



INDUSTRIA 4.0

CIBERSEGURIDAD INDUSTRIAL



Contenido

Ciberseguridad y la Industria 4.0.....	3
¿Qué es la Ciberseguridad?.....	3
Principios fundamentales de la Ciberseguridad	4
Principales diferencias entre Ciberseguridad y seguridad de la información.....	6
Norma estándar de ciberseguridad ISO/IEC 27032	7
Infraestructuras Críticas.....	8
Ciclo de vida de la Ciberseguridad	9
Prevención.....	10
Detección.....	10
Respuesta	11
Inteligencia	12
Ciberataques: Herramientas utilizadas por los atacantes	13
La Ciber-resiliencia.....	15
Los Ciber-riesgos.....	15
La necesidad de un seguro de Ciber-riesgos en la empresa	16
La Ciberseguridad en la empresa y la empresa ante la Ciberseguridad.....	17
La Ciberseguridad y la Inteligencia Artificial.....	18
Tendencias de Ciberseguridad en tecnología.....	19
Otras tecnologías de impacto en el futuro de la Ciberseguridad.....	19
El futuro de la Ciberseguridad.....	19
Ciberseguridad 4.0.....	20



Ciberseguridad y la Industria 4.0

La Industria 4.0 está impulsando los procesos de digitalización de sistemas y procesos industriales. La transformación digital de las empresas y organizaciones con la integración de las nuevas tendencias tecnológicas como Big Data, Cloud Computing (la Nube) e



Internet de las Cosas –como pilares nucleares– junto con la movilidad y medios sociales –ya integrados en la sociedad– están produciendo el advenimiento de la Cuarta Revolución Industrial.

Por estas razones, dedicamos esta unidad específica a la ciberseguridad desde una visión global, pero analizando con detalle su estado del arte y el futuro previsible con referencias concretas a España, Latinoamérica y el Caribe, junto con un análisis detallado de sus principios fundamentales, así como los factores más importantes de las ciberamenazas y las herramientas utilizadas por los ciberatacantes, junto con la necesidad de una concienciación de empleados y ciudadanos en general ante la ciberseguridad de organizaciones y empresas.

¿Qué es la Ciberseguridad?

«La ciberseguridad es el conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los



activos de la organización y los usuarios en el ciber-entorno. Los activos de la organización y los usuarios son los dispositivos informáticos conectados, los



usuarios, los servicios/aplicaciones, los sistemas de comunicaciones, las comunicaciones multimedios, y la totalidad de la información transmitida y/o almacenada en el ciber-entorno. La ciberseguridad garantiza que se alcancen y mantengan las propiedades de seguridad de los activos de la organización y los usuarios contra los riesgos de seguridad correspondientes en el ciber-entorno. Las propiedades de seguridad incluyen una o más de las siguientes:

- confidencialidad;
- integridad, que puede incluir la autenticidad y el no repudio;
- disponibilidad»

Las propiedades de seguridad, confidencialidad, integridad y disponibilidad, se conocen como la triada de la seguridad de la información, CID (CIA, en inglés: confidentiality, integrity, availability), las cuales describiremos con mayor detalle más adelante.

Principios fundamentales de la Ciberseguridad

Los principios o propiedades de la ciberseguridad son la triada de la seguridad y algunos más que comentamos a continuación.

Confidencialidad. Protección de la información contra el acceso no autorizado o la divulgación. Dependiendo del tipo de información manejada, se puede requerir un mayor grado de confidencialidad; ésta se refiere –esencialmente– a la propiedad intelectual, cobertura de canales de comunicación, cifrado(encriptación) e inferencia y control de acceso.

