a los datos de acceso robados.

3 TIPOS DE CIBERDELINCUENTES Y ATAQUES MÁS COMUNES

El ciclo de vida de un ciberataque

Fase 7: acciones sobre los objetivos

Por ello, es importante tomar las **medidas** adecuadas para lograr romper la cadena y evitar que un ciberataque provoque daños más graves o incluso alcance más objetivos. Establecer y definir claramente las responsabilidades y funciones de los empleados, así como los procesos técnicos y los análisis que deben llevarse a cabo, son algunas de las medidas a tomar para evitar daños graves.

3 TIPOS DE CIBERDELINCUENTES Y ATAQUES MÁS COMUNES

Tipos de ataques

Es importante comprender que no existen dos ciberataques exactamente iguales, aunque es cierto que se pueden desarrollar estrategias y tácticas similares que se utilizan de forma habitual, dada la eficacia que han reportado a lo largo del tiempo. Veamos los tipos de ataques más comunes:

Inserción de código malicioso	Ataques por ingeniería social	Ataques a las conexiones	Ataques a contraseñas	Otros
Malware	*Phishing*	MitM	Fuerza bruta	Ataques de día cero o *0-day*
Ransomware	*Vishing*	DoS	Diccionario	
	Smishing	DDoS		
		EDoS		
		Inyección SQL		
		XSS		

Saber más

Tipos de ataques: Guía de ciberataques OSI. [15]

Fuente: *Guía de ciberataques* [Gráfico]
Elaborado a partir de https://www.osi.es

3 TIPOS DE CIBERDELINCUENTES Y ATAQUES MÁS COMUNES

Ataques por inserción de código malicioso: *malware*

El término «***malware***» proviene de la fusión de las palabras «*malicious*» y «*software*», que en castellano hacen referencia a «**código malicioso o dañino**»; aunque en numerosas ocasiones se utilizan los conceptos «*malware*» y «virus» como sinónimos, un virus es un tipo de *malware*.

Este ciberataque hace referencia a diferentes formas de *software* malicioso diseñado para **infiltrarse en un dispositivo** sin el conocimiento, ni el consentimiento del usuario. Es capaz de dañar el equipo o dispositivo, robar información confidencial, o emplear el equipo para realizar otro tipo de acciones, como hacer que forme parte de una *botnet.*

En el caso del *ransomware*, que veremos más adelante, destaca que, aunque sí se daña el dispositivo, es posible recuperar su uso después de pagar el rescate. Y mientras que el resto del *malware* está destinado a ser invisible y silencioso, el *ransomware* se hace visible al usuario cuando exige un pago del rescate.

3 TIPOS DE CIBERDELINCUENTES Y ATAQUES MÁS COMUNES

Ataques por inserción de código malicioso: *malware*

Este tipo de ciberataques también pueden ser **lucrativos**, pudiendo obtener dinero de diferentes formas:

- **Directamente del usuario infectado:** ya sea **robando información confidencial** del usuario como sus credenciales bancarias o recibiendo el dinero directamente del usuario si paga un **rescate**, como en el caso de un *ransomware* o bajo chantaje por la difusión de fotos privadas, por ejemplo.
- **Convirtiendo al usuario infectado en un *cesor* del dispositivo** y desde él realizar otras **acciones delictivas**, como el envío de correos electrónicos maliciosos o realización de ataques de Denegación Distribuida de Servicio (DDoS); o realizar acciones lucrativas como minar criptomonedas.

3 TIPOS DE CIBERDELINCUENTES Y ATAQUES MÁS COMUNES

Instalación de *malware*

Aunque existen diversos métodos para introducir este ciberataque en un sistema suele ser necesario que el usuario realice alguna acción para que el *malware* se instale. Una de las formas más habituales para que se instale este programa malicioso se produce cuando un usuario **hace clic en un enlace o en un archivo adjunto** en un correo electrónico. Por su parte, el *malware* para instalarse suele aprovechar alguna **vulnerabilidad** del sistema, por este motivo es tan importante tener todo el *software* del ordenador debidamente actualizado.

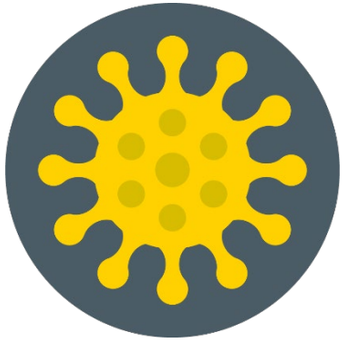
¿Sabías qué?

Spyware Darkhotel era red de espionaje que utilizaba la red wifi de los hoteles para acceder a los dispositivos de las víctimas y acceder a datos e información confidenciales. [16]

3 TIPOS DE CIBERDELINCUENTES Y ATAQUES MÁS COMUNES

Tipos de *malware*

Tradicionalmente, el *malware* se ha clasificado en los siguientes tipos, atendiendo a su **propagación**:



Virus informático

Gusano informático

Troyano

3 TIPOS DE CIBERDELINCUENTES Y ATAQUES MÁS COMUNES

Tipos de *malware*

- **Virus informático**: fueron los primeros en surgir. Su código malicioso estaba incrustado en un archivo legítimo y generalmente buscaban en el ordenador otros archivos del mismo tipo y los infectaban, actuando de forma similar a los virus biológicos, de ahí su nombre. Tiene como objetivo alterar el correcto funcionamiento del dispositivo. Para ello, necesita de la acción o intervención del usuario, que debe abrir el fichero infectado y, en el momento en que lo hace, el virus puede replicarse y conseguir así realizar sus acciones maliciosas. En los orígenes de la informática (con el MS-DOS), había pocos programas y pocos archivos, de tal manera que la existencia de algún archivo adicional podía resultar sospechosa y la mejor forma de introducir un programa malicioso en un equipo era modificando alguno de los ficheros ya existentes. Hoy en día, los programas tienen una gran cantidad de archivos y programar un virus es técnicamente muy complejo, por lo que ya no existen, en detrimento de los otros dos tipos de *malware* que vamos a explicar, gusanos y troyanos.

3 TIPOS DE CIBERDELINCUENTES Y ATAQUES MÁS COMUNES

Tipos de *malware*

- **Gusano informático**: este tipo de *malware* no requiere de la intervención del usuario y es capaz de replicarse a sí mismo para **enviar copias a otros dispositivos** conectados al primero o que estén en su lista de contactos. Se suele utilizar para la creación de *botnets*, es decir, unas redes de ordenadores *zombies* que pueden actuar de manera simultánea.
- **Troyano**: este *malware* se encuentra dentro de un programa legítimo o aparentemente legítimo para introducirse en el equipo como el «caballo de Troya», aludiendo a su nombre. Un troyano suele tratar de pasar inadvertido en el sistema para realizar acciones ocultas, como **abrir una puerta trasera o robar información**. Sin embargo, este tipo de *malware* no se replica a sí mismo, como los virus o gusanos.

3 TIPOS DE CIBERDELINCUENTES Y ATAQUES MÁS COMUNES

Acciones *malware*

Hoy en día, el *malware* se clasifica más en función de las acciones maliciosas que realiza, siendo las más habituales las siguientes:

Spyware

Adware

3 TIPOS DE CIBERDELINCUENTES Y ATAQUES MÁS COMUNES

Acciones *malware*

- ***Spyware***: trabaja de forma oculta **recolectando información** de la víctima. Este tipo de ataque se instala en el equipo sin necesidad de intervención del usuario o mediante la interacción de una segunda aplicación o programa que lo lanza sin que el usuario sea consciente. Esta palabra es el resultado de la fusión de las palabras inglesas «*spy*» (en castellano, espiar) y «*malware*».
- ***Adware***: este tipo de *malware* no siempre es dañino para el equipo, sin embargo, sí es molesto ya que su objetivo es introducirse en el ordenador para **mostrar publicidad al usuario**, ya sea mientras navega por Internet o de forma aleatoria como una alerta que salta durante la ejecución de un programa. Su término proviene de la fusión de las palabras inglesas «*ad*» (en castellano, anuncio) y «*malware*» y, por lo general, se instala en el ordenador a la par que otras aplicaciones.

3 TIPOS DE CIBERDELINCUENTES Y ATAQUES MÁS COMUNES

Ataques por inserción de código malicioso: *ransomware*

Se trata de un tipo de *malware* que está especializado en infectar un equipo o red y **cifra los archivos que encuentra o bloquea la posibilidad de usar libremente el sistema infectado**. Por lo general, el ciberdelincuente cifra los archivos de los dispositivos y exige un pago para que la víctima obtenga la clave y así poder descifrarlos. Este tipo de ataque es el más popular hoy en día para los PC.

El ejemplo más famoso de *ransomware* es el de WannaCry. En 2017, más de 230.000 ordenadores fueron afectados en 150 países. Los cibercriminales aprovecharon una vulnerabilidad en el sistema operativo Microsoft Windows, conocida como *EternalBlue*, consiguiendo así cifrar los archivos de los dispositivos y pedir un rescate por ellos. Se estimó que este ataque provocó pérdidas de alrededor de 4.000 millones de dólares en todo el mundo.

3 TIPOS DE CIBERDELINCUENTES Y ATAQUES MÁS COMUNES

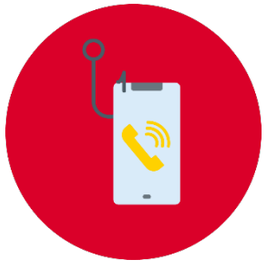
Ataques por ingeniería social: *phishing*, *vishing* y *smishing*

Se trata de tres ataques basados en la ingeniería social que, aunque son muy similares entre sí, cada uno de ellos tiene sus propias características. Generalmente, el atacante envía un mensaje suplantando la identidad de alguna entidad o persona legítima, que nos genere confianza, y así lograr su objetivo. A continuación, vamos a conocer cada uno de ellos:

- ***Phishing***: este ciberataque suele hacer uso del **correo electrónico**, las **redes sociales** o las **aplicaciones de mensajería instantánea.** Aunque suele estar asociado al robo de credenciales bancarias este no es el único caso, por ejemplo, en 2020, se produjo una campaña de *phishing* que suplantaba a una empresa de mensajería, en la que se mencionaba que no se había podido producir la entrega de un paquete y que el usuario debía reprogramar la entrega previo pago.

