“La ciberseguridad es una cuestión de supervivencia empresarial”

Vicente Gea Vidal,
especialista en Gestión de Riesgo Humano en SoSafe

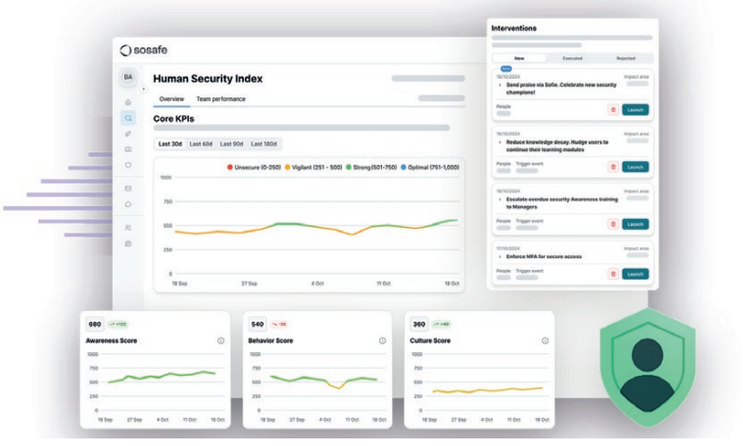
El factor humano sigue siendo el eslabón por el que menos se invierte en ciberseguridad. SoSafe ayuda a reforzar la cultura de ciberseguridad y a prepararse para nuevas exigencias como NIS2

Los ciberataques son ya un riesgo cotidiano: pueden paralizar operaciones, comprometer datos sensibles y causar pérdidas económicas y reputacionales en pocas horas. Su creciente sofisticación, impulsada por la profesionalización del cibercrimen y las nuevas tecnologías, amplía la exposición de todo tipo de empresas. Además, la directiva europea NIS2 eleva las exigencias y la responsabilidad. Hablamos con Vicente Gea Vidal, especialista en Gestión de Riesgo Humano en SoSafe.

P. Se dice que no debes preguntarte si te atacarán, sino cuándo lo harán, ¿es así?
Respuesta. Sí, cualquier empresa está expuesta, sin importar tamaño, sector o mercado. En los últimos años, la profesionalización del cibercrimen y el uso de la IA han multiplicado la capacidad de lanzar ataques masivos, rápidos y cada vez más realistas. La ingeniería social, además, se aprovecha de nuestras emociones para manipularnos y obtener datos personales y profesionales. El impacto puede ser devastador: según INCIBE, una brecha de seguridad cuesta de media unos 35.000 euros en España, y muchas pymes no logran recuperarse. La ciberseguridad ya es una cuestión de supervivencia.

P. ¿Cuáles son los principales errores que cometen las empresas en ciberseguridad?
Respuesta. Bajo mi punto de vista, hemos hecho muchas cosas bien, especialmente en infraestructura y monitorización, pero hemos cometido y seguimos cometiendo dos errores que muchas veces nos sentencian.

Por un lado, considerar la ciberseguridad como una temática aislada y gestionada por un departamento, cuando realmente es cosa de todos y, en conjunto, somos la primera línea de defensa de los activos de la empresa.



Por otro, el desgaste de muchas organizaciones que han invertido millones en productos técnicos y siguen siendo ciberatacadas porque no han logrado reforzar correctamente al factor humano, que es el origen del 82% de las brechas de seguridad.

P. ¿Cómo afecta la directiva NIS2 a este entramado?
Respuesta. La NIS2 es una nueva directiva europea que pretende reforzar la ciberseguridad y mantener la continuidad de infraestructuras críticas en toda la UE. Actualmente, más de 180.000 empresas de industrias esenciales e importantes del mercado común (sanidad, transporte, energía, farma, alimentación...) están impactadas.

Por primera vez en ciberseguridad, los directivos de las compañías impactadas pueden enfrentar responsabilidad penal si no destinan los recursos necesarios para la adecuación a dicha directiva.

Actualmente, no está transpuesta en España, pero en otras economías más maduras en ciber, como Alemania, entra en vigor en marzo de 2026. En otras palabras, va a llegar y hay que prepararse.

NIS2 nos ayudará a globalizar la ciberseguridad dentro de la organización y dejar de considerarla algo aislado.

P. ¿Cómo pueden las empresas evitar estos ataques?
Respuesta. Es importante que construyan y auditen regularmente su Plan Estratégico de Ciberseguridad y los distintos pilares que lo componen.

Dada la importancia del factor humano en las brechas de seguridad, es un pilar clave que puede ser reforzado por empresas como SoSafe, destinadas a ayudar al aprendizaje, entrenamiento y refuerzo de la cultura de ciberseguridad de las empresas, ajustado al contexto de cada una de ellas, como ya hemos hecho con más de 6.000 clientes en Europa.

Desde recrear ataques reales, crear formaciones interactivas a partir de políticas, así como prepararse para las auditorías como NIS2, DORA, ISO27001... el enfoque de SoSafe es multimodal.

Más información
www.sosafe.de