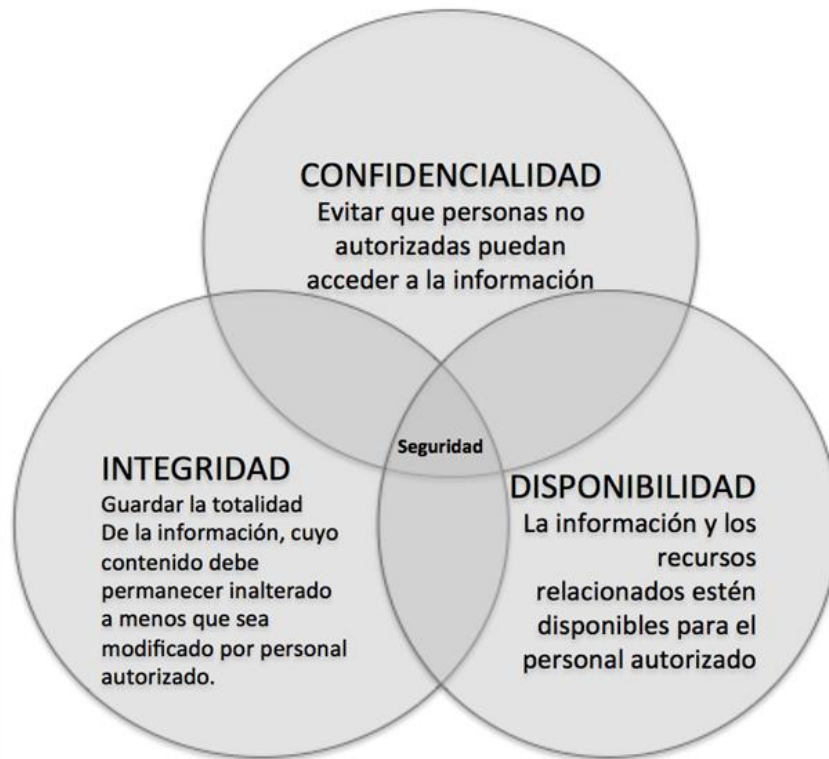
Integridad. Protección de la información contra modificaciones no autorizadas, ya sea por personal o por procesos. La integridad debe aplicarse, por extensión, al software y a las configuraciones. Los datos han de ser consistentes tanto interna como externamente entre todas las entidades intervinientes y el mundo exterior. La integridad de los servicios de información se puede controlar mediante registros y controles de acceso, firma digital, resúmenes criptográficos y cifrado.



Disponibilidad. Asegura el acceso confiable y a tiempo, al uso de los datos de los sistemas de cómputo. La disponibilidad garantiza que los sistemas funcionen adecuadamente cuando se necesiten y debe incluir salvaguardas para asegurarse de que los datos no se pueden eliminar en forma accidental o malintencionada. Un ataque de denegación de servicios (DoS) es un ejemplo de una amenaza frente a la disponibilidad. Ésta se puede proteger mediante copias de seguridad, controles de acceso y redundancia.

