Especialista en Ciberseguridad

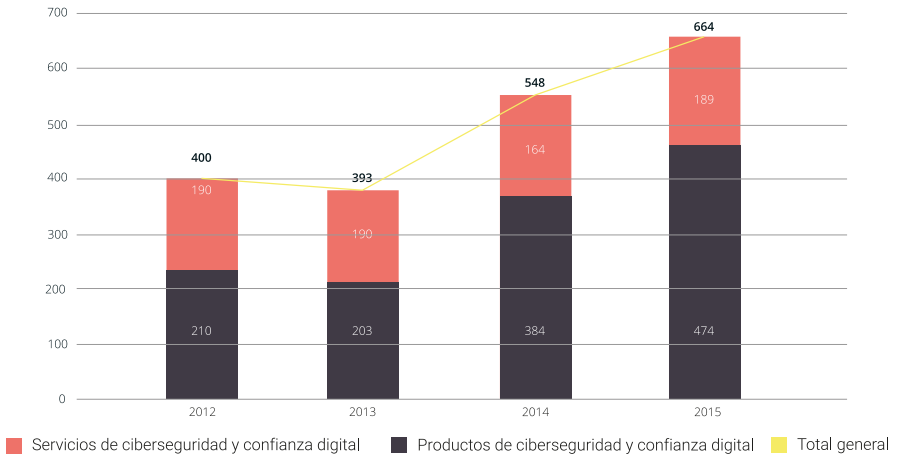
PROFESIÓN

Se estima que en los próximos años se necesitarán tres millones de expertos en ciberseguridad en todo el mundo. Sólo en Europa habrá unos 825.000 empleos vacantes en esta área. España se sitúa en el tercer lugar por número de ataques virtuales, solo por detrás de Estados Unidos y Reino Unido. Sin embargo, y pese a estar en el top de países más perjudicados, seguimos arrastrando un importante déficit de profesionales cuyo principal trabajo es evitar la fuga masiva de datos de las empresas.

La ciberdelincuencia representa una gran amenaza para la seguridad de nuestras empresas. Según el Instituto Nacional de Ciberseguridad (INCIBE), en 2017 fueron registrados 123.000 ataques cibernéticos en España. De ellos, 116.000 fueron contra empresas y ciudadanos, 5.000 contra la Red IRIS, y 885 contra operadores estratégicos. Para hacer frente a esta situación, las empresas están aumentando sus recursos tecnológicos y humanos en ciberseguridad. Según la OTAN, el término Ciberseguridad se refiere a ''la aplicación de medidas de seguridad para proteger las infraestructuras de los sistemas de información y comunicaciones frente a los ciberataques". En concreto, hace referencia a las tecnologías y procesos creados para proteger los sistemas informáticos, el software, las redes y los datos de los usuarios ante posibles ataques informáticos, hackeos o cualquier otro tipo de robo de datos o de identidad.

La ciberseguridad es un factor cada vez más importante dentro de las empresas de nuestro país. En el año 2017, inviertieron 664 millones de euros en productos y servicios de ciberseguridad y confianza digital; 474 en productos como cortafuegos, anti-fraude, anti-malware o seguridad en movilidad, y 189 en servicios como auditoría técnica, formación sobre ciberseguridad y confianza digital o en firma electrónica y servicios de certificación.

BIENES Y SERVICIOS DE CIBERSEGURIDAD Y CONFIANZA DIGITAL



Fuente: Informe Anual del sector TIC ONTSI 2018

¿QUÉ HACE UN ESPECIALISTA EN CIBERSEGURIDAD?

Estos expertos desarrollan todo tipo de estrategias para prevenir cualquier ataque cibernético. En esta profesión resulta fundamental el trabajo en equipo, ya que hay una gran cantidad de medidas de seguridad que deben aplicar.

En función de la empresa o el tipo de servicio que se necesita cubrir, hay seis tareas concretas que desempeña un especialista en ciberseguridad:

- Planificación y desarrollo de medidas de seguridad
- Auditorías internas o externas en temas de ciberseguridad
- Gestión de equipos encargados de establecer las medidas de seguridad
- Detección y prevención ante posibles amenazas o ciberataques
- Administración y mejoras los mecanismos de seguridad empleados
- Aseguración del cumplimiento de todas las normativas relacionadas con la protección y almacenamiento de datos.

