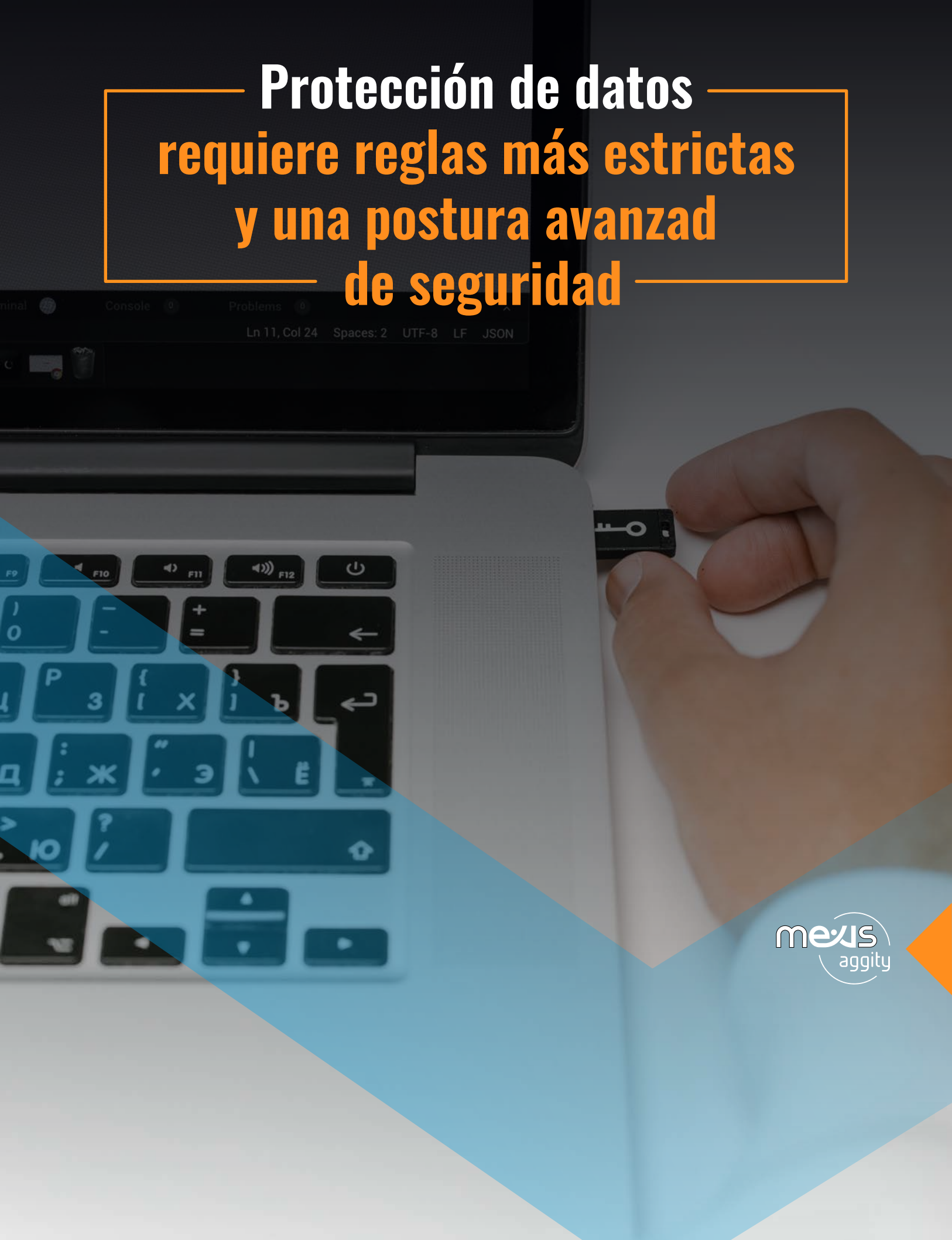
Protección de datos requiere reglas más estrictas y una postura avanzad de seguridad



mews aggity

Aunque la privacidad de los datos todavía es una asignatura pendiente para muchas compañías, el Día de la Privacidad de Datos representa una oportunidad para tomar conciencia de su importancia y difundir las mejores prácticas para su protección.

Con las leyes de privacidad de datos extendiéndose y endureciéndose a nivel mundial, el cumplimiento regulatorio se ha convertido en un complicado proceso que afecta a todas las áreas de una organización. De hecho, Gartner predice que, para 2024, el 75 % de la población mundial tendrá sus datos personales cubiertos por alguna normativa sobre privacidad.