3 TIPOS DE CIBERDELINCUENTES Y ATAQUES MÁS COMUNES

Ataques por ingeniería social: *phishing*, *vishing* y *smishing*



- ***Vishing***: este ataque, generalmente, se produce a través de llamadas de teléfono. Uno de los tipos de *vishing* más conocidos son los ***scams*** (en castellano, timos), por ejemplo, los de asistencia técnica, donde el atacante llama por teléfono simulando pertenecer a una empresa conocida y ofreciendo un soporte técnico, informando de que se ha producido un ciberataque y que el usuario debe realizar una serie de pasos, como, por ejemplo, descargar un programa, acceder a un portal que en realidad es fraudulento, etc., y conseguir así datos o accesos no autorizados.

- ***Smishing***: el modo de actuación de este ciberataque es través de SMS.

¿Sabías qué?

Han aumentado los ataques de *smishing* en los últimos años en los que las víctimas recibían un SMS simulando la entrega de un paquete. [17]

3 TIPOS DE CIBERDELINCUENTES Y ATAQUES MÁS COMUNES

Ataques por ingeniería social: *phishing*, *vishing* y *smishing*

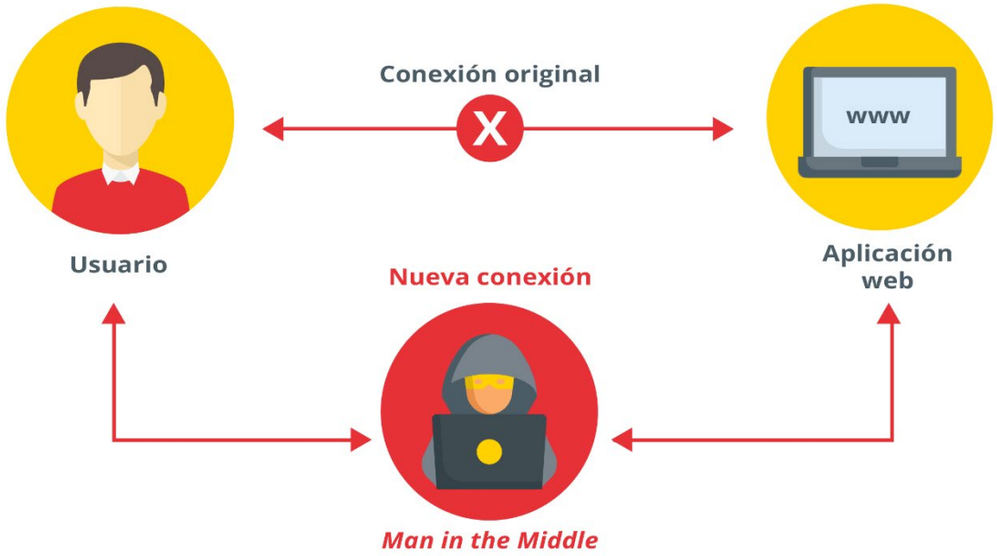
¿Sabías qué?

Se ha detectado una nueva campaña de *smishing,* enfocada a vendedores, que ofrecen un determinado medio de pago. Los atacantes intentan engañar a la víctima simulando querer comprar un producto y realizan la transacción, sin embargo, lo que hacen es solicitar una cuantía de dinero. En caso de que la víctima (el vendedor) lo acepte, estará pagando una cuantía al supuesto comprador. [18]

3 TIPOS DE CIBERDELINCUENTES Y ATAQUES MÁS COMUNES

Ataques a las conexiones: *Man in the Middle* (MitM) u «hombre en el medio»

Este ciberataque sucede cuando un ciberdelincuente **intercepta una comunicación entre dos partes**, posicionándose en el **medio**, recibiendo así los mensajes enviados e imitando, al menos, a una de las partes que se están comunicando. Por ejemplo, si dos usuarios se están comunicando, el atacante podría simular ser el receptor para contestar y enviar paquetes según la información que recibe del emisor, además de conocer toda la información que el este último está enviando. En otras ocasiones, simplemente se sitúan para escuchar las comunicaciones o interactúan como si fueran una de las dos partes.



Fuente: *Punto de acceso inalámbrico Man-in-the-Middle dentro de un contenedor de Docker* [Gráfico] Elaborado a partir de https://tecnonucleous.com

3 TIPOS DE CIBERDELINCUENTES Y ATAQUES MÁS COMUNES

Ataques a las conexiones: *Man in the Middle* (MitM) u «hombre en el medio»

Existen diferentes escenarios de ataque en los que se puede producir un ataque «MitM»:

- Puntos de acceso a la red wifi abiertos o con baja seguridad.
- Redes locales (LAN), donde el atacante deberá obtener acceso a la Red y engañará al resto de dispositivos haciéndoles creer que es un dispositivo legítimo.
- *Software* de navegación anticuado.

¿Sabías qué?

Los ciberdelincuentes aprovechan las transacciones bancarias para realizar estafas mediante el método MiTM. [19]

3 TIPOS DE CIBERDELINCUENTES Y ATAQUES MÁS COMUNES

Ataques a las conexiones: Denegación de Servicio (DoS), Denegación de Servicio Distribuido (DDoS) y Denegación Económica de Sostenibilidad (EDoS)

El objetivo de un **ataque de Denegación de Servicio** es inhabilitar el uso de un sistema, una aplicación o una máquina, para así lograr **bloquear el servicio que ofrece**. Los atacantes utilizan un único dispositivo (en el caso del ataque DoS) o varios dispositivos (en el caso de DDoS) que están preparados para lanzar el ataque y, con ello, **incapacitan la posibilidad de completar las solicitudes** que sí son legítimas. Vamos a conocer el ciberataque DoS y sus variantes con más detalle:

- El **ataque DoS (*Denial of Service*)**: este ciberataque genera una **cantidad masiva de peticiones al servicio desde una misma máquina o dirección IP**, consiguiendo así la incapacidad de respuesta por parte del servicio, ya que se satura y es incapaz de responder a todas, por lo que comienza a rechazar las peticiones y se bloquea, logrando, de este modo, la denegación del servicio.

3 TIPOS DE CIBERDELINCUENTES Y ATAQUES MÁS COMUNES

Ataques a las conexiones: Denegación de Servicio (DoS), Denegación de Servicio Distribuido (DDoS) y Denegación Económica de Sostenibilidad (EDoS)

- El **ataque DDoS (*Destributed Denial of Service*)**: su misión es generar peticiones o conexiones **empleando varias máquinas o direcciones IP, al mismo tiempo y contra el mismo objetivo**.

¿Sabías qué?

En 2021, Microsoft mitigó uno de los mayores ataques DDoS de la historia contra un cliente en Asia, alcanzando los 3,47 terabits por segundo, proveniente de 10.000 fuentes distribuidas entre 10 países diferentes del mundo.

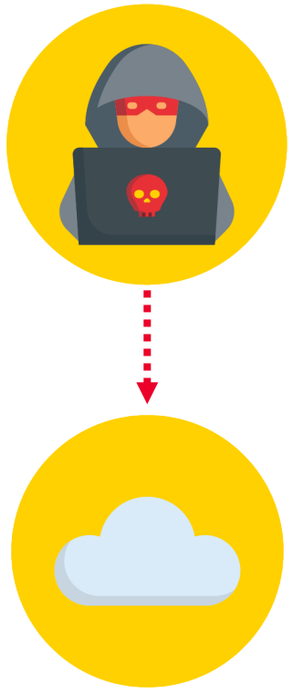
Saber más

Conoce más ataques DDoS. [20]

3 TIPOS DE CIBERDELINCUENTES Y ATAQUES MÁS COMUNES

Ataques a las conexiones: Denegación de Servicio (DoS), Denegación de Servicio Distribuido (DDoS) y Denegación Económica de Sostenibilidad (EDoS)

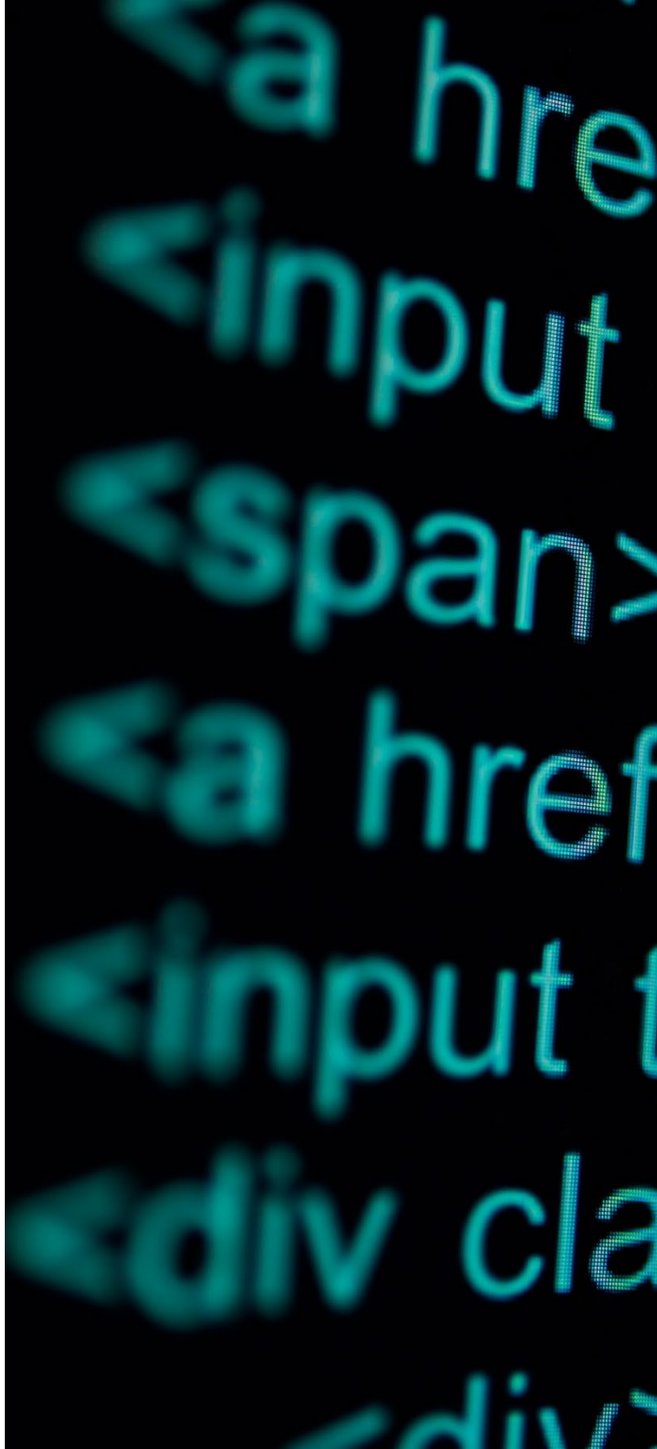
- El **ataque EDoS (*Economic Denial of Dustainability*)**: se trata de un nuevo tipo de ataque que afecta al **servicio *cloud*** y se aprovecha de las características de elasticidad y autoescalado de la nube para cargar en la factura de un usuario de la nube una **cantidad excesiva de costes**, ya que los atacantes se encargan de contratar servicios sin el conocimiento ni consentimiento del usuario afectado, buscando su quiebra. Este tipo de ataques afecta a todos los usuarios, no únicamente a los que sufren este ataque de forma directa, ya que los proveedores de servicios en *cloud*, al atender gran cantidad de peticiones no legítimas, pierden capacidad para atender las que sí lo son.