Estos especialistas deben dominar los diferentes sistemas operativos, redes y lenguajes de programación, desde el punto de vista de las comunicaciones y de la seguridad informática. Se encargan también de analizar las medidas de seguridad implementadas para proteger la información, de detectar las amenazas de seguridad y elaborar técnicas de prevención, y de crear proyectos de seguridad informática y de las comunicaciones.

Además, desarrollan pruebas de vulnerabilidad y actualizar los sistemas de seguridad, a otorgar los premisos de acceso correspondientes a los usuarios autorizados, a monitorear los accesos a la información, y a ejecutar programas de defensa ante cualquier tipo de traspaso o violación.

Por lo tanto, la figura de un especialista en ciberseguridad resulta fundamental para proteger la confidencialidad de una empresa y su información.

SALARIO

El salario medio de un especialista en ciberseguridad se sitúa entre los 30.000 y los 60.000 euros anuales. Los sueldos más bajos corresponden a los puestos técnicos que cuentan con una menor responsabilidad y experiencia, como el técnico/a de seguridad que cuenta con un sueldo de aproximadamente 28.000 euros anuales o el técnico de redes con 24.000 euros. Por su parte, los sueldos más altos suelen corresponder a los directores de los sistemas de información, con un sueldo anual en torno a los 60.000 euros.

SALIDAS PROFESIONALES

- Administrador de seguridad de sistemas y redes
- Consultor de seguridad y hacking ético
- Arquitecto de sistemas de seguridad
- Director de proyectos de ciberseguridad
- Analista de informática forense
- Gestor de protección de datos
- Ingeniero de control de ciberseguridad

- Arquitecto de análisis de riesgos
- Ingeniero de ventas de ciberseguridad
- Perito judicial tecnológico

LA FORMACIÓN

Las titulaciones más demandadas por las empresas para estos puestos en esta área son las de: Ingeniero Informático, Ingeniero Técnico de Gestión, Ingeniero Técnico de Sistemas, Ingeniero de Telecomunicaciones y las titulaciones de Formación Profesional de Grado Medio y Superior que forman parte de la Familia Profesional de Informática y Comunicaciones.

Hace años, estos expertos tenían que formarse por su cuenta u optar por estudiar fuera de España, pero actualmente se pueden realizar programas máster y cursos de especialización impartidos por universidades y empresas de seguridad.

Ciberseguridad, seguridad informática, tecnologías de la información, gestión y sistemas de información o ingeniería del software son algunos de los másteres que se pueden cursar para dedicarse a alguna de las especializaciones en ciberseguridad. Para acceder a ellos se suele requerir formación previa en programación informática para poder contar con unos conocimientos básicos.

Pero los másteres no son la única opción para tener acceso a esta profesión. Titulaciones como la de Técnico Superior en automatización y Robótica Industrial, de Administración de Sistemas Informáticos en Red o de Sistemas de Telecomunicación e Informática son algunas de las mejores opciones que ofrece la Formación Profesional, especializándose después en alguna materia de la ciberseguridad.

¿QUÉ ES LO MÁS VALORADO DE ESTE PERFIL?

Estos profesionales deben tener un gran sentido del compromiso, ser personas en las que se puedan confiar, que trabajen con ética y profesionalidad y garanticen la confidencialidad de la empresa. Deben contar con una alta disponibilidad y flexibilidad, además de tener iniciativa y facilidad para trabajar tanto en equipo como de forma autónoma.

Como competencias, se valoran mucho las certificaciones profesionales, como: CISA, CISM, CISSP, CDPP, CCSK, CHFI, CEH, DLP, IRM, GIAC, LOPD, SOX, PCI, LEAD AUDITOR, CCNA, CCNP, ISO 27001; la securización y virtualización de sistemas; las tecnologías FIREWALLS, IDS/IPS, SIEM, DLP, antimalware solutions, VPNS, CISCO; herramientas de hacking, como AppScan o Fortify, y conocimientos en las nuevas políticas y normativas de seguridad y protección de datos.

