Publicado en Madrid el 15/12/2022

# DXC Technology identifica cinco tendencias de ciberseguridad que cambiarán el 2023

## El sector mundial de la ciberseguridad contratará a 3,4 millones de profesionales más para neutralizar la amenaza cibercriminal

DXC Technology (NYSE: DXC), empresa líder mundial en servicios tecnológicos que figura en la lista Fortune 500, ha pronosticado cinco escenarios en los que la seguridad digital configurará la vida cotidiana de los próximos cinco años.

1. La carrera armamentística de la ciberseguridad se acelerará

Tanto los ciberdelincuentes como los profesionales de la ciberseguridad utilizarán la inteligencia artificial (IA) en una batalla de ingenio cada vez más sofisticada. En el caso de la defensa de la ciberseguridad, la IA se ha utilizado principalmente para identificar patrones de comportamiento sospechoso. Debido al volumen de actividad sospechosa y al número de falsos positivos, el personal de ciberseguridad se ve a menudo desbordado.

La buena noticia es que, a partir de 2023, se debería poder empezar a automatizar los controles de seguridad y los mecanismos de respuesta basados en IA, lo que ayudaría a reaccionar con mayor rapidez y precisión ante los ciberataques, reduciendo los posibles tiempos de inactividad y protegiendo los datos personales y empresariales críticos.

"Sin embargo, aunque la IA puede automatizar la detección y eliminación de amenazas, los procesos subyacentes se basan en la comprensión de la actividad pasada, lo que incentivará a los ciberdelincuentes a soñar con nuevos tipos de ataques", según Mikel Salazar, Director de Servicios de Seguridad para España y Portugal. "Mantener el ritmo será un desafío, especialmente si la computación cuántica entra en la refriega, lo que podría ver las defensas actuales violadas en segundos".

2. Se debe tener cuidado con quién se habla en el metaverso (mientras se mantiene un firme control de las carteras digitales)

2023 va a ser un año importante para el metaverso, con Meta, Microsoft, Virbela y otros apostando por la generalización de los mundos virtuales. Sin embargo, la actividad en el metaverso puede plantear problemas de legitimidad: "¿cómo saber si la persona con la que crees que estás hablando es quien dice ser?. Los certificados digitales basados en blockchain ayudarán a asegurar las transacciones virtuales en el metaverso. Lo que está claro es que a medida que el metaverso se expande, también lo hacen los riesgos", según Mark Hughes, Presidente de Security.

3. Los ataques geopolíticos a la ciberseguridad aumentarán, pero también llevarán a la innovación en defensa

El ataque de Rusia a Ucrania recordó de la manera más cruda posible, que la guerra es ahora híbrida y que los riesgos de ciberataques por motivos geopolíticos son reales. Como resultado, muchas

pólizas de ciberseguros se están actualizando para excluir los actos de ciberguerra, lo que plantea retos para la mitigación del ciber-riesgo.

Con las persistentes tensiones geopolíticas, esta amenaza continuará e irá más allá de 2023. De hecho, con más de 70 países en los que se celebrarán elecciones gubernamentales en 2023, será un año difícil para las defensas de ciberseguridad.

4. Los ataques de ciberseguridad tendrán como objetivo las infraestructuras nacionales críticas que abastecen los hogares
Cuando se va la luz o se corta el gas, es poco probable que la mayoría de la gente piense que es el resultado de un fallo de ciberseguridad industrial. Pero la tecnología operativa (OT) es un campo de batalla emergente para los ciberataques, ya que los sistemas que controlan y automatizan las fábricas y la infraestructura civil, incluidas las centrales eléctricas y las presas, se están convirtiendo en un objetivo.

"Con las continuas tensiones geopolíticas, la amenaza cibernética de las tecnologías de la información crecerá en 2023, presionando a las industrias para que se aseguren ir un paso por delante mediante la protección de la ciberseguridad en todas sus operaciones", según Mikel Salazar, Director de Servicios de Seguridad para España y Portugal.

5. Aumentarán las oportunidades profesionales en ciberseguridad
Se calcula que en el mundo faltan unos 3,4 millones de trabajadores en ciberseguridad. Esta falta de profesionales, y más aún con las crecientes amenazas, es un número que no parará de crecer en los próximos 5 años.

El déficit de competencias en ciberseguridad crea oportunidades profesionales para personas de todas las edades y procedencias. Cada vez son más las empresas que ofrecen la posibilidad de reciclarse en ciberseguridad.

"La inclusividad del espacio de la ciberseguridad se extiende a la neurodiversidad", según Mark Hughes, Presidente de Seguridad. "Por ejemplo, el Programa Dandelion de DXC ayuda a personas con autismo, TDAH, dislexia y otras afecciones neurológicas a desarrollar carreras en TI, incluida la ciberseguridad. El crecimiento de la amenaza cibernética crea oportunidades profesionales para personas de todos los orígenes".

"Las ciberamenazas seguirán aumentando en velocidad y complejidad durante 2023 y más allá, pero también lo hará la capacidad de aplicar las últimas tecnologías, enfoques y talento para hacerles frente", según Mikel Salazar, Director de Servicios de Seguridad de DXC Technology para España y Portugal.

**Datos de contacto:**
María Guijarro

622 83 67 02

Nota de prensa publicada en: Madrid

Categorías: Telecomunicaciones Software Ciberseguridad