3 TIPOS DE CIBERDELINCUENTES Y ATAQUES MÁS COMUNES

Ataques a las conexiones: inyección SQL

El **código SQL** es un **lenguaje de programación** que se utiliza para administrar y obtener información de bases de datos. Una **base de datos** es una recopilación de información o datos organizados que pueden ser utilizados o consultados posteriormente. Muchas páginas web utilizan bases de datos, por ejemplo, para almacenar la información de los usuarios que están registrados en ellas. Si un usuario se registra en una página, introduce un nombre de usuario y una contraseña, estos datos se almacenarán en la base de datos de esa página, lo que permitirá que la próxima vez que el usuario desee iniciar sesión se haga una comprobación de que ese nombre de usuario existe en la base de datos y que la contraseña que el usuario ha introducido corresponde con la que está almacenada en la base de datos.



3 TIPOS DE CIBERDELINCUENTES Y ATAQUES MÁS COMUNES

Ataques a las conexiones: inyección SQL

Una **inyección SQL** se basa en utilizar las instrucciones de una base de datos que no han sido correctamente aseguradas, insertándole instrucciones adicionales, de forma que el atacante gana acceso a información que no debería.

¿Sabías qué?

En 2016, se produjo una filtración de la base de datos del Banco Nacional de Qatar, tras el que se expusieron los nombres y contraseñas de unos 1.200 clientes. [21]

3 TIPOS DE CIBERDELINCUENTES Y ATAQUES MÁS COMUNES

Ataques a las conexiones: XSS (derivado de *Cross-Site Scripting*)

Aunque los ataques XSS se basan en la misma teoría que los ataques de inyección SQL, en este caso, el objetivo no es un servidor o base de datos, sino la **aplicación que sirve a la página web**, es decir, los atacantes aprovechan una **vulnerabilidad** o fallo de seguridad de la página web e **implantan *scripts* maliciosos** en ese sitio web, que es legítimo, para que cuando un usuario accede a dicho sitio web a través del navegador, el *script* se ejecute y afecte al navegador del usuario, pudiendo entonces robar credenciales, redirigir al usuario a otro sitio web malicioso, etc.

Recordemos que un ***script*** es una secuencia de comandos o fragmentos de código cuyo objetivo de realizar o añadir funciones dentro de un dispositivo o servicio. En este caso, el atacante trata de añadir una serie de instrucciones extra esperando que el navegador las reconozca y las ejecute.

3 TIPOS DE CIBERDELINCUENTES Y ATAQUES MÁS COMUNES

Ataques a contraseñas: de fuerza bruta y por diccionario

Este ciberataque es el método más extendido para realizar la autenticación del acceso a un sistema de información seguro, ya que, al acceder con la contraseña de un usuario, el atacante puede acceder a todos los datos, información y sistemas a los que pueda acceder el usuario suplantado. Existen dos métodos de acceso con contraseña muy conocidos:

- **Ataque de fuerza bruta**: se trata del proceso basado en utilizar una lista de contraseñas comunes para intentar acceder a la Red, es decir, a través de un proceso de ensayo y error.
  - **Ataque por diccionario**: este ciberataque es el subtipo de ataque de fuerza bruta más conocido y está basado en el mismo modelo de ensayo y error, con la diferencia de que, en este caso, existe un «diccionario» en el que se encuentran listadas las contraseñas conocidas o de uso común. Por ejemplo, el objetivo más común es acceder a la contraseña que aparece por defecto en los *routers* de conexión a Internet.

3 TIPOS DE CIBERDELINCUENTES Y ATAQUES MÁS COMUNES

Ataques a contraseñas: *fuzzing*

¿Sabías qué?

Estas han sido las contraseñas más utilizadas, según un estudio anual. [22]

- Un ataque que se utiliza también en estos casos es el *fuzzing*. El **ataque por *fuzzing*** consiste en enviar a una aplicación o formulario unos datos deliberadamente incorrectos. El objetivo de este tipo de ataque es descubrir vulnerabilidades durante los procesos de *login* y envío o recepción de información y, en algunos casos, lograr autenticarse en las aplicaciones aprovechándose de estos fallos de seguridad. Por ejemplo, un ataque por *fuzzing* en un formulario de autenticación intentaría introducir caracteres especiales en el campo usuario/contraseña como caracteres chinos, arábicos o de un conjunto de idioma diferente al de la aplicación o incluso intentar afectar a la integridad de la memoria de la aplicación.

3 TIPOS DE CIBERDELINCUENTES Y ATAQUES MÁS COMUNES

Otros ataques: ataques de día cero *o zero-day exploit*

Este tipo de ciberataques se basan en explotar las vulnerabilidades presentes en un *software* o de la Red que aún no han sido anunciadas por los desarrolladores de que existen y, por lo tanto, aún no existe un parche o una solución. En este caso, los ciberdelincuentes aprovechan la vulnerabilidad revelada en la pequeña ventana de tiempo, en la que no existe ninguna solución o medida preventiva.

¿Sabías qué?

Microsoft alertó de múltiples *exploits zero-day* que estaban siendo utilizados por un grupo de ciberdelincuentes apoyados por el estado chino, consiguiendo acceder a cuentas de correo electrónico e instalando *malware* adicional para facilitar el acceso a largo plazo a los dispositivos de las víctimas y así extraer información. [23]

4

INTRODUCCIÓN A LA CIBERSEGURIDAD OT

4 INTRODUCCIÓN A LA CIBERSEGURIDAD OT

¿Qué es la ciberseguridad industrial (OT)?

La ciberseguridad no está únicamente enfocada (o no afecta únicamente) a los sistemas informáticos al uso de una oficina, sino que también afecta al entorno industrial ya que, en sus comienzos, la industria se mantenía aislada y sin conectividad a la Red pero, a medida que ha ido creciendo e incorporando la automatización y la tecnología, ha ido evolucionado hasta lo que hoy se conoce como Industria 4.0, donde dichas fábricas, antes aisladas, hoy en día se conectan a la Red global, lo cual, a pesar de las enormes ventajas que esto supone, también han incrementado el riesgo de ser atacadas, ya que a los posibles ataques que podían recibir anteriormente, ahora se suman los ciberataques.

La Industria 4.0 se caracteriza por introducir en la ingeniería industrial los avances de las tecnologías de la información, digitalizando la producción y distribución, y así conseguir una cadena de suministro inteligente, digitalizada y conectada.

La evolución de la Industria 1.0 a la Industria 4.0

La industria ha evolucionado a lo largo de los años como consecuencia de diferentes factores que han influido en las cadenas de producción y logística:

Fuente: *Industry 4.0 - The future of making «Smart Industries»*
[Ilustrativo] Elaborado a partir de https://medium.com

4 INTRODUCCIÓN A LA CIBERSEGURIDAD OT

La ciberseguridad industrial: entornos OT y entornos IT

La **conectividad de la Industria 4.0** y de los **sistemas tradicionales del ámbito OT (Tecnologías de las Operaciones)** han incrementado la exposición de los dispositivos en Internet, lo que los ha vuelto más vulnerables y fáciles de explotar. Además, al contrario que en IT, tampoco tienen soluciones triviales de parcheado o aislamiento por las características especiales del entorno.

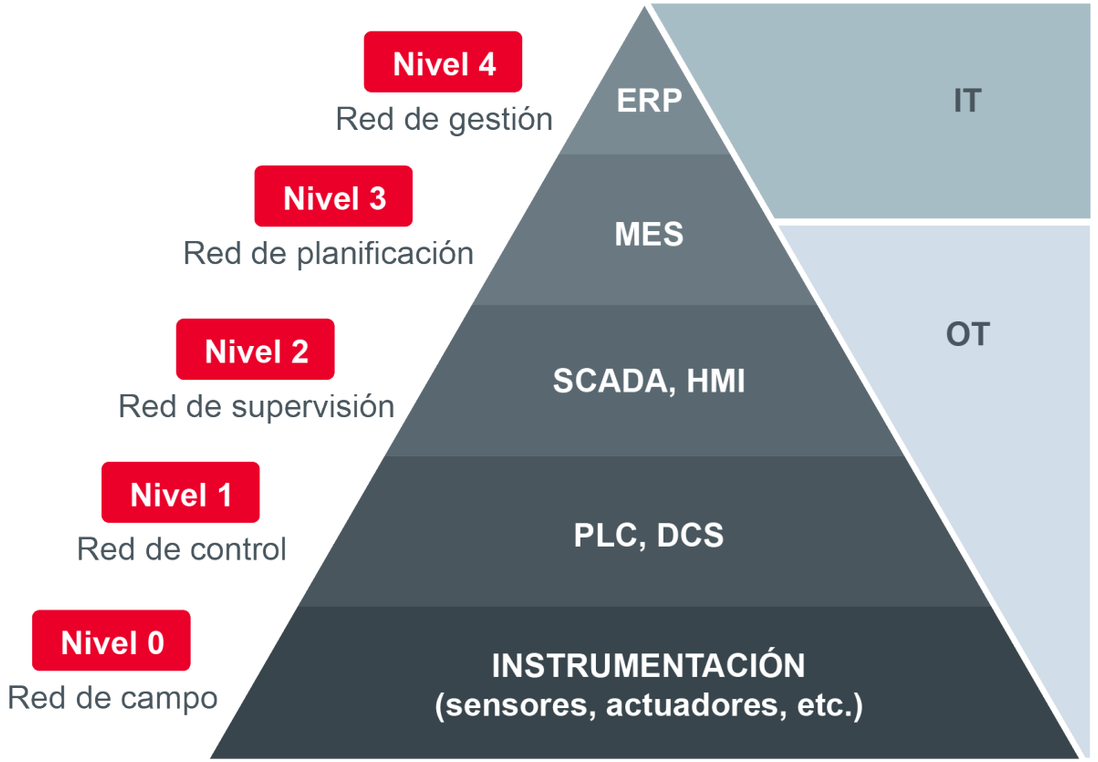
La **ciberseguridad industrial** aúna diferentes principios de seguridad de los entornos OT y principios de seguridad de los entornos IT (tecnologías de la información), con el fin de proteger los distintos activos de una industria, así como las redes, los procesos existentes, los datos y la información.