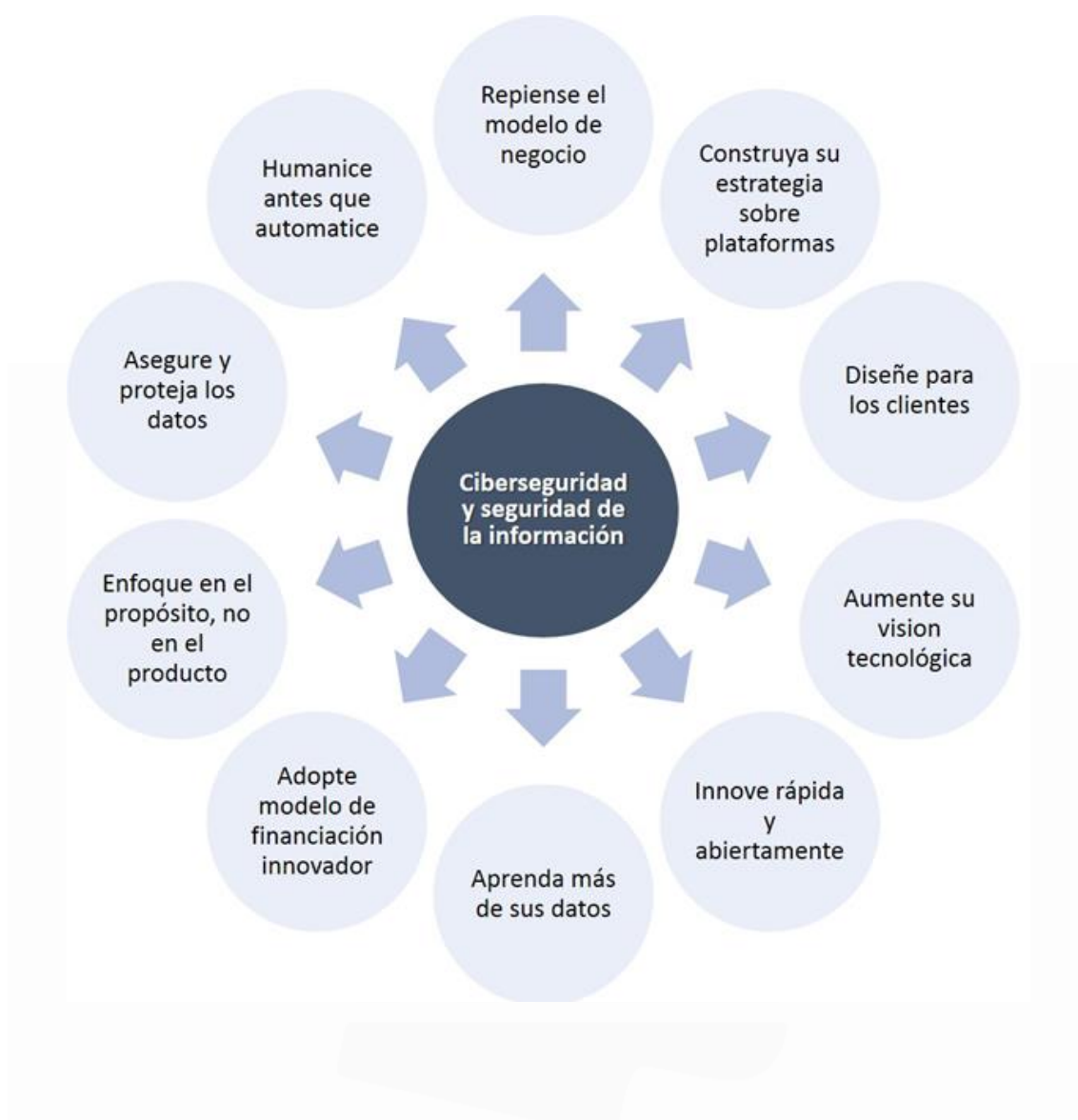
Otras propiedades. La ciberseguridad requiere también otras propiedades, como: autenticación (comprobación de la evidencia de la identidad del usuario), autorización (derechos y privilegios garantizados a una persona o proceso que facilita el acceso a los recursos de computación y activos de información), auditoría (se necesita mantener el aseguramiento operacional y las organizaciones requieren sistemas de auditoría y monitorización), contabilidad (responsabilidad) (capacidad para determinar las acciones y comportamiento de un individuo en un sistema y la identificación de ese individuo) y no repudio.

La contabilidad está relacionada con la propiedad de no repudio (nonrepudiation). No repudio se refiere al aseguramiento de que los mensajes e información sean originales y que la integridad de los datos ha sido protegida. También se garantiza que la parte emisora o receptora no puede negar o repudiar que enviaron o recibieron el mensaje o información. El no repudio se garantiza a través de firmas digitales y registro de transacciones.



Principales diferencias entre Ciberseguridad y seguridad de la información

En primer lugar, resaltamos que la seguridad de la información tiene un alcance mayor que la ciberseguridad, puesto que la primera busca proteger la información de riesgos que puedan afectarla, en sus diferentes formas y estados. Por el contrario, la ciberseguridad se enfoca principalmente en la información en formato digital y los sistemas interconectados que la procesan, almacenan o transmiten, por lo que tiene un mayor acercamiento con la seguridad informática.



Norma estándar de ciberseguridad ISO/IEC 27032

En octubre de 2012, la Organización Internacional de Normalización (ISO, por sus siglas en inglés) anunció la creación del estándar ISO/IEC 27032 para la ciberseguridad. La organización explicó en su presentación oficial, que pretende garantizar la seguridad en los intercambios de información en la Red con este nuevo estándar, que puede ayudar a combatir el cibercrimen con cooperación y coordinación. Concretamente, proporciona un marco seguro para el intercambio de información, el manejo de incidentes y la coordinación para hacer más seguros los procesos. «La norma (ISO/IEC 27032) facilita la colaboración segura y fiable para



proteger la privacidad de las personas en todo el mundo. Pretende ayudar a prepararse, detectar, monitorizar y responder a los ataques de ingeniería social, hackers, malware, spyware y otros tipos de software no deseado.»

