Ciberseguridad y empleados: conviértelos en tu mejor defensa

El mayor riesgo digital no es tecnológico, sino humano. Refuerza la seguridad con una cultura de la privacidad sólida y confianza cero.

1 de enero de 2026

Por Tawfiq Alashoor

En 2024, un empleado de la oficina de Hong Kong de la multinacional británica Arup transfirió 20 millones de libras esterlinas a varias cuentas después de que se lo pidiera, aparentemente, el director financiero de la compañía. Al principio, desconfió del correo electrónico supuestamente procedente de la oficina de Londres en el que se le solicitaba realizar esas transacciones en secreto. Sin embargo, accedió tras mantener una videollamada con el director financiero y otros empleados a los que reconoció. Solo más tarde se descubrió la estafa: la videollamada era un *deepfake* que utilizaba voces e imágenes generadas por IA. “Como ocurre en muchas otras empresas de todo el mundo, nuestras operaciones son objeto de ataques habituales, entre ellos fraudes de facturación y estafas de *phishing*. Pero el volumen y la sofisticación de estos ataques han ido en aumento”, declaró un portavoz de la empresa.

Este caso ilustra una verdad importante sobre la ciberseguridad. La resume este testimonio del hacker convicto Kevin Mitnick: “Pese a la facilidad con que se explota, el lado humano de la seguridad informática suele obviarse. Las empresas gastan millones de dólares en cortafuegos, encriptación y dispositivos de acceso seguro, un dinero desperdiciado porque ninguna de estas medidas aborda el eslabón más débil de la cadena de la seguridad: las personas que usan, administran, operan y responden por los sistemas informáticos que

contienen información protegida”.

Las capas de la ciberseguridad

Como las amenazas y riesgos cibernéticos son constantes, las empresas intentan mitigar su impacto o evitarlos por completo mediante controles de acceso, es decir, controlando literalmente el acceso al sistema. Para ello despliegan múltiples protecciones de tecnologías de la información (TI) y tecnologías operacionales (TO), como encriptación, cortafuegos, protocolos de seguridad, autenticación de dos pasos, copias de seguridad o parches. Pero, por esenciales que sean todas estas capas de protección técnica, no bastan, ya que dejan fuera el factor humano, en sí mismo otra capa.

Por eso, las protecciones técnicas deben ir de la mano de controles de gestión, el foco de este artículo. Por controles de gestión nos referimos a algo más que ofrecer a los empleados programas de educación, formación y concienciación en seguridad (SETA, por sus siglas en inglés). Tales programas enseñan a los empleados los aspectos básicos –no compartas contraseñas, actualiza tu software, no abras enlaces sospechosos–, pero no abordan los errores potencialmente más graves que cometemos en nuestras decisiones cotidianas de privacidad. Como muestra el gráfico, por muy riguroso que sea tu diseño técnico para mantener a los hackers fuera, de nada sirve si descuidas el factor humano y un empleado crédulo los invita sin querer por la puerta de atrás. Después de todo, es más fácil “iniciar sesión” que “hackear”. ¿Dónde está poniendo el foco tu empresa?

Recientemente, en un webinar del IESE sobre ciberseguridad, pregunté a los asistentes: “¿Cuántas veces aceptáis las *cookies* al abrir una web?”. La mayoría dijo que casi siempre o a veces, y menos de un tercio, nunca. Aunque la tasa de rechazo era más alta de lo habitual, aún debería haberlo sido más a tenor de la otra pregunta que les planteé: “¿Alguna vez habéis sufrido u os ha afectado un ciberataque, personalmente o en el trabajo?”. La respuesta fue un sí abrumador; y probablemente los pocos que contestaron que no fue porque lo desconocían. Como muestra el caso de Arup, los ciberataques son cada vez más sofisticados, por lo que nadie puede permitirse el lujo de bajar la guardia.

Qué es la cultura de la privacidad y por qué es clave

Es fundamental complementar los programas SETA con otros de educación, formación y concienciación en privacidad, o PETA. Si, como estiman los estudios, del 80 al 90% de las brechas de seguridad se deben a errores humanos, las empresas deberían prestar tanta atención a su cultura de la privacidad como a sus sistemas de TI/TO.

