Always Designing for People®

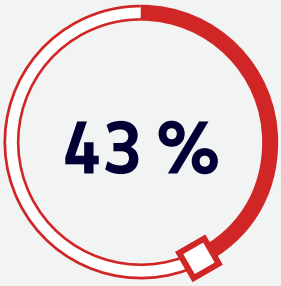
CÓMO FOMENTAR LA RESILIENCIA CIBERNÉTICA

Los sistemas de nómina contienen algunos de los datos más confidenciales de una organización, como identificadores personales, datos bancarios, información de sueldo y registros fiscales. Esto los convierte en un objetivo atractivo para los ataques a la ciberseguridad.

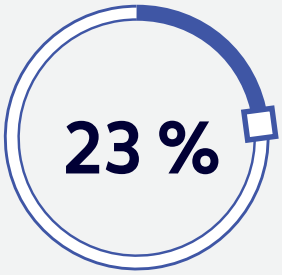
En nuestra encuesta sobre nómina global, **El potencial de la nómina en 2026**, se observa un aumento significativo de este tipo de incidentes. El 70 % de los responsables de nómina reportan al menos un incidente de ciberseguridad que afectó sus operaciones de nómina en los últimos 24 meses. Esta cifra representa un aumento con respecto al 57 % del año anterior.

El incremento de 13 puntos porcentuales sugiere que la amenaza seguirá creciendo a medida que las estrategias de ataque se vuelvan más sofisticadas.

Las nuevas tecnologías y herramientas, incluidas las de inteligencia artificial (IA), facilitan más que nunca la generación de grandes cantidades de correos electrónicos de phishing de una sola vez o la creación de llamadas de spam sorprendentemente convincentes. La nómina está adquiriendo un rol cada vez más estratégico en las organizaciones, por lo que contar con equipos resilientes será más importante que nunca.



sufrió uno o dos incidentes de seguridad en los últimos 24 meses que afectaron su nómina



sufrió tres o cuatro incidentes de seguridad en los últimos 24 meses que afectaron su nómina

sufrió cinco o más incidentes de seguridad en los últimos 24 meses que afectaron su nómina

De la concienciación a la preparación

Los equipos de nómina no ignoran este riesgo. La mayoría de los líderes comprenden la exposición que conlleva. Sin embargo, para lograr que las organizaciones estén preparadas para esta nueva realidad, se sigue necesitando mucho trabajo.

Solo el 41 % de las organizaciones cuenta con un plan de contingencia para la nómina en toda la empresa. Esto significa que casi seis de cada diez organizaciones (muchas de las cuales ya han sufrido un incidente de seguridad) aún operan sin un plan de respuesta coordinado.

No obstante, las organizaciones están mejorando. El 49 % ya dispone de planes y protocolos para algunos de sus países, frente al 33 % del año pasado.

Invertir en capacidades de seguridad especializadas

La respuesta a las crecientes amenazas se integra cada vez más en las operaciones de nómina. El 47 % de los equipos de nómina ahora cuentan con recursos dedicados a la seguridad de datos. Se trata de profesionales centrados específicamente en la protección de los datos y sistemas de nómina. Otro 37 % afirma que le gustaría desarrollar esta capacidad, lo que sugiere un amplio reconocimiento de que la seguridad ya no puede ser responsabilidad exclusiva de los equipos de TI.

El 33 % de los líderes de nómina han señalado la seguridad de datos como una de las principales prioridades de mejora global para los próximos dos o tres años. Esto la sitúa junto a la conformidad y la elaboración de informes como una preocupación fundamental.

Cómo desarrollar resiliencia a nivel local y global

A medida que la nómina adquiera un rol cada vez más estratégico en las organizaciones, contar con equipos resilientes será más importante que nunca. Las organizaciones mejor posicionadas para administrar las amenazas de ciberseguridad son aquellas que no solo responden de forma reactiva ante un incidente, sino que cuentan con experiencia en seguridad integrada en todos los niveles de sus operaciones.

Esto implica desarrollar y probar planes de contingencia tanto a nivel local como a nivel global, garantizar que la nómina tenga la experiencia y la autoridad para administrar los problemas de seguridad, establecer protocolos claros de respuesta a incidentes (incluso con proveedores externos) y mantener una estrecha coordinación con el Departamento de TI.

Las organizaciones que consideran la protección de datos como un motor estratégico (no solo como una obligación de conformidad) están mejor posicionadas para prevenir incidentes y recuperarse más rápidamente cuando ocurren.

41 %

han desarrollado un manual de estrategias y un plan de contingencia en todos los países

49 %

ha desarrollado manuales de estrategias y planes para algunos de los países

9 %

ha considerado crear un plan, pero no ha implementado ninguno hasta el momento

1 %

no ha considerado crear un plan de este estilo

DESCUBRE MÁS

Entérate de cómo las organizaciones están reforzando la seguridad de la nómina y desarrollando la ciberresiliencia en el informe completo, El potencial de la nómina en 2026: encuesta de nómina global.

WF3615202

Always Designing for People®