¿Sabías qué?

En los coches inteligentes se han identificado los principales vectores de ataque con el objetivo de mejorar su ciberseguridad y reducir los riesgos a los que están expuestos. [24]

La pirámide de automatización industrial

La pirámide de automatización industrial representa la integración de la tecnología en la industria. Existen cinco niveles tecnológicos que podemos encontrar en cualquier entorno industrial (OT) y donde dichos niveles se relacionan entre sí, dentro de cada nivel y entre los diferentes niveles, a través de estándares de comunicación industriales.

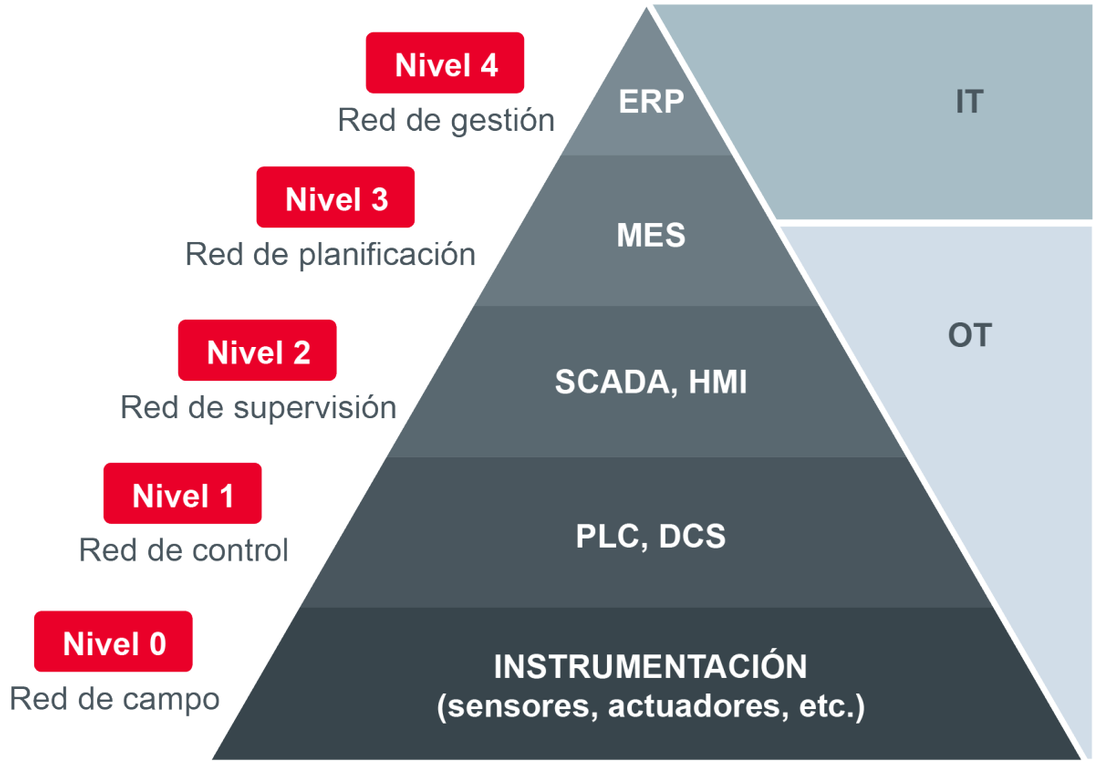


Fuente: *Pirámide CIM de Automatización Industrial* [Gráfico] Elaborado a partir de https://atec-energy.com

La pirámide de automatización industrial

Esta pirámide muestra la forma en la que los procesos de fabricación se integran con los sistemas de gestión de producción y administración.

Existen diferentes aproximaciones de pirámides de automatización industrial, sin embargo, el modelo de cinco niveles es el más extendido.



Fuente: *Pirámide CIM de Automatización Industrial* [Gráfico] Elaborado a partir de https://atec-energy.com

La pirámide de automatización industrial

Nivel 0: red de campo

En el nivel 0 se encuentra **la red de campo**, que hace referencia a todos aquellos dispositivos que se utilizan para la instrumentación, es decir, para realizar el **trabajo físico** y la **monitorización**. Estos dispositivos pueden ser:

- **Sensores**: estos mecanismos generan señales eléctricas a partir de variables físicas, como la temperatura, el nivel o la velocidad.
- **Actuadores**: estos sistemas convierten la energía en movimiento o sirven para activar el funcionamiento de otro dispositivo acoplado a él. Por ejemplo, las válvulas o bombas mantienen variables, como el flujo, el calor o la presión dentro de unos parámetros establecidos.
- **Mecanismos**: estos dispositivos se activan a raíz del funcionamiento de los actuadores a los que están conectados.

La pirámide de automatización industrial

Nivel 1: red de control

En el nivel 1 se encuentra **la red de control**, que permite a los operadores controlar las **variables**, actuando como el «cerebro» en todo el proceso. Por lo general, consta de los siguientes dispositivos:

- **El controlador lógico programable o PLC** (del inglés *Programmable Logic Controller*), que se encarga de procesar los datos del nivel 0 y emitir órdenes a otros dispositivos, tanto del nivel 1 como del nivel 0, en base a esos datos**.**
- **El sistema de control distribuido o DCS** (del inglés *Distributed Control System*), realiza la misma función que el PLC, con la diferencia de que, en este caso, encontramos varios dispositivos de control distribuidos de forma geográfica, que se gestionan desde un punto de control específico.

Ambos dispositivos tienen un funcionamiento digital y su objetivo es controlar los distintos tipos de máquinas y procesos.

La pirámide de automatización industrial

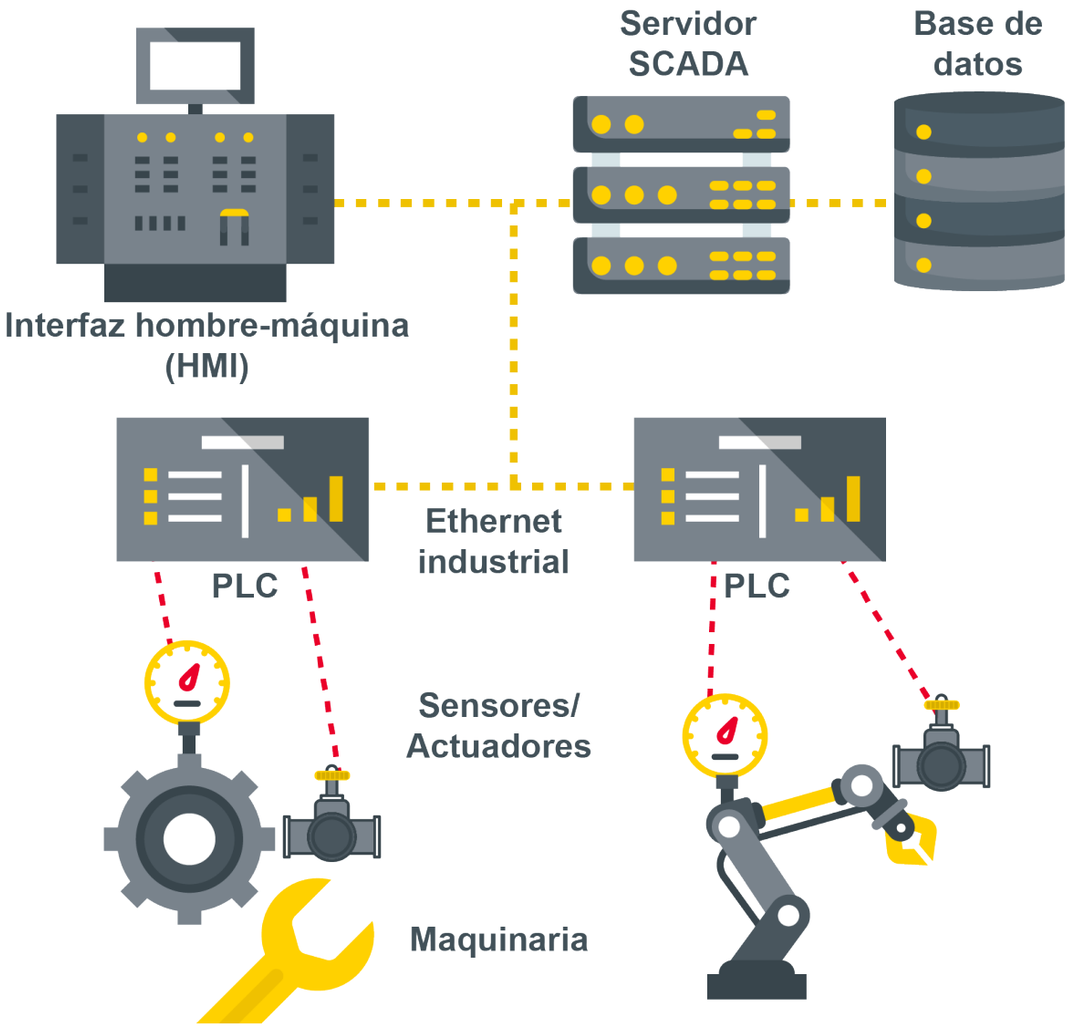
Nivel 2: red de supervisión

El nivel 2 comprende la **red de supervisión** tanto los sistemas de control de supervisión y adquisición de datos (SCADA) como las interfaces hombre-máquina (HMI). Veamos en qué consiste cada uno de ellos:

- **SCADA** (del inglés *Supervisory Control and Data Acquisition*): este sistema controla múltiples máquinas en diferentes procesos complejos. Se encarga de controlar, supervisar, recopilar y analizar datos y generar informes, lo que permite mejorar la eficiencia de los procesos, tomar mejores decisiones de negocio y comunicar los problemas que puedan surgir. Además, también permite almacenar esos datos en bases de datos para su posterior análisis o procesamiento.
- **HMI** (del inglés *Human Machine Interface*): esta interfaz o panel de control permite que un usuario u operario pueda interactuar con un dispositivo. Normalmente, se utiliza para la monitorización o visualización de lo que ejecuta el SCADA, aunque también lo podemos encontrar en el nivel 1 con los PLC.