La cultura de la privacidad de una empresa engloba los valores, creencias y prácticas colectivas con un profundo arraigo en sus operaciones que guían cómo se aborda y prioriza la gestión de datos y la protección de información personal. Abarca las actitudes y comportamientos de los empleados de todos los niveles de la compañía, haciendo hincapié en la importancia de proteger la privacidad y los datos personales. Requiere ser proactivo en el cumplimiento de los estándares de privacidad, con formación para toda la organización y un compromiso compartido que garantice la integración de los principios de protección de datos en todas las operaciones, procesos de toma de decisiones y objetivos estratégicos. De ahí que, en el gráfico propuesto, la **cultura de la privacidad** cubra tanto la parte técnica como la de gestión de los controles de seguridad de una empresa.

En un estudio que he realizado con colegas de Brasil, Arabia Saudí, Reino Unido y Estados Unidos, desarrollamos un modelo de apoyo al desarrollo de una cultura empresarial de la privacidad.

Para definir un punto de partida común sobre la privacidad, empezamos encuestando a más de mil empleados de diversos departamentos (ventas, compras, marketing, estrategia y gobernanza) y sectores (industria manufacturera, tecnología, salud, distribución minorista, comercio electrónico y clubs deportivos). Les hicimos una serie de preguntas, primero sobre sus expectativas en materia de privacidad y después sobre su percepción de las prácticas de sus empresas. También medimos su comportamiento general (mediante afirmaciones como “Sé lo que hay que hacer si advierto o sufro una incidencia de seguridad o una brecha de datos”) y evaluamos sus respuestas a situaciones concretas (con una serie de preguntas del tipo “¿Qué harías si…?”). Asimismo, tomamos como referencia la legislación existente, como el Reglamento General de Protección de Datos de la Unión Europea (RGPD). Todo ello generó un índice compuesto de diez pilares de la cultura de la privacidad.

Los 10 pilares de la cultura de la privacidad

1. Seguridad de la información

Se han aplicado las medidas adecuadas (políticas, procedimientos y sistemas), seguidas y monitorizadas por colaboradores para proteger la información personal de los sujetos de datos.

2. Gestión de riesgos

La organización ha definido los niveles de riesgo y la documentación actualizada para gestionar los riesgos de privacidad y protección de datos, incluida la evaluación, monitorización y comunicación de los riesgos a las partes implicadas.

3. Transparencia

Las políticas de privacidad y los controles de acceso a datos personales se revisan regularmente y están a disposición de toda la organización. Los cambios importantes relativos al uso de datos se comunican proactivamente a los afectados.

4. Gobernanza organizacional

Se ha implementado una estructura organizacional bien definida, con cargos y responsabilidades claras y comunicadas, y apoyada por el consejo y los directivos. Además, se han nombrado colaboradores “paladines de la privacidad”.

5. Propósitos del procesamiento

Los miembros de la organización saben por qué manejan datos personales y cuáles son las bases legales de ese manejo para cada actividad.

6. Intercambio de datos

Existen contratos o acuerdos firmados y actualizados para el procesamiento de datos personales con todas las terceras partes con que se comparten.

7. Derechos de los sujetos de datos

Los clientes, usuarios y empleados reciben instrucciones sobre cómo ejercer sus derechos de privacidad y protección de datos. Además, la organización cuenta con una estructura y un procedimiento claros para atender esos derechos.

8. Gestión de incidencias

Existen procesos claros para identificar las incidencias y filtraciones de seguridad de datos, incluida la evaluación y comunicación de tales incidencias a las partes afectadas y a las autoridades.

9. Formación

La organización dispone de políticas, formación y apoyo a los que pueden acceder fácilmente sus empleados, y los directivos supervisan regularmente su participación.

10. Principios del procesamiento de datos

La organización cuenta con operaciones y procedimientos para garantizar que el

procesamiento de datos está limitado a la necesidad, tiene un alcance definido y los datos solo se guardan el tiempo necesario.

Tras establecer este índice, repetimos la encuesta un año después con otro grupo de más de 1.400 empleados de departamentos y sectores igual de diversos. Esta evaluación comparativa nos permitió ver si la cultura de la privacidad evolucionaba en las empresas y cómo lo hacía, además de identificar disparidades entre las expectativas y las prácticas y entre los comportamientos generales y las respuestas situacionales.

