PROFESIONES → DIGITALES

ciberseguridad

Protegiendo la información vulnerable

Telefónica FUNDACIÓN

NEWTON LEE

INFORMÁTICO Y ESCRITOR

A medida que el mundo está cada vez más interconectado, todos compartimos la responsabilidad de hacer el ciberespacio seguro

→ CIBERATAQUES POTENTES

A finales de 2014, un grupo de *hackers* autodenominado **#GOP** consiguió acceder a la intranet de **Sony Pictures** y robó numerosa información, desde contraseñas hasta archivos y documentos internos de la compañía, además de obtener acceso anticipado a varias películas que aún no habían sido estrenadas en cartelera.

Quedas con alguien a través de WhatsApp, mantienes una conversación por videoconferencia a través de Skype, muestras las fotos de tus vacaciones en Facebook, aprendes gracias a un tutorial de YouTube, compras online a través de Amazon, pagas en una tienda física con el teléfono móvil... No hay duda de que ya vivimos en una sociedad digital. Cada vez es mayor la parte de nuestra vida que volcamos en las redes para trabajar, divertirnos, formarnos o relacionarnos con otras personas. Ya no es concebible que una empresa o institución viva de espaldas a internet, y no solo debe tener presencia allí, sino convertirlo en un canal para desarrollar su actividad e interactuar con sus grupos de interés.

Un mundo más tecnológico tiene innumerables ventajas y puede mejorar sobremanera la vida de las personas y el funcionamiento de las organizaciones. Pero al igual que en el mundo físico, en donde nos pueden robar la cartera o forzar la puerta de nuestra vivienda, en la red existen numerosas amenazas relacionadas con conductas delictivas. Desde la simple introducción de *malware* en ordenadores personales, hasta el robo de contraseñas y la suplantación de identidad; desde robar información sensible a las empresas, hasta derribar los servidores corporativos mediante millones de peticiones de conexión simultáneas realizadas por ejércitos de dispositivos *zombis*. Los ataques suelen perseguir el robo, alteración o destrucción de información, la extorsión a los usuarios o el boicot del negocio llevado a cabo por una empresa.

Se conoce como ciberseguridad la práctica basada en proteger los sistemas informáticos, las redes y los programas de ataques digitales. En general, en una organización se trata de una estrategia que implica a las personas, los procesos y la tecnología para crear múltiples capas de protección ante los ciberataques.

BRUCE SCHNEIER

CRIPTÓGRAFO Y EXPERTO EN SEGURIDAD INFORMÁTICA

El hardware es fácil de proteger: lo encierras bajo llave en una habitación, lo encadenas a una mesa o compras uno de repuesto. La información plantea más problema. Puede existir en más de un lugar, ser transportada a través de medio planeta en segundos y ser robada sin que te enteres

DE LA SERIE DE TELEVISIÓN MR. ROBOT

Nunca me ha costado hackear a la mayoría de la gente. Si les escuchas, si les observas, sus vulnerabilidades son como una señal de neón atornillada a sus cabezas

la seguridad está en nuestras manos

Nuestra actividad en la red configura nuestra identidad digital, que está compuesta por el rastro de datos que vamos dejando mientras navegamos y utilizamos servicios online. La formulación de la identidad digital de una persona depende en gran medida del entorno en el que se va a utilizar. Por ejemplo, la información que requiere el centro médico al que acudimos con una dolencia es distinta a la que demanda Amazon para validar una compra.

El grado de seguridad y privacidad que debe proteger nuestra información personal depende de la sensibilidad de la misma y de si la ofrecemos de forma voluntaria o forzada. Por ejemplo, comentar de forma neutral en una red social es un contenido que aportamos de forma voluntaria y no constituye información especialmente sensible, por lo que no requiere un control especial. En el caso de que esa información poco sensible se le exija al usuario de forma forzada, como puede ser el tener que darse de alta como usuario para poder comentar en un blog, se le debe garantizar por lo menos el derecho al anonimato.

Cuando la información que vertemos en las redes es de carácter sensible, entramos en terrenos que exigen más control. En el caso de que la ofrezcamos voluntariamente, ese control y la obligación de estar informados sobre los peligros que ello conlleva recae sobre nosotros, algo que ocurre al subir fotos personales y de niños a redes sociales públicas. Si nuestra información se nos exige, entonces debemos asegurarnos de que el proveedor del servicio es de absoluta confianza, y conocer las condiciones de prestación del mismo.