Infraestructuras Críticas

La cuarta revolución industrial auspiciada por las tecnologías facilitadoras de Industria 4.0 se enfrentan a un gran reto: la protección de infraestructuras críticas, claves en las fábricas inteligentes y en la transformación digital de organizaciones y empresas.

Las infraestructuras críticas son muy numerosas y cada país tiene reconocidas un conjunto determinado acordes con su estructura física, pero en general se pueden considerar al menos las siguientes:

Transporte. Aeropuertos, puertos, ferrocarriles, redes de transporte público, sistemas de control de tráfico...

- Centrales y redes de energía (hidráulica, eléctrica, térmica, nuclear, solar...)
- Embalses de agua y su almacenamiento, tratamiento, redes...
- Centros comerciales
- Instituciones deportivas
- Hospitales

La mayoría de estas instalaciones están controladas por sistemas industriales de control y supervisión (Industrial Control Systems, ICS) que permiten supervisar y gestionar el funcionamiento de instalaciones industriales. El sistema clásico y más conocido y utilizado es SCADA, que se compone de:

- Sensores, actuadores, controladores y medidores
- Interfaces humanos con las máquinas
- Comunicaciones (líneas, protocolos, interfaces...)
- Controladores lógicos programables (PLC)



- Dispositivos electrónicos inteligentes

Los ataques más peligrosos sobre infraestructuras críticas son:

- Incendio de centros de datos
- Acceso no autorizado a información digitalizada
- Denegación de servicio, DDoS
- Robo de equipamiento, credenciales, datos...
- Suplantación de identidad (credenciales digitales).



Ciclo de vida de la Ciberseguridad

La ciberseguridad debe ser considerada como un proceso y no una actividad aislada y diferenciada del resto de los servicios o herramientas informáticas. La organización debe ser capaz de prevenir y reaccionar antes los ciberataques generando las medidas necesarias para mantener su estado ordinario.



La ciberseguridad, según Telefónica, consta de las siguientes etapas:

- Prevención
- Detección
- Respuesta (reacción)

Prevención

Es necesario que la empresa y sus trabajadores, estén informados de la evolución de las amenazas, de las posibles etapas y de qué soluciones existen contra ellas. Se requiere formación constante en la prevención y adquirir una serie de conocimientos sobre seguridad que han de ponerse en marcha. También se necesita conocer el funcionamiento de las herramientas o productos de seguridad, así como sus características para obtener la protección más efectiva. Se requiere también la protección física de las instalaciones para garantizar que nadie sin autorización pueda manipular los terminales, los accesos a la red o conectar dispositivos no autorizados. La prevención tiene tres procesos críticos:

- Control de accesos y gestión de identidades.
- Prevención de fuga de datos.
- Seguridad de red.

Detección

La detección de incidencias es clave en el proceso y puede ocurrir mientras se está produciendo el ataque o pasado un tiempo de haber ocurrido. La detección de un ataque o amenaza en tiempo real suele producirse gracias a la detección de malware por parte de un antivirus. Si no se detecta en el momento que sucede el ciberataque, los problemas aumentan porque los hackers disponen de más tiempo para actuar libremente.

Las herramientas de ciberseguridad modernas realizan de modo eficaz la detección de patrones de ataque conocidos. El gran problema se produce cuando se realizan



ciberataques con patrones desconocidos y la detección no se ha producido en tiempo real, sino tras un largo periodo.

La detección proactiva es el mejor método a emplear. Las acciones a realizar para la detección son:

- Gestión de vulnerabilidades.
- Monitorización continua.

Se necesita un plan de gestión de vulnerabilidades que contemple una monitorización continua de los sistemas informáticos de la empresa u organización.