Rosa Díaz Molés

Cybersecurity Strategy Advisory

"La mujer dedica más tiempo a defender que a intentar atacar o acceder a un sistema para comprobar la seguridad del mismo. Dado que la ciberseguridad tiene un problema de género, contar con más mujeres en las empresas y en los organismos que se dedican a protegernos nos daría otros enfoques y otras perspectivas que mejorarían sin lugar a dudas esa protección"

BIOGRAFÍA

Rosa Díaz Moles es licenciada en Ciencias Exactas por la Universidad Autónoma de Madrid y cuenta en su formación con un Programa de Dirección General por el IESE.

Con una sólida experiencia en el sector TIC, ha desempeñado diferentes cargos directivos en empresas como SantanderElavon y Sage. Durante cuatro años ha liderado la Dirección General de Panda Security para Iberia con el objetivo principal de consolidar su posición como líderes tecnológicos de referencia en soluciones de seguridad de nueva generación en el EndPoint. Pertenece al grupo #SomosMujeresTech que tiene como objetivo la visibilidad de la mujer en puestos de liderazgo dentro del mundo de los sectores de la tecnología y la innovación.

ENTREVISTA

P.¿En qué consiste el trabajo de una especialista en ciberseguridad? ¿Cómo es su día a día?

En el sector de la ciberseguridad hay diferentes y muy variadas especialidades. Si bien es cierto que, en sentido estricto, lo que hace un experto en ciberseguridad es analizar sistemas de seguridad informática y crear estrategias que permitan prevenir y anticiparse a los ciberdelincuentes. Algunas de las especialidades son: CSO (Chief Security Officer), CISO (Chief Information Security Officer), Arquitecto de Seguridad, Analistas de Seguridad, Analistas deAataques, Analistas Forenses, Especialistas en Incidencias, DPO (Data Protection Officer), etc.

Y las tareas a realizar son, entre otras: planificación y desarrollo de medidas de seguridad, auditorías internas o externas en temas de ciberseguridad, gestión de equipos encargados de establecer las medidas de seguridad, detección y prevención ante posibles amenazas o ciberataques, administración y mejoras los mecanismos de seguridad empleados o asegurar el cumplimiento de todas las normativas relacionadas con la protección y almacenamiento de datos.

En mi caso, mi experiencia está más en la parte directiva y en ventas, que es donde he desarrollado mi carrera profesional y se encuentra mi principal valor. Liderando a equipos de personas con el objetivo de ayudar a las empresas y a las personas en su vida digital, asesorando y acompañándoles en la toma de decisiones para que estén más seguros.

P. ¿Qué parte de su trabajo le gusta más?

Lo cierto es que lo que más me gusta tiene que ver con la dimensión social de ayudar a estar protegido. Es muy gratificante saber que con tu trabajo estás ayudando a las personas y a las organizaciones a estar más seguras.

P. ¿Cuáles son los principales retos a los que suele enfrentarse en su trabajo?

Podría hablar de varios retos, pero me gustaría centrarme sólo en uno para que el mensaje llegue mejor. España es un país de pymes, más del 98% del tejido empresarial español está formado por pymes. Y en estas empresas aún hay poca conciencia de que la ciberseguridad debe estar en el "core" del negocio. No entienden el gran valor añadido que les aporta, incluso para diferenciarse de sus competidores, tener unas políticas rigurosas en materia de ciberseguridad.

Las empresas deben ser conscientes de que tienen que invertir en ciberseguridad, aplicar buenas prácticas para evitar la fuga de información, crear procedimientos seguros, y hacer un uso responsable de las herramientas para detectar y gestionar posibles peligros y riesgos para la seguridad.

Uno de mis principales retos concienciar a estas empresas. Todavía tenemos mucho camino por recorrer, porque seguimos escuchando cosas como "esto a mí no me va a pasar" o "quien va a querer atacarme a mí". No nos damos cuenta de que, aunque seamos una empresa pequeña, alguien puede estar interesado en nuestra información o en convertirnos en el punto de acceso hacia otras empresas de mayor envergadura.

P. ¿Puede explicarnos qué diferencias hay entre la ciberseguridad y la seguridad de la información?

La seguridad de la información tiene como objetivo proteger la información en cual-

quier formato a través de metodologías, normas, técnicas, herramientas, estructuras organizacionales, tecnología y otros elementos en las distintas facetas de la información. La ciberseguridad pone el foco en la información en formato digital y los sistemas interconectados que la procesan, almacenan o transmiten. De forma que la ciberseguridad es una parte de la seguridad de la información.