El catálogo de amenazas que acechan en las redes al usuario es tan grande como la imaginación de los ciberdelincuentes, pero se pueden destacar las siguientes:

- Introducir *malware* (programas maliciosos) en ordenadores y dispositivos.
- Tomar el control de un ordenador para utilizar su capacidad de procesamiento para realizar tareas que requieren gran poder de computación o para lanzar ataques masivos desde una *botnet* (red de robots informáticos).
- *Phishing*, suplantar la identidad de una empresa u organización para intentar recabar información confidencial del usuario. Por ejemplo, una web que se hace pasar por nuestro banco y nos pide las contraseñas de nuestras cuentas.
- Robos económicos, accediendo online a los recursos financieros del usuario, como las cuentas bancarias, PayPal o bitcoin.
- Robos lúdicos, como fotografías, vídeos u otro material personal guardado en la red.
- Robos de imagen, accediendo al perfil del usuario en redes sociales y actuando de una forma que dañe su imagen.

CIBERATAQUES POTENTES

En octubre de 2016 tuvo lugar un ataque perpetrado por la red de robots o *botnet* **Mirai** que, infectando dispositivos del internet de las Cosas (IoT) (fundamentalmente cámaras-IP y *routers* domésticos), constituyó una red de dispositivos *zombis* y lanzó un ataque masivo de denegación de servicio distribuido (DDoS) contra la infraestructura de DNS del proveedor de infraestructura Dyn, afectando a usuarios de empresas tan relevantes como Twitter, Amazon, Tumblr, Reddit, Spotify, Paypal y Netflix, denegándoles el acceso.

la empresa vulnerable

ROBERT MUELLER
DIRECTOR DEL FBI

Solamente hay dos tipos de empresas: aquellas que han sido hackeadas y aquellas que lo serán

Las empresas son otro de los objetivos preferidos de los *hackers*. En este caso, los ataques se pueden dirigir hacia la red privada, es decir, los ordenadores donde trabajan los empleados, o hacia las infraestructuras corporativas, como son los servidores, las redes o las bases de datos, entre otros. El objetivo del agresor es o bien robar información sensible de la compañía, o bien dañar sus sistemas informáticos impidiendo el funcionamiento del negocio y dañando su reputación comercial.

→ **CIBERATAQUES POTENTES**

La empresa global de soluciones de información **Equifax** sufrió la que ha sido catalogada como la fuga más grave de datos de la historia, que expuso información sensible de más de 143 millones de personas, incluyendo números de la Seguridad Social, direcciones e información bancaria. Una vulnerabilidad pública del servidor web Apache de la compañía fue la puerta de entrada para los criminales.

Entre las ciberamenazas a las que se enfrentan las empresas y organizaciones, las más frecuentes son:

Ransomware

Es un programa dañino que infecta los ordenadores de la compañía, encriptando la información que contienen y exigiendo un rescate (*ransom*, rescate en inglés) para desencriptarla. El virus *WannaCry*, que afectó en 2017 a muchas empresas de distintos países, es un ejemplo de esta categoría.

Inyección SQL (*SQL injection*)

SQL corresponde a la expresión en inglés *Structured Query Language* (Lenguaje de Consulta Estructurado) que identifica a un tipo de lenguaje vinculado con la gestión de bases de datos de carácter relacional. El método de ciberataque Inyección SQL aprovecha una vulnerabilidad para infiltrar código SQL intruso.

Ataque de día cero (*zero-day attack*)

Aprovecha una vulnerabilidad en una aplicación o sistema, que ha sido detectada por el atacante antes que por el dueño, para introducir código malicioso en el intervalo de tiempo previo a su localización y reparación mediante un parche informático.

Ataque de denegación de servicio (*denial-of-service*, *DoS*) y ataque de denegación de servicio distribuido (*distributed denial-of-service*, *DDoS*)

Consiste en la saturación por exceso de tráfico de los sistemas o redes de las empresas, inutilizándolos. Al desbordar el servidor de red de peticiones, este acaba denegando el servicio, de ahí el nombre de esta práctica delictiva. Se habla de denegación de servicio distribuido (*DDoS*) cuando el ataque se produce simultáneamente desde múltiples puntos, como, por ejemplo, desde una *botnet* o red de robots informáticos.

la innovación beneficia al hacker

→ CIBERATAQUES POTENTES

El ataque de *phising* que millones de usuarios de **Gmail** sufrieron el mes de marzo de 2017 fue tan sofisticado que no solo el correo procedía realmente de un contacto de confianza, sino que el estilo de redacción del mail se asemejaba al del contacto de origen.

