Los responsables de la toma de decisiones en materia de seguridad se ven obligados a estar siempre un paso por delante de los ciberdelincuentes. Esto ha llevado a una cultura de aversión al riesgo y a la creación de checklists de forma compulsiva. Por otra parte, las organizaciones y las tecnologías que utilizan cambian constantemente, en 2020 más que nunca. En la unión de estos dos factores, cambio rápido y procedimientos estrictos, reside el desafío de la seguridad.

El estudio "10 de 10" de Bitdefender muestra la brecha existente entre la visión de los responsables de seguridad sobre el panorama actual en este campo y las medidas que deben poner en marcha.

Necesidad de cambiar la seguridad desde dentro

82%

82% (72% global) creen que es necesario **incorporar a profesionales con habilidades y conocimientos de seguridad más diversos**

18%

El 18% de los profesionales de infosec afirma que **una mayor neurodiversidad** en el sector ayudará a combatir posibles ciberguerras.

41%

El 41% piensa que la neurodiversidad servirá para **fortalecer las defensas de ciberseguridad.**

38%

El 38% opina que una fuerza laboral con más neurodiversidad **nivelará el campo de juego en el que se lucha** contra los malos.

11%

El 11% (22% global) cree que si el déficit de habilidades actual continúa durante otros cinco años **muchas empresas desaparecerán.**

El estudio de Bitdefender muestra que el sector de la seguridad está firmemente convencido de la necesidad de incorporar diversidad.

La comunicación es clave

Los profesionales de seguridad creen que debe cambiar su forma de comunicar:

53%

El 53% de los profesionales de seguridad de España afirma que **su comunicación debe cambiar drásticamente** para lograr que sus empresas incrementen la inversión en ciberseguridad.

54%

El 54% de los encuestados españoles piensa es necesario **mejorar el intercambio de conocimientos** entre los profesionales del sector para eliminar riesgos más rápido en el futuro.

36%

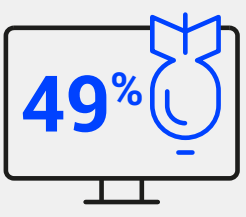
36% piensan que utilizar **un lenguaje menos técnico** ayudaría a comunicar de forma más eficaz, y toda la organización comprendiera los riesgos y cómo mantenerse protegida.

El cambio en la comunicación es imperativo para que los profesionales de infosec puedan reaccionar con rapidez a la hora de proteger sus organizaciones y obtener la inversión que necesitan.

La guerra cibernética preocupa mucho

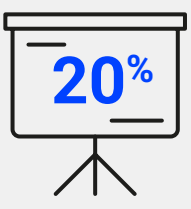
Los riesgos de la ciberguerra aumentan y, aunque preocupados, algunos profesionales de seguridad aún no están preparados.

El 49% de los profesionales españoles creen que las prácticas de ciberguerra perjudicarán a la economía en los próximos 12 meses



El 68% de los profesionales españoles encuestados piensa que la ciberguerra supone una amenaza para su organización.

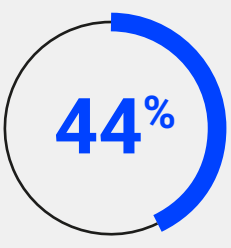
El 20% dice no contar con una estrategia para protegerse contra la ciberguerra.



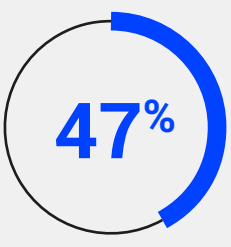
Una mayor inversión en ciberseguridad (44%) y una mayor cooperación entre los sectores público y privado (34%) son puntos clave para poder afrontar una ciberguerra, según los profesionales españoles.

Subida y caída (y subida de nuevo) del ransomware

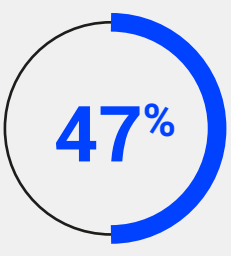
Los ataques de ransomware están aumentando nuevamente, pero la seguridad contra estos incidentes no ha mejorado al mismo ritmo.



El 44% de los profesionales de infosec españoles están observando un resurgimiento de los ataques de ransomware, pero la protección contra ellos no ha avanzado mucho en los últimos 5 años.



Al 47% le preocupa que un ataque de ransomware pueda acabar con su empresa en los próximos 12 a 18 meses si no aumentan la inversión en seguridad.



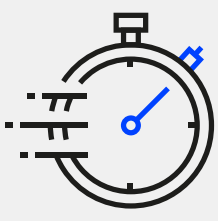
47% cree que si sufriera un ataque de ransomware, **su empresa acabaría pagando el rescate.**

El ransomware ha llegado para quedarse, por lo que es necesario encontrar, desarrollar e invertir en mejores defensas.

Todos estamos conectados, pero no protegidos

El 30% de los profesionales españoles (40% global) cree que para los piratas informáticos **resulta fácil controlar los dispositivos IoT** que los empleados utilizan a la hora de trabajar desde sus hogares

Un 68% está convencido de que, como resultado del mayor uso de dispositivos de IoT, el conocimiento sobre cómo proteger estos dispositivos **ha mejorado en su empresa**.



19% afirman que el uso de los dispositivos IoT crecerá en los próximos 18 meses a un ritmo más rápido de lo que serán capaces de asegurar

El ritmo de crecimiento de los dispositivos IoT es más rápido que la seguridad establecida para proteger a los usuarios.

Metodología

6.724 profesionales de ciberseguridad encuestados, 526 en España.

Los encuestados trabajan en empresas de varias industrias, incluyendo el sector de la energía y la industria financiera, y organismos públicos, con 100 empleados o más, de **EE. UU., Reino Unido, Australia, Nueva Zelanda, Alemania, Francia, Italia, España, Dinamarca** y **Suecia**..

El panorama global de amenazas está en constante evolución

Descubra cómo puede mantenerse a la vanguardia.