Al comparar los resultados de un año con los del siguiente, observamos pequeñas mejoras en los diez pilares, lo cual resulta algo reconfortante. Sin embargo, persistían brechas, en particular entre las expectativas de los empleados y las prácticas de las empresas.

Nuestro análisis de los datos por cargos señaló que la puntuación de los líderes empresariales era menor que la del personal de operaciones en ambos años. Es un dato preocupante, porque los líderes son los responsables de garantizar la aplicación de políticas de protección de datos y el cumplimiento por parte de la compañía de las leyes y regulaciones pertinentes.

La identificación de tales disparidades permite que las empresas dirijan mejor sus intervenciones. Como comentó un responsable de privacidad de datos, este ejercicio reveló cuáles eran las áreas prioritarias de mejora en su compañía.

El índice sirve como referencia para que las empresas evalúen el estado de su cultura de la privacidad y sus niveles de madurez, ya que destaca las vulnerabilidades que deben abordarse con los empleados. (Si te interesa usar nuestra herramienta de evaluación como referencia y adaptarla a tu propio contexto, puedes consultar las preguntas exactas que utilizamos en el apéndice de nuestro artículo científico). Para traducir este diagnóstico en acción, resumimos nuestro enfoque en un marco de tres pasos al que llamamos las 3P (3B en inglés, por *Baseline*, *Benchmark* y *Bridge*).

Las 3P: un marco en tres pasos

Punto de partida

Valora exhaustivamente la cultura de la privacidad de tu empresa para comprobar su estado actual. Elabora tu propio índice base identificando las áreas clave en las que centrarse.

Punto de referencia

Compara los resultados de tu índice de cultura de la privacidad con los estándares y las mejores prácticas de tu sector. Además, al repetir este ejercicio anualmente, podrás seguir el progreso de tu empresa en cultura de la privacidad.

Puente

Cierra las brechas identificadas en los pasos anteriores, tanto internas (discrepancias entre las prácticas y aspiraciones de tu empresa) como externas (la posición de tu empresa con respecto a los competidores y el mercado).

Creemos que este enfoque desplaza constructivamente el foco de las meras estrategias técnicas o de cumplimiento normativo hacia un pensamiento más holístico sobre privacidad y seguridad de datos, alineando los comportamientos de los empleados con los objetivos del liderazgo y la organización. Y, lo que es crucial, involucra a los empleados en el proceso, ya que suelen ser la primera línea de defensa frente a ciberataques y brechas de datos.

Conciencia a los empleados sobre sus vulnerabilidades

¿Por qué son tan importantes los programas de formación en privacidad centrados en los empleados? Lo ilustraré con un experimento que realicé con dos grupos para evaluar su propensión a revelar información privada. Todos participaron en un taller de concienciación sobre seguridad que les enseñaba los riesgos de los *emails* de *phishing* y similares, y completaron una encuesta inmediatamente antes, otra justo después y una tercera dos semanas más tarde, respondiendo a preguntas como "¿Repites contraseña en distintas webs? ¿Usas la fecha de tu cumpleaños para tus contraseñas? ¿Compartes detalles personales en las redes sociales?". En el grupo de control, los participantes podían responder sí/no o saltarse las preguntas, mientras que el grupo de tratamiento, responder sí/no o "Prefiero no dar esta información". Este "empujón de privacidad" sirvió para que se dieran cuenta de que no tenían por qué responder si no querían. Quienes recibieron ese "empujón" acabaron compartiendo menos información que los demás.

Este experimento indica que todo buen programa de formación en privacidad debería concienciar a los empleados sobre la psicología conductual que hay detrás de sus decisiones de privacidad. El simple hecho de dar la posibilidad de pararse a pensar antes de tomar una decisión de este tipo (como hizo el "empujón") puede ayudar a los empleados a no revelar datos de forma automática, irreflexiva y potencialmente arriesgada.

Otro experimento que hice muestra que, cuando estamos contentos y relajados, somos más

propensos a revelar información personal que cuando nos encontramos en un estado anímico neutral, aunque nos preocupe la privacidad. De nuevo, si los errores humanos son la mayor causa de las brechas de seguridad, formar a los empleados para que resistan la fatiga de la privacidad y concienciarlos sobre los diversos trucos psicológicos en juego les ayudará a tomar mejores decisiones de privacidad.