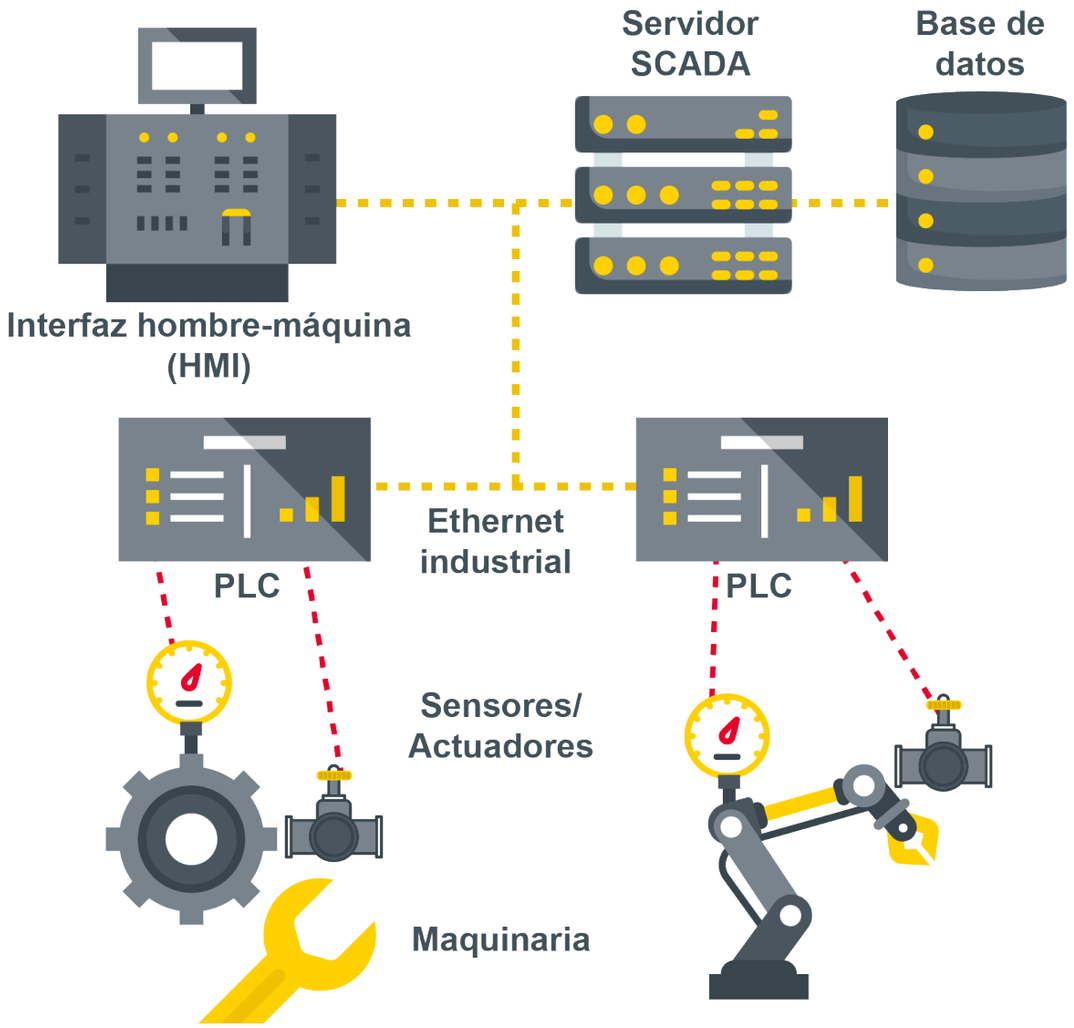
La diferencia entre el nivel 1 y el nivel 2

Una de las principales diferencias entre el nivel de control y el de supervisión es que, aunque ambos niveles reciben información de los procesos y emiten órdenes a los distintos dispositivos, **los sistemas SCADA propios de la red de supervisión se utilizan para corregir errores o restablecer valores en la red de control**.



La diferencia entre el nivel 1 y el nivel 2

Como podemos ver en la imagen, estos tres niveles inferiores de la pirámide de automatización, la red de campo con la maquinaria, sensores y actuadores, la red de control con los PLC, y la red de supervisión con los sistemas SCADA y HMI, se pueden relacionar de la siguiente manera: el PLC controla los dispositivos de campo, como los sensores o actuadores, y de los PLC, llegan los datos de esos dispositivos a los servidores SCADA, que muestran los datos en el HMI y permiten que el usuario interactúe con los dispositivos; además, de almacenar esos datos en la base de datos.



La pirámide de automatización industrial

Nivel 3: red de planificación

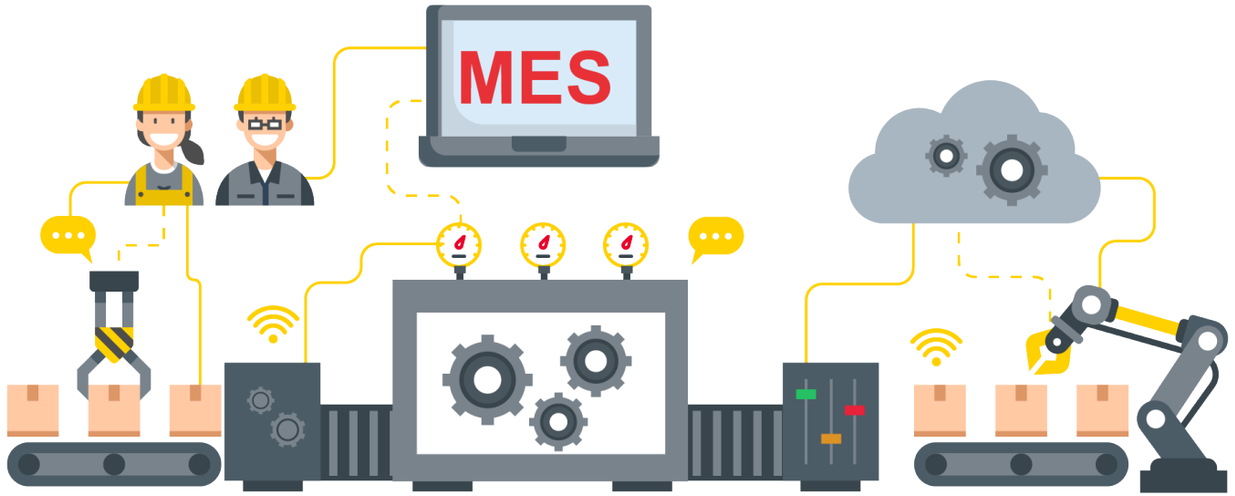
El nivel 3 está constituido por el **nivel de planificación o red de operación**, en la que encontramos los **sistemas MES** (del inglés *Manufacturing Execution System*) que ofrecen datos e información, permitiendo así la optimización de las actividades de producción, desde el lanzamiento hasta los productos finales, es decir, los sistemas MES guían, inician, responden e informan sobre las actividades que están sucediendo en la planta en tiempo real.

También encontramos los **sistemas MOM** (del inglés *Manufacturing Operations Management*), que, aunque muchas veces se utilizan MES y MOM indistintamente, MOM hace referencia a un concepto más global, aportando una visibilidad completa de los procesos de fabricación, con el objetivo de ofrecer una mejora constante del rendimiento de las operaciones de fabricación.

INTRODUCCIÓN A LA CIBERSEGURIDAD OT

La pirámide de automatización industrial

El sistema MES engloba los datos de todos los procesos de fabricación que suceden en la planta, es decir, está relacionado con los sistemas SCADA, los HMI a través de los cuales los operarios interactúan con los dispositivos, los PLC y todos los demás dispositivos, ya sean de nivel 0, 1 y 2. Esto permite tener una visibilidad de las actividades que se realizan en la planta y facilita la corrección de errores y la toma de decisiones para aumentar la producción y optimizar los procesos.



La pirámide de automatización industrial

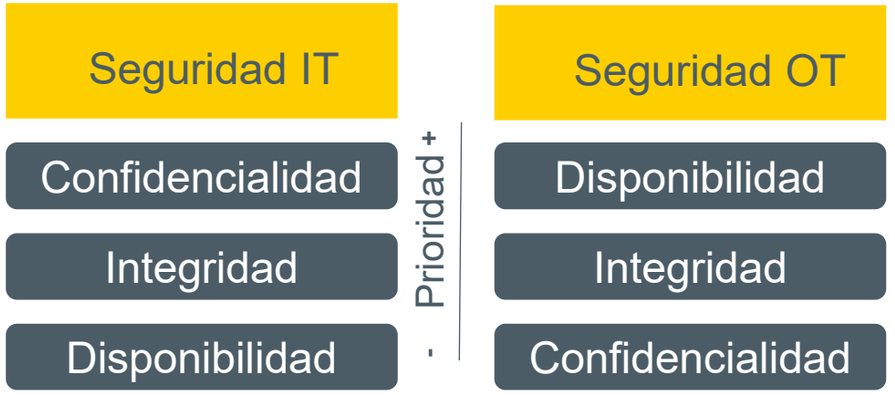
Nivel 4: red de gestión

Por último, en el nivel 4 o **red de gestión**, encontramos los sistemas que administran los recursos empresariales (ERP). Estos **sistemas ERP** proporcionan información global de la producción de una organización, además de aspectos diversos como las ventas, la logística, el inventario, facturación, RRHH, etc., lo que permite la toma de decisiones de negocio a nivel global; es decir, mientras que los sistemas MOM o MES monitorizan y controlan los procesos de fabricación para facilitar la toma de decisiones de dichos procesos y optimizar la producción, los sistemas ERP permiten obtener una visión globalizada, seguimiento y control de toda la organización.

Principales diferencias entornos IT y entornos OT

A nivel de ciberseguridad, las principales diferencias entre los entornos IT (tecnologías de la información) y los entornos OT (tecnologías de las operaciones) son las siguientes:

- Mientras que en los entornos IT se da prioridad y mayor importancia a la confidencialidad de la información y seguridad de los datos, en los entornos OT, sin embargo, la prioridad es la disponibilidad de las máquinas y dispositivos.
- Por otro lado, la media de vida útil de los dispositivos IT es de 3-5 años y son más sencillos de actualizar, mientras que la vida media de los equipos OT es de más de 20 años. Por este motivo, existen muchos sistemas obsoletos, no actualizados y mucho más vulnerables a las amenazas.



Fuente: *Principales diferencias entornos IT y entornos OT* [Gráfico] Elaboración propia

Últimos ciberataques en los entornos OT

La convergencia entre entornos IT y OT, con la llegada de la industria 4.0, ha provocado un aumento de los ataques a los entornos industriales. Algunos de los ciberataques más destacados en la última década han sido los siguientes:

2010 **Ataque de Stuxnet a una instalación nuclear iraní**

Se destruyeron 1000 máquinas en la central nuclear de Natanz, Irán.

2014 **Ciberataque a una fábrica de acero alemana [25]**

El ataque afectó a numerosos sistemas, imposibilitando el apagado controlado del alto horno y causando un daño masivo a la infraestructura de la fábrica.