El desarrollo tecnológico sin duda pone en manos de los ciberdelincuentes herramientas cada vez más poderosas. Los avances que se producen en campos como la inteligencia artificial, el *big data* o el internet de las cosas (IoT) no hacen sino perfeccionar las técnicas de ataque y extender exponencialmente su capacidad para hacer daño.

En el caso concreto de la inteligencia artificial, el peligro puede venir por tres caminos:

- **Aumentando el número de amenazas existentes**, pues, al abaratarse el coste de realizar un ataque, dado que se automatizan numerosas funciones que antes tenían que realizar los humanos, se incrementa notablemente el número de actores que ahora pueden permitirse llevarlo a cabo.
- **Introduciendo nuevas amenazas**, al posibilitar la inteligencia artificial la realización de tareas que antes eran impracticables para los humanos. Y, por si fuera poco, las máquinas inteligentes permiten analizar las vulnerabilidades de los sistemas informáticos de defensa.
- **Cambiando el carácter de las amenazas**, haciendo más efectivos los ataques, más precisos en alcanzar el objetivo y más difíciles de atribuir a un agente concreto.

Si a esto le sumamos la capacidad del *big data* para procesar volúmenes colosales de información, la situación es aún más alarmante. También pueden producirse nuevos tipos de amenazas que se aprovechen de la capacidad de la inteligencia artificial para analizar el comportamiento humano, los estados de ánimo y las creencias, alimentándola con los millones de datos personales distribuidos por la red. Es más, el análisis de esta ingente cantidad de datos personales puede colaborar en la manipulación social, el engaño y la difusión de propaganda dirigida; por ejemplo, mediante la creación y edición por inteligencia artificial de imágenes de vídeo que parezcan reales.

Por último, el creciente número de dispositivos conectados a las redes, cuya base instalada está previsto que se incremente a razón de un 15 a un 20% anual hasta 2020, convierte la seguridad del internet de las cosas en un factor clave para prevenir amenazas. Muchos de estos dispositivos, especialmente las cámaras y los grabadores de vídeo digital, no resultan difíciles de hackear y pueden ser incorporados a una *botnet*, una red de robots maliciosos, para llevar a cabo ataques del tipo DDoS. Esto fue lo que ocurrió en 2016, cuando un ciberataque contra los servidores del proveedor de servicios DNS Dyn, a través de un gran número de dispositivos IoT hackeados, bloqueó Twitter, Amazon y varias decenas de otros sitios de tráfico intenso.

el ciclo de la ciberseguridad

La ciberseguridad es como la salud de una persona: hay que vigilarla y cuidarla constantemente, no vale con realizar intervenciones esporádicas. Por ello, se habla de un ciclo o un proceso, es decir, una estrategia que se aplica constantemente en todo momento y que contiene distintas fases.

- **Prevención** Requiere una formación continua para conocer las nuevas amenazas que acechan en las redes en cada momento y qué medidas hay que llevar a cabo para evitar poner en peligro la información y los sistemas corporativos.

  Las tareas de prevención incluyen:

  - El control sobre quién accede a los recursos de la empresa y la asignación de permisos y credenciales al personal en función de los roles desempeñados.
  - Establecimiento de medidas técnicas, organizativas y legales para evitar fugas de información de la empresa.
  - Definición de una política de seguridad de la red, que debe ser implementada a través de herramientas de *software* y *hardware* y que debe ser auditada con frecuencia para garantizar su eficacia.

- **Detección** de un ataque, que puede tener lugar en tiempo real o después de que haya ocurrido. Esta fase del ciclo de la ciberseguridad reposa sobre dos acciones complementarias:

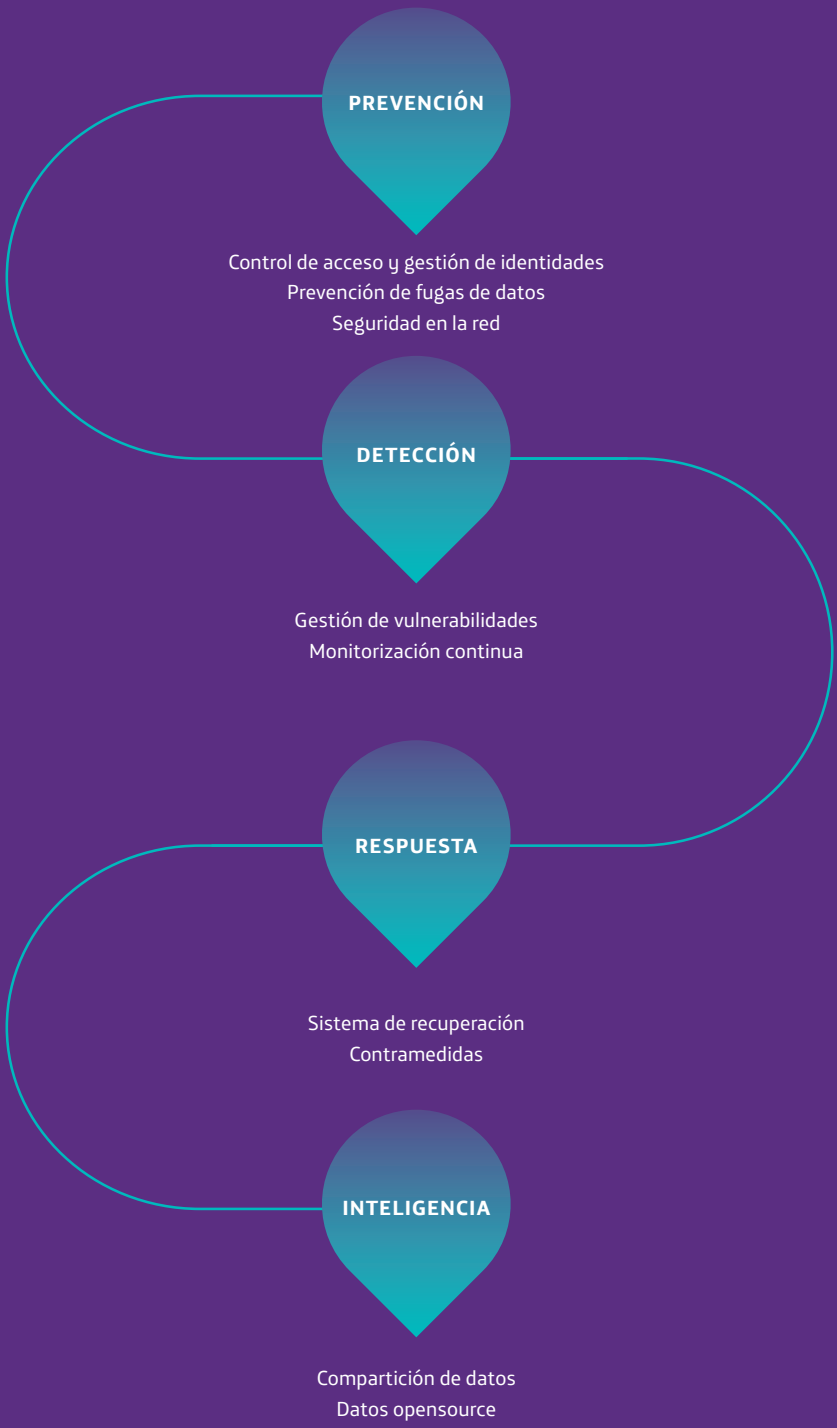
  - La monitorización continua de los sistemas y redes de la empresa para poder identificar lo antes posible los intentos de agresión y limitar el daño que puedan causar.
  - La identificación de los puntos flacos en nuestras infraestructuras informáticas que pueden dejarnos expuestos ante conductas maliciosas.

- **Respuesta** cuando finalmente la empresa ha sufrido un ciberataque se inicia esta etapa, que conlleva:

  - Los sistemas de recuperación, que permiten devolver el estado de los equipos y las aplicaciones al punto de partida anterior a que se haya producido el problema.
  - La aplicación de nuevas medidas de seguridad que eviten que la situación se vuelva a producir en el futuro.

- **Inteligencia** Se trata de compartir la información sobre los ataques con otras empresas e instituciones, así como con organismos relacionados con la seguridad, para conocer mejor la operativa de agresión y hacer más efectiva la respuesta al cibercrimen.