Respuesta

Se ha producido un ataque y los sistemas se han visto infectados; es necesario dar una respuesta técnica y, si se ha producido un robo de identidad o robo de datos, acudir a las fuerzas y cuerpos de seguridad del Estado e iniciar acciones legales para luchar contra los delitos que se hayan podido cometer. La metodología de Telefónica¹³ contempla los siguientes pasos a seguir ante un ciberataque:

- Desconectar el equipo de internet
- Instalar un equipo antivirus
- Realizar un análisis completo del sistema.
- Modificar las contraseñas.
- Limpieza manual

Se necesitan tomar acciones legales ante un ataque informático, un robo de datos o una suplantación de identidad en Internet. La respuesta ante los ciberataques tanto técnica como jurídica, ha de ser lo más ágil posible y requiere: los sistemas de recuperación que existen y la recolección de evidencias digitales que permiten emprender acciones legales contra los atacantes y cumplimiento con la regulación.



Inteligencia

Se necesita inteligencia para dotar de eficiencia a las medidas de ciberseguridad. Las amenazas afectan a todos los estados, a las empresas y organizaciones, y a los ciudadanos. Se requiere la compartición de información y su análisis eficiente. Esta situación demanda la colaboración público-privada:

- Los cuerpos y fuerzas de seguridad de los Estados.
- Entidades y empresas del mundo de la ciberseguridad.
- Empresas y organizaciones de la sociedad civil.

La colaboración entre los agentes mejora la información y permite dotar de mayor inteligencia a los sistemas de ciberseguridad. Las acciones a realizar son:

1. Análisis de la información proveniente de fuentes diversas y búsquedas de correlación.
2. Fuentes de datos abiertas (OSINT- Open Source Intelligence).
3. Perfiles de usuario (creación y gestión) y atribución.
4. Compartición de datos de incidentes entre corporaciones.
5. Diversidad de estándares





Ciberataques: Herramientas utilizadas por los atacantes


Los ciberataques se realizan con técnicas y herramientas, algunas de propósito general y otras diseñadas para conseguir sus objetivos finales. Las técnicas y herramientas son muy numerosas, desde los primitivos virus, spam... hasta los más empleados en la actualidad y que se prevén para el futuro como son los ataques DDoS, malware, ransomware, etc. Las tendencias son:

- Herramientas construidas para otros fines (herramientas desarrolladas para otros fines comerciales o de investigación y adaptadas para producir ataques)
- Exploits (herramientas más utilizadas en la actualidad para realizar ataques).
- Código dañino, Ransomware, cryptoware... representan a las herramientas más utilizadas para realizar las infecciones que preceden a los ataques.
- Spam (correo basura), Phishing, Spearphishing
- Botnet (abreviatura de Robot Network). Red de robots o zombies, equipos infectados por un atacante remoto. Los equipos quedan a su merced cuando deseen lanzar un ataque masivo como envío de spam o denegación distribuida de servicios (DDoS).
- Ataques DDoS.
- Ofuscación
- Ingeniería social
- Watering hole
- Librerías JavaScript
- Las macros como vector de ataques
- Routers inalámbricos
- Robos de identidades
- A nivel popular, el término más empleado entre los profesionales de la ciberseguridad es el malware (Malicious Software), código malicioso o en lenguaje coloquial, por extensión los virus, aunque tiene mucha tipología y una gran cantidad de ciberataques. Los más extendidos son:
- Virus
- Gusanos



- Troyanos. Son muy populares y muy extendidos: Backdoors (puertatrasera), Keyloggers, Stealers, Ransomware (uno de los códigos dañinos más extendidos en los años 2015 y 2016 y que los informes de 2017 destacan también como los de mayor penetración).
- Spyware (software espía)
- Adware (software de ataques de publicidad)

TIPOS DE CIBERATAQUES



MALWARE

Es la abreviatura de “Malicious Software” y se trata de programas que dañan los equipos informáticos y/o extraen información de los usuarios sin que éstos consientan su autorización.

SPYWARE

Es un software espía que recopila información de un ordenador sin conocimiento de su propietario y la transfiere a otros dispositivos.

DDOS

Ataques a webs que provocan su colapso y la denegación de servicio a los clientes.

TROYANOS

Son programas que al ejecutarlos permiten un acceso remoto al equipo infectado.

PHISHING

Se trata de emails que suplantán la identidad de un servicio o compañía, por ejemplo, de una entidad bancaria, solicitando datos confidenciales del usuario para usarlos en beneficio propio.