P. ¿Qué perfiles son los más demandados dentro del sector de la ciberseguridad?

Aunque históricamente la seguridad de los sistemas era competencia casi exclusiva de los departamentos de IT, como las ciberamenazas van en aumento y las compañías tienen que gestionar gran cantidad de información y cumplir con obligaciones normativas y legislativas, ahora también hay otros departamentos implicados. Por ejemplo, el área jurídica. Por ello, se requieren perfiles mixtos con competencias en áreas legales, técnicas y de negocio.

Además, en las organizaciones que se dedican a protegernos y a luchar contra la ciberdelincuencia también es necesario estudiar el comportamiento de estos individuos y son necesarios psicólogos, filólogos, criminólogos, forenses, etc. En definitiva, equipos de alto rendimiento diversos que ayuden con diferentes habilidades en la lucha contra la ciberdelincuencia.

Y no podemos olvidar el amplio ecosistema de empresas que se dedican a vender productos y servicios de ciberseguridad, dando cabida a otro tipo de perfiles para acercar a los clientes las propuestas de valor como son: especialistas en marketing, ecommerce, preventas, técnicos, consultores, comerciales, etc.

P. ¿Cuáles son los ataques informáticos más comunes actualmente?

La mayoría de amenazas que existen hoy en día son aquellas que buscan algún beneficio económico, directo o indirecto. Por ejemplo, uno de los tipos de ataques más prevalentes hoy en día en el mundo de la empresa es el del "ransomware", que secuestra la información y pide un rescate para poder recuperarla. También tenemos ataques protagonizados por troyanos cuyo principal objetivo es el robo de información confidencial, robo de credenciales, etc. Existen igualmente otras amenazas que tratan de comprometer cuentas de correo corporativo, en una forma más evolucionada de realizar "phising". En este tipo de ataques hay más conocimiento acerca de las víctimas y alguien se hace pasar por el CEO o por un alto ejecutivo e instruye a una persona para que realice determinadas acciones como, por ejemplo, realizar una transferencia a una determinada cuenta.

También hay ataques de denegación de servicio (DDoS). Este tipo de ataque informático consiste en generar una enorme cantidad de tráfico desde numerosos dispositivos a un sitio web. Debido a este drástico aumento del tráfico, el rendimiento de la red disminuye hasta el punto de que dicha red se satura y se interrumpe su funcionamiento normal. Y, por supuesto, la proliferación de dispositivos IOT les hacen muy susceptibles de recibir ataques.

Y no olvidemos que un 95% de los incidentes son debidos a fallos humanos (según el informe elaborado por investigadores en seguridad de IBM, conocido por IBM X-Force Threat Intelligence Index 2018). El ser humano, y en este caso el empleado de la

empresa, sigue siendo el eslabón más débil y el más vulnerable.

Por este motivo, los conocimientos en materia de seguridad que tengan los empleados en una compañía son la mejor barrera contra los ataques, ya que el empleado puede ser la mayor debilidad o la mayor fortaleza de una estrategia de ciberseguridad dependiendo del nivel de formación del que dispongan.

P. En su opinión, ¿qué habilidades, más allá de la formación, son imprescindibles para estos especialistas?

Además de la formación y las habilidades técnicas, se requieren habilidades sociales, dado que es necesario escuchar a las personas, ponerse en su piel, detectando sus problemas y proponiendo soluciones. Hay que tener capacidad de negociación, de hablar en público, de formar a los usuarios y enseñarles el uso de los dispositivos informáticos. Y añadiría también la capacidad de liderazgo para poder llevar a cabo los proyectos.

P. ¿Qué se valora más en esta profesión, la formación o la experiencia?

Lo cierto es que en este sector aún falta mucho camino por recorrer, aunque en España hay una gran oferta de máster en ciberseguridad que ayudan a las personas a formarse en aquellas materias que demandan las empresas.

Pero lo más valorado, y algo que es crucial en este sector, es el aprendizaje continuo y constante, dado que las amenazas evolucionan y los ciberdelincuentes trabajan unidos para rentabilizar y maximizar la efectividad de los ciberataques. Es por ese motivo que se hace necesario estar siempre a la última y, si es posible, ir por delante de ellos para anticiparnos al ataque de manera más efectiva, o por lo menos, en su etapa más temprana con el objetivo de minimizar los riesgos y el impacto en las organizaciones.