Últimos ciberataques en los entornos OT

2017 ***Ransomware* WannaCry [26]**

Un *ransomware* afectó a más de 300.000 empresas en 150 países. Aunque estaba pensado para afectar a los sistemas IT, al afectar a sistemas Windows que manejaban software de control industrial, también afectó a los sistemas OT.

2021 ***Darkside* a oleoducto Colonial Pipeline [27]**

Un *ransomware* que afectó al suministro de combustible en EE.UU. y produjo una brecha de seguridad.

¿Sabías qué?

El grupo de cibercriminales Darkside pudo acceder a los sistemas a través de una contraseña comprometida de un empleado. [28]

Causas de los ciberataques en los entornos OT

Los ciberataques son cada vez más numerosos y se debe a diferentes causas que caracterizan a los entornos industriales:

Falta de visibilidad de los activos
En muchas ocasiones no se sabe qué dispositivos están conectados a la Red.

Mala segregación de entornos
La mala o escasa segregación conlleva la posibilidad de que el atacante pueda afectar a ambas redes (IT y OT).

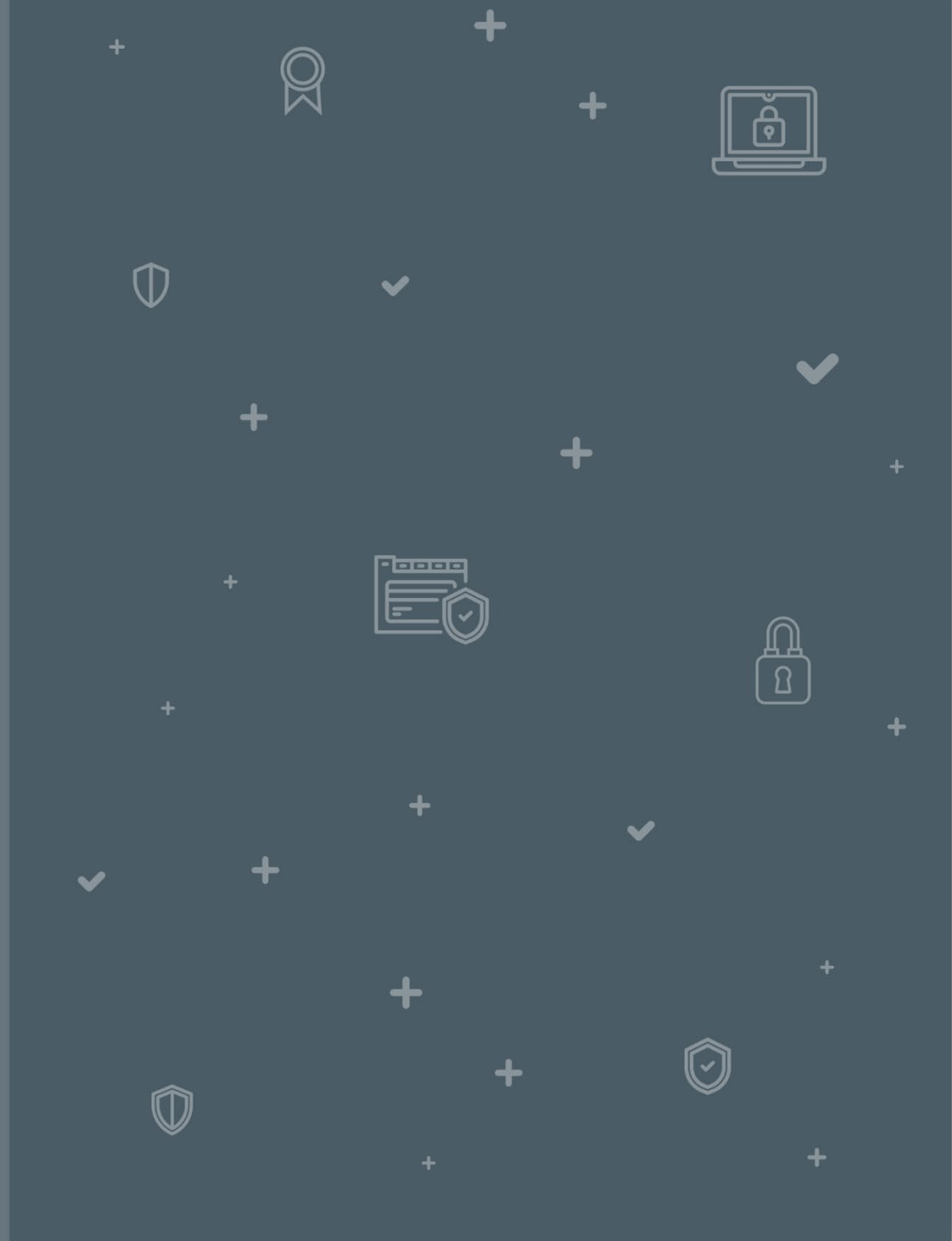
Ausencia de sistemas de protección
No se suele realizar una correcta monitorización del tráfico y los activos, lo que dificulta la detección temprana de un posible ataque.

Ausencia de políticas
Aunque ahora existen normativas enfocadas a OT, estas políticas de gobierno venían impulsadas tradicionalmente por IT y no había herramientas y medidas claras a implementar en OT.

Vulnerabilidades y amenazas
La priorización de la disponibilidad de la información ha hecho que se suelan emplear protocolos no cifrados, sistemas abiertos a Internet, etc. sin contemplar otros factores, como la confidencialidad, integridad y autenticidad de la información.

5

MÉTODOS Y TIPOS DE PROTECCIÓN



5 MÉTODOS Y TIPOS DE PROTECCIÓN

Introducción

A lo largo de esta unidad, hemos conocido los riesgos que existen y los ataques a los que son susceptibles y vulnerables los activos y los sistemas de información. Por ello, tomar las medidas adecuadas para protegerlos y, de este modo, mitigar el impacto y las consecuencias que un ataque pudiera causar, es un factor fundamental.

En este apartado, vamos a analizar qué métodos, tipos y medidas de protección podemos llevar a cabo para prevenir un posible ataque y para proteger nuestros activos, en caso de que se llegue a materializar uno.

Las medidas de seguridad que se apliquen variarán en función del sistema que se pretenda proteger, de la información que contiene, de las características particulares y las amenazas a las que están expuestos.

5 MÉTODOS Y TIPOS DE PROTECCIÓN

Medidas de protección

Instalación de *software* legal y antivirus

La instalación de un *software* legal, es decir, que haya sido descargado de su web oficial, aporta la seguridad de estar libre de *malware* y permite disponer de las actualizaciones necesarias, lo que incrementa la protección contra vulnerabilidades.

Con independencia del uso que vaya a tener el ordenador y los programas que sean necesarios que disponga, un *software* indispensable que deben tener todos los equipos es un antivirus. Al igual que cualquier otro programa, el antivirus deberá ser descargado de la página oficial del fabricante y tendrá estar actualizado para que pueda cumplir su cometido, independientemente de si es un *software* gratuito o de pago. Disponer de un buen antivirus es muy importante ya que previene, protege y elimina los posibles programas maliciosos que puedan intentar atacar el ordenador.

5 MÉTODOS Y TIPOS DE PROTECCIÓN

Medidas de protección

Instalación de *software* legal y antivirus

Por otro lado, llevar a cabo una correcta configuración de los equipos resulta esencial, además de realizar un uso adecuado de la misma; por ejemplo, no navegar por Internet con una cuenta de administrador, sino dejar esta cuenta con permisos especiales únicamente para la instalación de programas, o utilizar siempre la última versión, que suele corregir los fallos de seguridad o vulnerabilidades que se han localizado.

5 MÉTODOS Y TIPOS DE PROTECCIÓN

Medidas de protección

Segregación o segmentación de redes

Se trata de dividir la Red en subredes más pequeñas que permiten un mayor y mejor control sobre las mismas, aumentar su seguridad, aislar los posibles incidentes que ocurran y mejorar su rendimiento, ya que se reduce el tráfico.

Este método consiste en acotar el acceso a los activos, como la información o los recursos y así limitar o dificultar la propagación de los incidentes de seguridad, ya que estos quedan limitados al segmento de Red donde tienen lugar.

Así, la Red de nuestra casa puede segmentarse en subredes distintas, por ejemplo, una subred para los dispositivos IoT, otra subred wifi para que puedan utilizar los invitados y otra diferente para el resto de dispositivos, consiguiendo así una mayor protección.

5 MÉTODOS Y TIPOS DE PROTECCIÓN

Medidas de protección

Firewall

El *firewall* o cortafuegos se encarga de analizar el tráfico existente en la Red, reconocer a los usuarios autorizados y restringir el acceso de aquellos que no lo están, es decir, se trata de un sistema que previene y protege la Red de intrusiones o ataques, bloqueando su acceso.

Esta herramienta gestiona el tráfico entrante y saliente que hay entre redes o entre ordenadores de una misma Red, permitiendo únicamente el tráfico que cumpla con las reglas que se han especificado previamente. En caso de no cumplirlas, el tráfico será bloqueado. Aunque los *firewalls* vienen con unas reglas configuradas por defecto, lo ideal es realizar nuestra propia configuración estableciendo las reglas que deseemos, y siempre tratando de ser lo más restrictivas posibles.

5 MÉTODOS Y TIPOS DE PROTECCIÓN

Medidas de protección

Sistema de Detección de Intrusiones (*Intrusion Detection System* – IDS).

Este método se encarga de la detección de accesos no autorizados a un ordenador o una Red y lo hacen monitorizando el tráfico entrante y cotejándolo con una base de datos actualizada de ataques conocidos. En caso de sospechar de alguna actividad poco habitual, se emite una alerta. Los dispositivos IDS solo emiten alertas sobre posibles intrusiones, no mitigan la intrusión. Sin embargo, existen algunos IDS que también permiten tomar medidas como bloquear ciertas acciones.

MÉTODOS Y TIPOS DE PROTECCIÓN

Medidas de protección

Sistema de Prevención de Intrusiones (*Intrusion Prevention System* – IPS).

Un IPS es una versión más avanzada del IDS, ya que abarca las mismas funciones que el IDS, pero además puede configurarse para que en vez de simplemente avisar, realice determinadas acciones configuradas previamente. Esta medida se encarga de proteger los sistemas de posibles ataques e intrusiones. Se analizan las conexiones y los protocolos en tiempo real para precisar si está ocurriendo o va a ocurrir un incidente, y se realiza según el análisis de patrones o comportamientos sospechosos, por lo que también es capaz de rechazar paquetes.