RANSOMWARE

“Ransom” significa “rescate” en inglés, por lo tanto, es un tipo de programa que restringe el acceso a determinados archivos y pide un rescate para liberar esta información.



La Ciber-resiliencia

La resiliencia (en inglés resilience) es un término muy utilizado a nivel de organizaciones y empresas, y que en los últimos años se ha extendido al campo de la ciberseguridad, donde algunos utilizan el término ciber resiliencia.

El término ha llegado al campo de la ciberseguridad y se utiliza indistintamente como resiliencia y como ciber resiliencia. El glosario de términos del CCN-CERT de España, define la resiliencia como: «Capacidad de los sistemas para seguir operando pese a estar sometidos a un ciberataque, aunque sea en un estado degradado o debilitado. Así mismo incluye la capacidad de restaurar con presteza sus funciones esenciales después de un ataque»

Las vulnerabilidades de software seguían constituyendo el elemento más problemático y afectaron a los grandes fabricantes de software. Además de los productos de software también afectaron a: firmware, hardware, usuarios, servicios en la nube, tecnología criptográfica, protocolos de internet, comunicaciones y dispositivos móviles y apps móviles, y sistemas de control industrial. Según el CCN-CERT en 2015, las medidas que han contribuido de manera más significativa a aumentar la resiliencia de los sistemas de información sobre los que se aplican y, en consecuencia, de las organizaciones afectadas, se dividen en grandes grupos: medidas no técnicas (prevención, detección, respuesta) y técnicas (organizativas, formativas y jurídicas), y desde un punto de vista organizativo enumera las más importantes adoptadas: personales, tecnológicas y regulatorias.

Los Ciber-riesgos

Las amenazas (ciberamenazas o ciberriesgos) son cada vez más frecuentes y avanzadas, por lo que gestionar una crisis cibernética es algo más que probable: los ataques de denegación de servicio distribuidos (DDoS), el robo de credenciales mediante técnicas de phishing o malware, la fuga masiva de información digital, el ransomware²²(programas que impiden el acceso a la información mediante



técnicas de cifrado, pidiendo un rescate para el descifrado), o las amenazas avanzadas persistentes (APT, Advanced Persistent Threats).

Los hackers, sin duda, nunca descansan. Un ciberataque muy sonado realizado en agosto de 2015 fue el robo de datos de clientes de la página web de contactos Ashley Madison, que durante las siguientes semanas trajo de cabeza no sólo a la compañía, sino también a sus 37 millones de usuarios.



La necesidad de un seguro de Ciber-riesgos en la empresa

los ciberriesgos han pasado a ser uno de los principales focos de atención de los gerentes de riesgos de las empresas, de cualquier tamaño y sector. Ello ha obligado al estudio y posible implantación de un seguro de ciberriesgos al igual que cualesquiera otros riesgos relevantes en las empresas y en cualquier industria.

Un informe de Allianz Global 24 sobre ciberseguridad, dado a conocer el 8 de septiembre de 2015, señalaba que las primas mundiales de seguros cibernéticos superarán los 20.000 millones de dólares en la próxima década frente a los 2.000 millones que capta en la actualidad. El aumento de este negocio se producirá por una mayor concienciación sobre estos riesgos y por los cambios



normativos que propician la contratación de esta cobertura asegurada por parte de las empresas, señala el citado estudio. En la actualidad menos del 10% de las empresas suscriben una póliza para cubrirse de los riesgos cibernéticos. La “ciberdelincuencia” cuesta 445.000 millones de dólares anuales a la economía mundial y la mitad de este importe recae en las diez principales economías mundiales (Estados Unidos con 108.000 millones lidera la clasificación, seguida de China con 60.000 millones y Alemania con 59.000 millones).

Los expertos recomiendan a las compañías que además de ser innovadoras en tecnología y atención al cliente, deberían hacer una inversión especial en ciberseguridad, tanto en protección como en la respuesta a los ataques de los hackers ya que los datos que manejan a diario son un material sensible por contener información personal de sus clientes.



