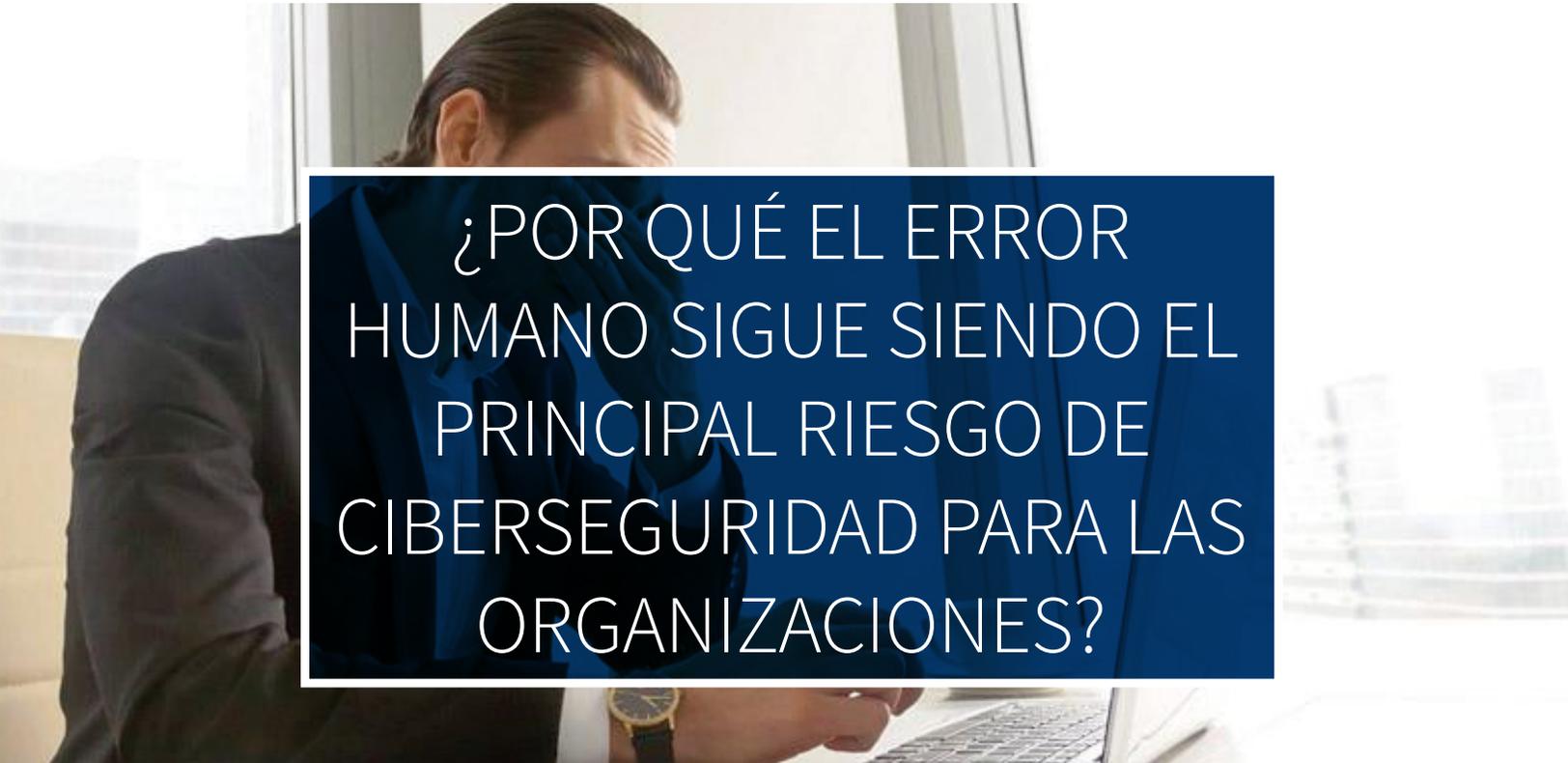




Managed secure IT | no matter what



¿POR QUÉ EL ERROR HUMANO SIGUE SIENDO EL PRINCIPAL RIESGO DE CIBERSEGURIDAD PARA LAS ORGANIZACIONES?

A pesar de las amenazas de los piratas informáticos y los estados nacionales, el error humano sigue siendo la principal preocupación de seguridad cibernética tanto para los ejecutivos de la suite C como para los responsables políticos, de acuerdo con un informe. Para combatir este problema, los profesionales deben invertir más en empleados, a través de la capacitación y la contratación, que, en tecnologías en los próximos dos años, según el informe.

Security

Sólo el 38% de los ejecutivos de C-suite dijeron que planean invertir en inteligencia artificial (IA) y aprendizaje automático para mejorar la seguridad en los próximos dos años, aunque estas tecnologías pueden ayudar a minimizar el error humano.



En términos de otras inversiones en seguridad durante ese período de tiempo, el 44% de los ejecutivos de C-suite dijeron que planean comprar un nuevo software con seguridad mejorada, y el 37% dijo que planean invertir en nuevas soluciones de infraestructura.

En los últimos cinco años, los ejecutivos de C-suite dijeron que han mejorado el software existente (60%), han capacitado al personal existente (57%), han comprado software nuevo con funciones de seguridad mejoradas (54%) e han invertido en nuevas soluciones de infraestructura (40%). Para mejorar la seguridad, el informe encontrado.

Amenazas crecientes

Cuando se les preguntó acerca de las mayores amenazas de seguridad para la industria de la tecnología específicamente, los encuestados de C-suite clasificaron los ataques de gobiernos extranjeros como los más altos (30%). Sin embargo, el 78% de estos ejecutivos dijeron que creen que la industria de la tecnología está bien equipada para proteger los datos. Solo el 35% de los ejecutivos dijo que creía que era responsabilidad del gobierno proteger los datos de los consumidores, destacando el papel fundamental que desempeña el sector tecnológico.

Si bien el gobierno tiene un papel importante que desempeñar para mantener seguros los datos de Estados Unidos, el panorama de la seguridad cibernética cada vez más peligroso de hoy en día significa que no se puede esperar que supere a los atacantes por su propia cuenta. El gobierno de los EE. UU. Y las empresas necesitarán confiar más en el sector de la tecnología para avanzar en la defensa cibernética de la nación. Se pueden construir centros de datos, contratar talentos y datos seguros a escala de manera más eficiente que cualquier cliente individual.



Cuando se trata de la IA, solo el 33% de los ejecutivos encuestados dijeron que planean adoptar e implementar la IA y el aprendizaje automático a su máximo potencial. Sin embargo, también dijeron que creen que las tecnologías autónomas basadas en estas herramientas mejorarán la forma en que protegen y defienden las amenazas de seguridad, según el informe.

Fuente de información
<https://www.techrepublic.com>

Síguenos en nuestras redes sociales:



MexisMX



Servicios
Administrados
Mexis, S.A. de C.V.



Mexis TI



Servicios
Administrados
Mexis, S.A. de C.V.