5 MÉTODOS Y TIPOS DE PROTECCIÓN

Medidas de protección

Hemos analizado los métodos y los dispositivos que nos pueden facilitar la protección de nuestros activos y sistemas de información, pero ¿qué medidas concretas podemos tomar como usuarios? Veamos algunas de ellas:

- **Limitar el acceso a la información**: la práctica más común sería cifrar la información para que la persona que pretenda conocer esa información no pueda hacerlo, si no dispone de la clave para descifrarla. Además, se debe tener precaución con el uso de redes sociales, con la información que se publica y con quién se comparte.
- **Proteger el correo electrónico**: una buena práctica es utilizar filtros antispam, así como cifrar los mensajes, ya que favorecen proteger la información almacenada.
- **Realizar copias de seguridad o *backups***: las copias de seguridad periódicas pueden restablecer la información en caso de pérdida. Por ejemplo, una buena medida de protección sería mantener una copia en la nube y una réplica en un disco duro local.

5 MÉTODOS Y TIPOS DE PROTECCIÓN

Medidas de protección

Otra medida de protección esencial es respecto a las contraseñas. Veamos algunas de las características o requisitos que se deben cumplir para tener una contraseña segura:

- **No repetir contraseñas en diferentes programas o páginas web en las que se deba realizar una autenticación**. Existe la posibilidad de utilizar un gestor de contraseñas que genera una contraseña aleatoria. Un gestor de contraseñas es una base de datos que recuerda tus contraseñas de acceso a cada servicio y/o páginas web por lo que facilita usar una contraseña diferente para cada sitio. Adicionalmente, al tener las contraseñas almacenadas se elimina la necesidad de recordarlas y es posible emplear contraseñas más robustas.
- **No hacerlas predecibles**, no utilizar datos personales como la fecha de cumpleaños, lugar de nacimiento o nombre de la mascota, por ejemplo. Incluso cambiar vocales por números similares ahora ya empieza a ser considerado contraseña predecible.

5 MÉTODOS Y TIPOS DE PROTECCIÓN

Medidas de protección

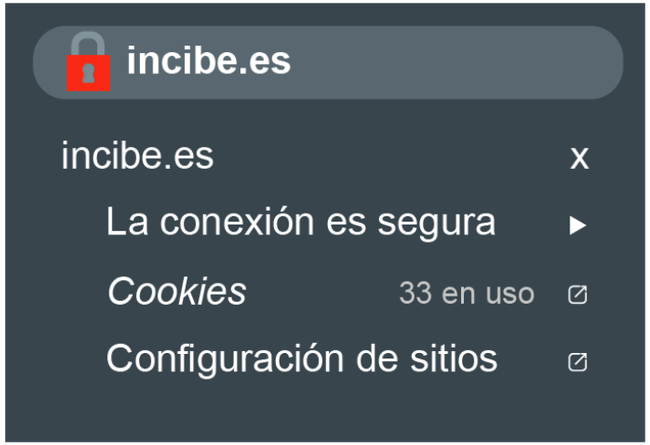
- **Deben tener** una longitud mínima de 8 caracteres, utilizando mayúsculas, minúsculas, caracteres, letras y números.
- **No deben compartirse con nadie**.
- En caso de sospecha de que se ha podido comprometer la contraseña, **cambiarla inmediatamente**, por ejemplo, cuando tenemos noticia de que han hackeado un sitio web o, al menos, obtenido datos de acceso de usuarios.
- **Cambiar las contraseñas con regularidad**.
- Cuando sea posible, **utilizar autenticación de varios factores**, por ejemplo, no solo introducir la contraseña de usuario, sino, además, un código PIN numérico y aleatorio que se envíe al teléfono móvil para vez que se desee iniciar sesión.

Un ejemplo de contraseña segura sería Xk3J4%a2./.

5 MÉTODOS Y TIPOS DE PROTECCIÓN

Medidas de protección

- **Acceder a páginas web y compras seguras**: las páginas web seguras disponen de un certificado SSL/TLS (*Secure Socket Layer/Transport Layer Security*) o utilizan el protocolo HTTPS (*Hyper Text Transfer Protocol Secure*), que acredita la seguridad de esa web y cifra la información para establecer conexiones seguras entre cliente y servidor. Así, aseguran que no pueda ser interceptada por personas no autorizadas. Así, por ejemplo, se puede comprobar la seguridad del sitio web con el icono del candado que aparece justo antes de la dirección de Internet en el navegador para verificar su certificado.
- **Evitar utilizar redes públicas u ordenadores compartidos** en caso de que se vayan a introducir credenciales de acceso o datos de pago, exceptuando los ordenadores domésticos.



5 MÉTODOS Y TIPOS DE PROTECCIÓN

Medidas de protección

- **Almacenar la información en la nube y en local**: la nube permite el almacenamiento de cualquier tipo de información de manera virtual, pero requiere estar bien protegida de posibles ataques. Otra opción, es el almacenamiento de local, es decir, mediante dispositivos físicos.

- **Proteger todos los dispositivos**: es importante utilizar métodos de protección en nuestros dispositivos (ordenadores, teléfonos móviles, tabletas, etc.), no solo a través de contraseñas o patrones seguros, es decir, un bloqueo de acceso, sino también realizando copias de seguridad o *backups* periódicos para minimizar el riesgo de pérdida de datos o información. Algunos sistemas operativos permiten la opción de hacer una copia diaria y automática de aquellos datos más relevantes.

RESUMEN

Aspectos básicos de ciberseguridad

- La seguridad de la información, la ciberseguridad y la seguridad informática hacen referencia a todas aquellas medidas preventivas y procedimientos que protegen el tratamiento de los datos y la privacidad de la información ante cualquier posible ciberataque.
- Una vulnerabilidad es una debilidad en un sistema de información que pone en riesgo a los activos de información de sufrir un ciberataque. Por otro lado, una amenaza (*malware*, ingeniería social, *botnet,* ATP, etc.) es un elemento que compromete una vulnerabilidad con el fin de atacar un activo de información. En este sentido, un riesgo sería la posibilidad de que una amenaza pueda llevar a cabo esta acción para causar una pérdida o daño en un activo de información.

RESUMEN

Aspectos básicos de ciberseguridad

- La ciberseguridad es el conjunto de prácticas que tratan de proteger los sistemas, los servidores de Red y los dispositivos móviles inteligentes de ciberataques maliciosos, como *malware*, *ransomware*, *phishing*, *vishing* y *smishing*, ataques a contraseñas, *Man in the Middle*, DoS, DDoS, EDoS, inyección SQL, *Cross-Site Scripting* (XSS) y ataques *zero-day,* entre otros.
- La Industria 4.0 se ha desarrollado gracias a los avances de las tecnologías de la información con el objetivo de digitalizar la producción y distribución de la cadena de suministro. En este sentido, la ciberseguridad industrial se refiere a aquellas políticas de seguridad de los entornos OT y de los entornos IT que tienen como objetivo proteger los activos más valiosos de una industria.

RESUMEN

Aspectos básicos de ciberseguridad

- Para proteger los activos de información, así como los sistemas electrónicos, servidores, redes sociales, aplicaciones y dispositivos móviles, es recomendable el uso de *software* legales y programas o dispositivos de seguridad como antivirus, *firewall* o cortafuegos, IDS e IPS**.** Otras medidas preventivas que se deben llevar a cabo son el utilizar contraseñas robustas, comprar de forma segura en páginas web legítimas, realizar copias de seguridad periódicas, limitar el acceso a la información de los sistemas controlando así el acceso de los usuarios para evitar accesos indebidos y proteger el correo electrónico y el teléfono móvil, siempre que sea posible, con credenciales de doble identificación.

CONCLUSIONES

Aspectos básicos de ciberseguridad

- La **seguridad de la información** es el conjunto de políticas, procedimientos y medidas preventivas y reactivas que afectan a la seguridad del tratamiento de los datos en cualquier formato, ya sea electrónico, en papel, verbal, etc., y en cualquier etapa de su uso, recopilación, almacenamiento, procesamiento, trasmisión y borrado.
- La **seguridad informática** es la disciplina que protege la integridad y la privacidad de la información que se almacena en el sistema informático u ordenador de cualquier posible ataque o acceso no autorizado. Es el proceso que trata de prevenir y detectar tanto el uso como el acceso no autorizado a un sistema informático.
- La **ciberseguridad** es el conjunto de prácticas que tratan de defender los ordenadores, los servidores, los dispositivos móviles, los sistemas electrónicos, las redes y los datos de ataques maliciosos, es decir, tiene por objetivo la protección de la información que se almacena y trasmite en los sistemas.

CONCLUSIONES

Aspectos básicos de ciberseguridad

- Mientras que la **seguridad informática** hace referencia a la protección de un único ordenador, la **ciberseguridad** se refiere a la protección de un conjunto de ellos.
- Los **principios básicos** de la seguridad de la información son la confidencialidad, integridad, disponibilidad, autenticidad, trazabilidad y el no repudio o irrenunciabilidad.
- Se considera **activo** todo aquello que tiene valor para la empresa o el usuario. Un **activo de información** comprende todos aquellos recursos utilizados para generar, procesar, almacenar o transmitir la información como las aplicaciones, ordenadores o móviles, a parte de la información y los datos.

CONCLUSIONES

Aspectos básicos de ciberseguridad

- Cuando hablamos de una **vulnerabilidad** nos referimos a una debilidad o fallo en un activo. Sin embargo, una **amenaza** hace referencia a todos aquellos elementos que aprovechan una vulnerabilidad para atentar contra la seguridad de un activo de información. Cuando una amenaza aprovecha una debilidad o vulnerabilidad de un sistema de información, estamos ante un **incidente de seguridad**. Los incidentes de seguridad de la información implican la explotación de una o varias vulnerabilidades que afecten a alguno de los principios de ciberseguridad: confidencialidad, integridad y disponibilidad de los recursos de dicho sistema.
- El **impacto** hace referencia a las consecuencias de la materialización de una amenaza sobre un activo aprovechando una vulnerabilidad.
- La **probabilidad** es la posibilidad de que ocurra un hecho, suceso o acontecimiento.

CONCLUSIONES

Aspectos básicos de ciberseguridad

- El **riesgo** se define como la posibilidad de que una amenaza concreta pueda aprovechar una vulnerabilidad para causar una pérdida o daño en un activo de información. Los riesgos a los que están expuestos los activos de información son los ataques externos, errores humanos, desastres naturales y situaciones extraordinarias.
- Las **amenazas y fuentes de amenazas** más comunes son las amenazas persistentes avanzadas, *malware*, ingeniería social, *botnet*, redes sociales y servicios en la nube.
- Una de las **medidas preventivas** que se pueden tomar para reducir los riesgos es realizar un **análisis de riesgos** que consta de seis fases: definir el alcance, identificar y valorar los activos de información, identificar las amenazas, averiguar las vulnerabilidades y las fortalezas de los activos; obtener la probabilidad de que suceda una amenaza y el impacto que conllevaría en el negocio; y, por último, tratar los riesgos.