Este vídeo ilustra con toda crudeza cómo los estafadores no dejan de idear métodos cada vez más retorcidos para manipularnos emocionalmente y conseguir que revelemos información privada sensible. Educar a tus empleados sobre qué factores humanos pueden explotar los estafadores es otro cortafuegos de privacidad para tu empresa.

Tests de intrusión y paladines de la privacidad

Para reforzar una mentalidad de "privacidad primero" en toda la organización, conviene aplicar la ingeniería inversa: partir del problema y analizar en retrospectiva la cadena de sucesos que condujo hasta él, con el fin de identificar los eslabones débiles y abordarlos directamente. Las empresas ya aplican este enfoque en el ámbito de la seguridad mediante tests de intrusión: reclutan a hackers éticos para poner a prueba sus redes y sistemas, detectar vulnerabilidades y defectos del software y el hardware y, a partir de ahí, fortalecer sus defensas técnicas. Las empresas deberían ser igual de proactivas con los tests de intrusión de la privacidad, pero aplicando la ingeniería inversa al cerebro humano en vez de a los sistemas de TI/TO.

Como en los tests de intrusión técnica, el primer paso es recopilar información, por ejemplo, mediante las encuestas de mi estudio. Este proceso puede incomodar a los empleados, porque deja al descubierto debilidades personales. Por eso es importante recordarles que sentirse vulnerables forma parte del experimento, y que este se desarrolla en un espacio seguro –un *sandbox*– precisamente para evitar que se sientan víctimas, algo que sí ocurriría en una situación real, como la del desafortunado empleado de Hong Kong.

Ayuda también contar con un alto nivel de confianza en la organización. Si no existe, tendrás que dedicar tiempo a generarlo, ya que el aprendizaje es más eficaz cuando los empleados sienten que pueden mostrar sus comportamientos reales y compartir información sin miedo a represalias. Con esos datos en la mano, los directivos podrán tomar medidas específicas: establecer políticas y directrices claras, como nuestros diez pilares, y los procedimientos

conductuales que los empleados deben seguir.

Otras medidas para garantizar el compromiso sostenido de la organización incluyen el nombramiento de “adalides de la privacidad” en los departamentos y la integración de las consideraciones de privacidad en las estructuras de gobernanza. Para ello, se necesitan personas con un gran interés por la privacidad y un amplio conocimiento, sobre todo en psicología y economía conductual. Si los hackers son expertos en manipulación, la organización necesita su equivalente: un “hacker de sombrero blanco”.

Lógicamente, esta función recaería en el director de tecnología o el de TI, aunque ambos cargos suelen centrarse en la parte técnica, no en la humana. Para cumplir con el RGPD, muchas empresas cuentan con un delegado de protección de datos (DPD), teóricamente encargado de impulsar esta agenda, pero que en la práctica suele quedar más absorbido por el papeleo del cumplimiento normativo que por los programas PETA. Lo ideal sería que el DPD asumiera el papel de principal impulsor de la privacidad y trabajara estrechamente con recursos humanos.

Es más, los programas PETA deberían ser una parte integral de cualquier proceso de incorporación, estableciendo el punto de partida de la organización sobre el que se crean los puntos de referencia. Las empresas también deberían priorizar los tests de intrusión de la privacidad en sus equipos de atención al cliente –su posición es más vulnerable– para convertirlos en su primea línea de defensa (acuérdate del vídeo).

Tal vez la mejor salvaguarda inmediata sea conseguir que la cultura de la privacidad arraigue entre los empleados de primera línea, porque permite abordar los comportamientos y capacidades cotidianos. Por eso, aunque resulte preocupante que en nuestras encuestas los líderes empresariales puntúen más bajo que el personal de operaciones en relación con los diez pilares, sería aún más inquietante que ocurriera lo contrario. Cuando solo los directivos piensan en la privacidad, esta suele reducirse al mero cumplimiento –a “marcar la casilla” de las obligaciones legales– y se descuida la dimensión cognitivo-conductual de la cultura corporativa.

La cultura de la privacidad debe incluir las capacidades metacognitivas, y eso exige un liderazgo claro desde arriba, al nivel del CEO y el consejo. Pero no toda la cultura se construye de arriba abajo: el trabajo de verdad, el de detectar y poner a prueba las vulnerabilidades de la plantilla, debe hacerse de abajo arriba.