ETAPAS DE LA GESTIÓN DE LA CIBERSEGURIDAD



Fuente: Fundación Telefónica. *Ciberseguridad, la protección de la información en un mundo digital*

lo que hacen los responsables de seguridad

El especialista en ciberseguridad tiene como función principal el detectar las posibles vulnerabilidades en los sistemas y redes de la empresa y el habilitar mecanismos para impedir que se produzcan ataques por culpa de esos fallos. Esta tarea se puede realizar desde distintas perspectivas, como son las siguientes:

Hacking ético

Básicamente, se trata de poner a prueba la seguridad de los sistemas actuando como un *hacker*, es decir, realizando un ataque (consentido y aprobado por la empresa) para identificar posibles fallos de seguridad y, de esta manera, solucionarlos. No es otra cosa que una manera de adelantarse al ciberdelincuente.

Análisis forense

Paralelo a su homólogo en medicina, el análisis forense informático se basa en técnicas científicas y analíticas para investigar qué ha ocurrido tras un incidente relacionado con la seguridad. Además de entender los hechos ocurridos, el objetivo puede ser identificar, preservar, analizar y presentar datos que sean válidos en un proceso legal.

Ingeniería inversa

Tradicionalmente, este concepto hace alusión al proceso de analizar un producto para descubrir cómo está fabricado y cómo actúan entre sí sus componentes para que funcione. En el campo de la ciberseguridad, la ingeniería inversa estudia el funcionamiento de un *malware* o programa malicioso para conocer cómo opera y de esta manera poder anticipar una solución o programa que actúe como una "vacuna" frente a sus efectos devastadores.

Gestión de la seguridad y el gobierno de las tecnologías de la información

Un modelo de gobierno de TI está dirigido a facilitar la toma de decisiones por parte de los responsables de la organización mediante la creación de sinergias entre tecnología, seguridad y procesos de negocio. En este caso, alude a las personas que planifican, implementan y supervisan la política de seguridad de la empresa, garantizando que esté alineada con los objetivos y procesos del negocio, así como con la legislación vigente en cada momento.

DEUSTO FORMACIÓN identifica tres perfiles profesionales clave dentro del campo de la ciberseguridad actual:

CISO o *Chief Information Security Officer*

Es el puesto del ejecutivo responsable de la seguridad informática de la empresa, tanto de su planificación, como del despliegue y supervisión.

Consultor de ciberseguridad

Es el encargado de auditar los sistemas de seguridad y de proponer programas de mejora en función de las vulnerabilidades detectadas.

DPO o Delegado en Protección de Datos

Un perfil que cobra una importancia creciente a partir de la entrada en vigor del Reglamento Europeo de Protección de Datos, puesto que es quien organiza y supervisa la política de protección de datos tanto en el interior de la organización como hacia el exterior, mediando en el tratamiento entre la empresa afectada por un posible ataque y la autoridad de control correspondiente.

Por último, un profesional de la ciberseguridad, aparte de los conocimientos técnicos y del dominio de las herramientas adecuadas, debe conocer bien la organización que "defiende", para poder identificar qué áreas y procesos son más susceptibles de sufrir un ataque.

AARON LEVIE

CONSEJERO DELEGADO DE BOX

Queridos niños: si queréis un empleo en los próximos cinco años, estudiad ciencia computacional. Si queréis un empleo para siempre, estudiad seguridad informática

Gran Vía, 28. 28013 Madrid (España)
http://fundaciontelefonica.com/

Edita
Fundación Telefónica

Gerencia editorial
Pablo Gonzalo Gómez

Coordinador del proyecto y textos
Pablo Rodríguez Canfranc

Coordinación editorial
Melisa Martínez Ciaurri

Proyecto gráfico
Lacasta Design

ISBN: 978-84-15282-40-2
Depósito legal: M-3023-2019
Impresión y encuadernación: CommerceGraf
Primera edición: enero de 2019
Impreso en España – Printed in Spain

Esta revista se ha impreso en papel reciclado Cyclus fabricado por Arjowiggins Graphic. Su uso ha reducido el impacto medioambiental en:

29 kg de residuos
713 litros de agua
7 kg de CO2
90 kWh de energía
47 kg de madera

¿Qué hace un científico de datos? ¿En qué se diferencia un desarrollador *backend* de uno *frontend*? ¿Quién es el *community manager* de la empresa? La revolución tecnológica ha traído consigo nuevas profesiones y ha cambiado por completo otras que ya existían.

PROFESIONES DIGITALES es una colección de monográficos de Fundación Telefónica que pretende dar a conocer aquellos perfiles profesionales más demandados por la economía digital.

Con un lenguaje sencillo y divulgativo, cada número acerca al lector una disciplina en la que desarrollan su actividad los trabajadores con los puestos más vanguardistas, ofreciendo de esta manera una breve orientación sobre nuevas áreas laborales.