P. ¿Qué consejos le daría a una mujer que quiere dedicarse a esta profesión?

El aumento de ciberataques y la proliferación de nuevas amenazas con un grado de sofisticación elevado y creciente, hace necesario incorporar profesionales expertos en ciberseguridad. Según una encuesta del Centro para la Ciberseguridad y Educación (ISC), para el año 2022 habrá 1,8 millones de empleos en ciberseguridad sin cubrir en todo el mundo, 350.000 de ellos en Europa. De forma que, sin lugar a dudas, esta es una profesión que debe tenerse muy en cuenta. Por este motivo, mi consejo sería que no lo dude, que es un sector muy interesante en el que podemos ayudar a las personas y a las organizaciones a estar más seguras.

P. ¿Ha encontrado barreras en su carrera profesional solo por el hecho de ser mujer?

Lo cierto es que en mi caso la única barrera que he encontrado en mi trayectoria profesional he sido yo misma. Al comienzo de mi carrera profesional no me planteé objetivos a largo plazo, ni por supuesto llegar a ser directiva en una compañía. Y como nos pasa muchas veces a las mujeres, tampoco buscaba visibilidad. Me centraba en el desarrollo de mi trabajo y dejaba en un segundo plano toda la parte tan importante de "networking" y relaciones. El cambio se produjo cuando en mi compañía estaban buscando incorporar a un directivo y una gran amiga, a la que tengo mucho que agradecer,

me animó a que me presentara. Llevaba realizando una gran labor profesional en la sombra durante muchos años, y no fui consciente de ello hasta ese instante. Me presenté y finalmente fui la elegida.

P. ¿Qué cree que puede aportar la visión de una mujer en el ámbito de la ciberseguridad?

Para mí, el valor diferencial de una mujer en el sector de la ciberseguridad es el mismo que en cualquier otro. Todos somos conscientes de que la diversidad en los equipos configura una posición más enriquecedora en la toma de decisiones y es una ventaja competitiva para las compañías. También es cierto que en el caso de la ciberseguridad hay diversos estudios que indican que, por ejemplo, si hablamos de hacker, la mujer dedica más tiempo a defender que a intentar atacar o acceder a un sistema para comprobar la seguridad del mismo. Y dado que la ciberseguridad tiene un problema de género y solo un 11% son mujeres, contar con ellas en las empresas y en los organismos que se dedican a protegernos es asegurar otros enfoques y otras perspectivas que mejorarían, sin lugar a dudas, la protección.

P. Usted es una de las diez directivas que pusieron en marcha la iniciativa #SomosMujeresTech ¿Qué retos les quedan aún por superar a las mujeres en los sectores de la tecnología y la innovación?

Tenemos aún muchos retos por delante. Solo un 14,6% de mujeres realizan estudios tecnológicos, y aunque podemos hablar de estereotipos y tradición cultural, lo que está claro también es que a las mujeres no nos atraen este tipo de carreras y es aquí donde se encuentra el problema. El reto está en motivar a las jóvenes para que hagan estudios relacionados con las TIC desde mucho antes de la universidad, en edades tempranas. Hay muchas personas que aún desconocen esta profesión y la falta de conocimiento hace que sea más fácil encaminar a los alumnos o hijos hacia otras profesiones más tradicionales, cuya finalidad está más claramente definida y divulgada.

La falta de conocimiento del sector TIC es uno de los elementos que entran en juego a la hora de hacer que pocas mujeres elijan estudios encaminados a esta profesión. Por este motivo, cobra especial importancia la comunicación y dar visibilidad a referentes y expertas en medios especializados y generalistas que muestren la creatividad, flexibilidad y versatilidad de estas carreras, en especial de las carreras STEM.

También tenemos un reto y una responsabilidad: transmitir a todos nuestros jóvenes, no sólo a las mujeres, otro modelo a seguir que esté sustentado en la cultura del esfuerzo; fomentando inquietudes y expectativas de futuro atractivas y responsables, que potencien una sociedad plural e igualitaria. Un futuro alejado de referentes utópicos y superficiales como los que vemos en redes sociales y en algún medio de comunicación en estos momentos.