CONCLUSIONES

Aspectos básicos de ciberseguridad

- Un ***hacker*** es aquella persona que trata de solventar, paliar o informar sobre los problemas de seguridad encontrados en programas, servicios, plataformas o herramientas. Como un ejemplo de *hacker*, destaca el *White Hat*. Sin embargo, un **ciberdelincuente** es la persona que buscará sacar beneficio de estos problemas o fallos de seguridad utilizando, para ello, distintas técnicas, como es la ingeniería social o el *malware*.
- Existen 3 tipos diferentes de ciberdelincuentes, *White Hat, Black Hat y Grey Hat*, aunque también existen subtipos de estos, como el *Blue Hat*, *Hacktivistas* y el *Green Hat* o «*newbies*».
- Un **«ciberdelito» o delito informático** hace referencia a la actividad ilícita que se realizan a través de Internet o mediante el uso de herramientas tecnológicas, ya sean ordenadores, teléfonos móviles, etc.

CONCLUSIONES

Aspectos básicos de ciberseguridad

- El término de «**ciberataque**» hace referencia a aquellas acciones que están dirigidas contra los sistemas de información digitales, con la finalidad y objetivo de perjudicar a personas, instituciones u organizaciones, robar información u obtener un beneficio económico.
- El **ciclo de vida de un ciberataque** o «*cyber kill chain*», consta de siete etapas o fases: reconocimiento, preparación, distribución, explotación, instalación, comando y control y acciones sobre los objetivos.
- **No existen dos ciberataques exactamente iguales**, aunque los más comunes son *malware*, *ransomware*, *phishing*, *vishing* y *smishing*, ataques a contraseñas por fuerza bruta o por diccionario, *fuzzing*, *Man in the Middle*, DoS, DDoS, EDoS, inyección SQL, *Cross-Site Scripting* (XSS) y ataques *zero-day*, entre otros.

CONCLUSIONES

Aspectos básicos de ciberseguridad

- La **industria 4.0** se caracteriza por introducir en la ingeniería industrial los avances de las tecnologías de la información, digitalizando la producción y distribución para conseguir una cadena de suministro inteligente, digitalizada y conectada.
- La **ciberseguridad industrial** aúna diferentes principios de seguridad de los entornos OT (Tecnologías de las Operaciones) y principios de seguridad de los entornos IT (Tecnologías de la Información), con el fin de proteger los distintos activos de una industria, así como las redes, los procesos existentes y los datos e información. Mientras que en los entornos IT, prima la confidencialidad, en el caso de los entornos OT, la prioridad es la disponibilidad.
- Las **principales causas de ataques a los entornos OT** vienen dadas por la falta de visibilidad de los activos, la mala segregación de entornos, la ausencia de sistemas de protección, la ausencia de políticas y la existencia de vulnerabilidades y amenazas.

CONCLUSIONES

Aspectos básicos de ciberseguridad

- La **segregación o segmentación de redes** consiste en dividir la red en subredes más pequeñas y controlables, limitando así la posibilidad de propagación de un ataque.
- El uso de **antivirus** y ***softwares* legales** previenen, protegen y eliminan numerosos *softwares* maliciosos. Los ***firewall*** o cortafuegos se encargan de analizar el tráfico existente en la Red, reconocer a los usuarios autorizados y restringir el acceso de aquellos que no lo están, es decir, se trata de un sistema que previene y protege la Red de intrusiones o ataques, bloqueando su acceso. Un **IDS** alerta de las intrusiones que se producen (aunque algunos también permiten realizar ciertas acciones adicionales), mientras que un **IPS,** abarca las mismas funciones que un IDS y además permite realizar ciertas funciones de prevención o bloqueo contra intrusiones.

CONCLUSIONES

Aspectos básicos de ciberseguridad

- Otras medidas que los usuarios pueden tomar es el uso de contraseñas seguras, el acceso a páginas web de confianza y seguras, realizar copias de seguridad, limitar el acceso a la información o proteger el correo electrónico y aquellos dispositivos que sea posible con doble factor de autenticación.

REFERENCIAS

- Ciberseguridad, seguridad informática y seguridad de la información.
  https://www.lisainstitute.com/blogs/blog/diferencia-ciberseguridad-seguridad-informatica-seguridad-información

- Amenazas y vulnerabilidades.
  https://www.incibe.es/protege-tu-empresa/blog/amenaza-vs-vulnerabilidad-sabes-se-diferencian

- Diferencias entre los tipos de ciberataque.
  https://www.ciberseguridad.guiaburros.es/descubre-diferencias-entre-ciberdelito-ciberataque

- Panorama actual de la ciberseguridad en España.
  https://www.ospi.es/export/sites/ospi/documents/documentos/Seguridad-y-privacidad/Google_Panorama-actual-de-la-ciberseguridad-en-Espana.pdf

- Ciclo de vida de un ciberataque.
  https://www.incibe.es/protege-tu-empresa/blog/las-7-fases-ciberataque-las-conoces

REFERENCIAS COMPLEMENTARIAS

[1] Una aseguradora sufrió un ciberataque *ransomware* en 2020.
https://www.businessinsider.es/fue-ciberataque-mapfre-minuto-minuto-aepd-835893

[2] Aprende ciberseguridad: glosario de ciberataques.
https://www.incibe.es/aprendeciberseguridad

[3] Oficina de Seguridad del Internauta: conceptos básicos de ciberseguridad.
https://www.osi.es/es/actualidad/blog/2021/06/28/conceptos-basicos-de-ciberseguridad-que-debes-conocer

[4] Protege tu empresa: glosario de ciberseguridad.
https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_glosario_ciberseguridad_metad.pdf

REFERENCIAS COMPLEMENTARIAS

[5] Una organización sufrió un ciberataque y los datos han sido publicados en Internet. https://www.incibe-cert.es/alerta-temprana/bitacora-ciberseguridad/comprometida-privacidad-millones-cuentas-usuario-facebook

[6] La erupción del volcán de la Palma provocó la pérdida de infraestructuras, sistemas e información. https://elpais.com/sociedad/2021-10-12/la-lava-atraviesa-un-poligono-industrial-son-todo-negocios-de-gente-de-aqui-que-puede-que-se-queden-sin-nada.html

[7] El *malware.* https://ayudaleyprotecciondatos.es/2021/04/12/adware/#Fireball

[8] La ingeniería social. https://www.incibe.es/protege-tu-empresa/blog/historias-reales-instagram-busca-cuenta-perdida

REFERENCIAS COMPLEMENTARIAS

[9] Las Amenazas Persistentes Avanzadas o APT (*Advanced Persistent Threats*).
https://blogs.protegerse.com/2020/07/10/diez-anos-despues-de-stuxnet-vuelven-las-sospechas-de-un-nuevo-ciberataque-a-iran/

[10] *Las botnets.*
https://www.bbc.com/mundo/noticias-55836181

[11] Las reacciones de las grandes empresas a sus crisis reputacionales.
https://www.apd.es/crisis-de-reputacion-mal-gestionadas/

[12] El sector sanitario y la privacidad de los datos de los pacientes.
https://www.incibe.es/protege-tu-empresa/blog/historias-reales-comprometi-seguridad-mi-empresa-y-mis-pacientes-darme

REFERENCIAS COMPLEMENTARIAS

[13] Uso de códigos QR: aumento de los fraudes y robos de datos.
https://www.incibe.es/protege-tu-empresa/blog/historias-reales-comprometi-seguridad-mi-empresa-y-mis-pacientes-darme

[14] El *hacktivismo.*
https://www.lisainstitute.com/blogs/blog/hacktivismo-definicion-tipos-modus-operandi-motivaciones

[15] Guía de ciberataques OSI.
https://www.osi.es/sites/default/files/docs/guia-ciberataques/osi-guia-ciberataques.pdf

[16] Spyware Darkhotel.
https://www.kaspersky.es/resource-center/threats/darkhotel-malware-virus-threat-definition

REFERENCIAS COMPLEMENTARIAS

[17] Ataques de *smishing* a través de SMS.
https://www.eleconomista.es/actualidad/noticias/11382643/09/21/Regresa-la-estafa-del-SMS-de-Correos-asi-intentan-robarte-tus-datos-o-introducir-un-virus.html

[18] Campaña de *smishing.*
https://www.osi.es/es/actualidad/avisos/2021/12/detectada-nueva-estrategia-de-estafa-traves-de-bizum-solicitando-dinero-en

[19] El método MiTM.
https://www.diariodenavarra.es/noticias/navarra/2020/07/27/estafan-180-000-una-empresa-navarra-con-metodo-man-the-middle-697293-300.html

[20] Ataques de Denegación de Servicio Distribuido (DDoS).
https://www.cloudflare.com/es-es/learning/ddos/famous-ddos-attacks/

REFERENCIAS COMPLEMENTARIAS

[21] Una filtración de la base de datos expuso los nombres y contraseñas de 1.200 clientes.
https://es.frwiki.wiki/wiki/Qatar_National_Bank#Fuite_d%E2%80%99informations_confidentielles_de_2016

[22] Las contraseñas más utilizadas.
https://nordpass.com/es/most-common-passwords-list/

[23] Microsoft alertó de múltiples *exploits zero-day.*
https://www.incibe-cert.es/alerta-temprana/bitacora-ciberseguridad/microsoft-alerta-ciberdelincuentes-apoyados-gobierno

[24] En los coches inteligentes: ciberseguridad y reducción de riesgos.
https://www.infoplc.net/plus-plus/mercado/item/110401-trend-micro-riesgo-coche-conectado-wp-29

REFERENCIAS COMPLEMENTARIAS

[25] Ciberataque a una fábrica de acero alemana.
https://www.incibe-cert.es/alerta-temprana/bitacora-ciberseguridad/fabrica-acero-alemana-ataque

[26] *Ransomware* WannaCry.
https://www.incibe-cert.es/blog/ransomware-wannacry-responsable-ciberataque-mundial

[27] Darskside al oleoducto Colonial Pipeline.
https://www.incibe-cert.es/alerta-temprana/bitacora-ciberseguridad/interrupcion-el-suministro-del-oleoducto-colonial-pipeline

[28] Darkside pudo acceder a los sistemas a través de una contraseña comprometida de un empleado.
https://www.kaspersky.es/blog/pipeline-ransomware-mitigation/25302/

¡GRACIAS!

GOBIERNO DE ESPAÑA
VICEPRESIDENCIA PRIMERA DEL GOBIERNO
MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL
SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

017