Mi consejo final es confianza cero. Hay quien dice: “Confía primero, verifica después”, pero

cuanto más conectados estamos, más vulnerables somos; por eso, es la mentalidad más segura. Deja de pensar en la privacidad como algo aislado. Dado que los empleados toman cada vez más decisiones de privacidad en su día a día, si los formamos y dotamos de las herramientas adecuadas, podemos mejorar la ciberseguridad por defecto.

+INFO: "Insights on how data privacy officers can build a corporate privacy culture", de Tawfiq Alashoor, Maheshwar Boodraj, André Quintanilha, Sabrina Palme y Hussain Aldawood, *MIS Quarterly Executive* (2025).

VÍDEO: el webinar "From humans to machines: the keys to secure digital transformation", con Tawfiq Alashoor y los expertos en ciberseguridad Abdulrahman Alsafh y Jessica Buerger, está disponible para los miembros de la Asociación de Alumni del IESE aquí.

El investigador agradece el apoyo recibido en el marco del proyecto Project 2024-2-IE01-KA210-VET-000281740 — Training and Reskilling for Smart Manufacturing (TRANSFORM), financiado por la Unión Europea bajo el programa ERASMUS+. Los puntos de vista y opiniones expresados son únicamente los de los autores y no reflejan necesariamente los de la Unión Europea ni los del programa Erasmus+. Ni la Unión Europea ni la entidad financiadora pueden ser consideradas responsables de los mismos.

Este artículo forma parte de la revista IESE Business School Insight núm. 171 (enero-abril 2026).

https://www.youtube.com/embed/F78UdORll-Q

El coste oculto de un ciberataque: clientes que no vuelven

Un ciberataque no acaba cuando se restablecen los sistemas, ni se limita a los servicios online; acarrea costes duraderos para el consumidor.

Así lo apunta una investigación de la profesora del IESE Laura Wagner en la que, junto con

otros autores, analiza un gran supermercado omnicanal que sufrió una brecha de datos corporativos y el cierre de su tienda online durante una semana tras un ciberataque.

A partir de los datos de fidelización de más de 20.000 clientes, los investigadores compararon el comportamiento de compra antes y después del ataque. Las transacciones y los ingresos online cayeron alrededor de un 10% durante las 13 semanas posteriores al incidente, sin indicios de recuperación. Esto contrasta con estudios anteriores, que solo documentaban reacciones de mercado a corto plazo.

La tienda física tampoco compensó la pérdida. Aquí también los resultados divergen de investigaciones previas que sugerían que el canal offline puede amortiguar las disrupciones online. Es decir, el comercio omnicanal no es la red de seguridad que aparenta ser.

Con todo, no todos los clientes reaccionaron igual. Los que tenían rutinas online más previsibles (y por tanto estaban más directamente expuestos al ataque) fueron más propensos a dejar de comprar, mientras que los vinculados a un servicio de suscripción mostraron mayor resiliencia y más inclinación a seguir con la marca.

Todo ello apunta a que los ciberataques van mucho más allá de las consideraciones técnicas. Tu equipo debe estar alerta, porque el comportamiento de compra tras un ataque afectará a tu negocio mucho después de que los servicios online se hayan recuperado.

Este proyecto cuenta con el apoyo financiero del programa de investigación e innovación de la Unión Europea 2023 en virtud del acuerdo de subvención Marie Sklodowska-Curie nº 101152906. Los puntos de vista y opiniones expresados son únicamente los de los autores y no reflejan necesariamente los de la Unión Europea ni la European Research Executive Agency. Ni la Unión Europea ni la entidad financiadora pueden ser consideradas responsables de los mismos.

TAMBIÉN PUEDE INTERESARTE:

Donar datos salva vidas: el equilibrio entre privacidad y ética en la era digital

[Cuidado con los zombis digitales: cómo gestionar los fantasmas del pasado online]

[Los escenarios que amenazan tu privacidad]

Tawfiq Alashoor

Profesor de Operaciones, Información y Tecnología en el IESE. Su investigación se centra en la privacidad y ciberseguridad, sobre todo la toma de decisiones relacionada con las tecnologías basadas en la IA, así como en el análisis y diseño de sistemas de información de gestión (MIS).

www.iese.edu/es/insight