La Ciberseguridad en la empresa y la empresa ante la Ciberseguridad

El Decálogo de Ciberseguridad es el siguiente:

1. Analizar los riesgos
2. Los responsables de seguridad
3. Seguridad en el proyecto de trabajo



4. La protección de la información
5. Movilidad con seguridad
6. Protección antimalware
7. Actualización y parcheo
8. La seguridad de la red
9. Monitorización
10. Seguridad gestionada

La Ciberseguridad y la Inteligencia Artificial

La inteligencia artificial desde el advenimiento de Big Data está llegando a numerosos sectores que hasta hace unos años prácticamente era impredecible y que en la actualidad están impactando en la ciberseguridad de las organizaciones y empresas.

El conocimiento en la inteligencia artificial integrada con Big Data está ayudando y ayudarán a los delitos informáticos. Una nueva generación de plataformas de negocio está surgiendo en la convergencia del aprendizaje automático (Machine Learning) y –recientemente el aprendizaje profundo (Deep learning)– y Big Data que generará un gran cambio en materia de ciberseguridad. Los algoritmos de aprendizaje automático y la ciber inteligencia asociada están potenciando las predicciones de ataques cibernéticos que mejorarán las tasas de detección y pueden ser la clave para revertir la tendencia actual en cuanto acrecimiento de delitos cibernéticos y potenciar la ciberseguridad.

Numerosas empresas especializadas en ciberseguridad han lanzado iniciativas para integrar soluciones de inteligencia artificial en sus sistemas de ciberseguridad. Estudiaremos dos casos significativos: IBM con su computador cognitivo Watson (ver unidad anterior) y Accenture -una de las grandes consultoras a nivel mundial.



Tendencias de Ciberseguridad en tecnología

Se resalta la conexión y ubicuidad de los datos basados en Internet de las Cosas, Cloud Computing, dando lugar a la creación de redes y ciudades inteligentes donde el Big Data es un elemento esencial, y las tendencias TIC que recomienda son:

- Big Data, Cloud Computing e Internet de las Cosas (IoT)
- Smart Cities y Smart Grids
- Industria 4.0
- Redes sociales
- Tecnologías cognitivas (que incluyen aprendizaje automático, procesamiento en lenguaje natural “NLP” y reconocimiento de voz)
- Sistemas ciberfísicos (incluyendo el uso de drones, redes de sensores y realidad aumentada)
- Tecnologías móviles, WiFi óptico y Redes 5G
- Nuevos modelos de pago

Otras tecnologías de impacto en el futuro de la Ciberseguridad

En capítulos anteriores también hemos considerado otras tecnologías de gran impacto en el ámbito de la ciberseguridad:

- Tecnologías financieras: Fintech y Blockchain,
- Robots colaborativos (Cobots), Bots y Chatbots (bots conversacionales),
- Aprendizaje profundo (Deep Learning). Una tecnología cognitiva de inteligencia artificial, y un tipo específico de gran impacto del aprendizaje automático (Machine Learning).

El futuro de la Ciberseguridad

Las tendencias del sector de seguridad de la información y ciberseguridad se centran en servicios en la nube, Big Data & Analytics, internet de las cosas (con todos sus



pilares fundamentales: sensores, redes inteligentes –contadores y medidores inteligentes–, drones –especialmente inteligentes y programables) y todas las tecnologías asociadas a Industria 4.0. Se requieren herramientas y soluciones que se centren en elementos como la vulnerabilidad de la empresa, la auditoría de TI y el hacking ético (especialistas en seguridad informática y ciberseguridad que permitan conocer y comprobar el grado de vulnerabilidad tecnológica de las organizaciones y empresas y que dispongan no sólo de los conocimientos informáticos adecuados, sino que estén dotados de herramientas que les ayuden a prevenir potenciales ataques).

Ciberseguridad 4.0

Nos encontramos al comienzo de la Cuarta Revolución Industrial como consecuencia del advenimiento de la tendencia Industria 4.0, y en los inicios de una nueva era tecnológica y social que obligará a todas las organizaciones y empresas a afrontar su transformación digital para implementar una Ciberseguridad 4.0, como una nueva era de la ciberseguridad que consideramos traerá grandes retos y oportunidades para afrontar con éxito las ciberamenazas, ciberataque, ciberdelitos y ciberriesgos del futuro.

Autor: Mg. Ing. Federico D'Alía

Bibliografía de referencia: Industria 4.0, Luis Joyanes 2017