Desde la creación del 28 de enero como Día de la Privacidad de Datos en 2007, el panorama de la legislación mundial sobre la privacidad ha cambiado notablemente. Leyes integrales como el GDPR, la CCPA y la CPRA imponen requisitos estrictos a las empresas y otorgan nuevos derechos a las personas.

Sin embargo, de acuerdo con datos revelados en Industry Today, el 92 % de las empresas aún no están completamente preparadas para cumplir con la Ley de Privacidad CCPA ni con la Ley de Derechos de Privacidad (CPRA), mientras que 91 % también muestra poca preparación para el

Reglamento General de Protección de Datos (GDPR). Basten un par de ejemplos: en el tercer trimestre de 2022 se aplicó la CCPA con una multa de 1,2 millones de dólares a la empresa de retail Sephora por vender información personal de los consumidores a empresas de seguimiento en línea sin su consentimiento. Además, a inicios de este año, la empresa matriz de Facebook, Meta, fue condenada a pagar dos multas: una, de 210 millones de euros (222,5 millones de dólares) por infracciones del GDPR; la segunda, de 180 millones de euros, relacionada con infracciones de la misma ley por parte de Instagram.

Combinadas, las sanciones ascienden a 390 millones de euros (414 millones de dólares) y las respectivas consecuencias reputacionales.

”El Día de la Privacidad de Datos brinda un recordatorio anual de que la privacidad y la seguridad de los datos están indisolublemente unidas. A pesar de que las leyes de todo el mundo reconocen cada vez más los derechos de las personas para controlar cómo se recopila, utiliza y almacena su información, también imponen una mayor responsabilidad a las empresas por ser buenos administradores de esos datos y responsabilizarlos cuando no lo hacen”, comenta especialista.

Especialista señala que es importante que tanto los usuarios como las organizaciones reflexionen sobre la protección de datos. “Las personas, como usuarios de la tecnología, tienen el derecho a que su información personal dentro del ciberespacio sea protegida.

Lo ideal es que siempre tengan claro qué datos personales han entregado a determinadas organizaciones para su almacenamiento y tratamiento y, sobre todo, que hayan leído antes las políticas de privacidad y condiciones y términos de uso de dichas organizaciones.

Por su parte, las organizaciones presentes en el medio digital tienen el deber de cumplir con requisitos de ciberseguridad y proteger la información de sus clientes o usuarios. Resulta fundamental que cada organización satisfaga estándares de seguridad internacionales para la protección de datos; defina correctamente unos términos y condiciones de uso de los datos, así como unas políticas de privacidad; sea plenamente consciente del peligro que representan las vulnerabilidades de seguridad en los sistemas informáticos; y tenga claro que un ciberataque puede dejar expuestos los datos sensibles de sus clientes o usuarios para usos ilícitos y por ende afectar su reputación”.

Especialista concuerda que proteger los datos de actores malintencionados es responsabilidad de todos. “Las organizaciones necesitan las defensas de ciberseguridad más sólidas posibles y las personas deben comprender las amenazas y cómo evitar ser víctimas de ellas, asumiendo su responsabilidad personal y entendiendo el impacto de compartir datos voluntariamente con servicios como las redes sociales”, dice.

La importancia de la ciberseguridad en la protección de datos y la privacidad

La ciberseguridad es esencial para garantizar la privacidad de la información, afirma especialista, **cuando el aumento de la adopción digital en toda Latinoamérica y el uso masivo de dispositivos móviles hace que los usuarios enfrenten un mayor riesgo de ataques cibernéticos y robo de información.**

"La industria de ciberseguridad prevé un incremento del 50 % en el número de incidentes relacionados con redes sociales y datos personales, así como un aumento en el riesgo de dispositivos móviles y aplicaciones maliciosas. Sectores como el financiero y las plataformas de pagos electrónicos, eCommerce, retail y portales de criptomonedas son especialmente vulnerables por la cantidad de información sensible que manejan".

Además, es importante priorizar estrategias que les permitan anticiparse y responder eficazmente ante la presencia de adversarios en su infraestructura, recomienda especialista."Tradicionalmente, se asume que las amenazas están fuera de la organización; sin embargo, no se mide de manera intencional y continua los contactos con infraestructura utilizada por ciberdelincuentes", comenta. Frente a ello, un modelo de evaluación continua del compromiso (Continuous Compromise Assessment) puede ayudar a las empresas a identificar compromisos en tiempo real y erradicar las amenazas presentes en la red con precisión y velocidad.

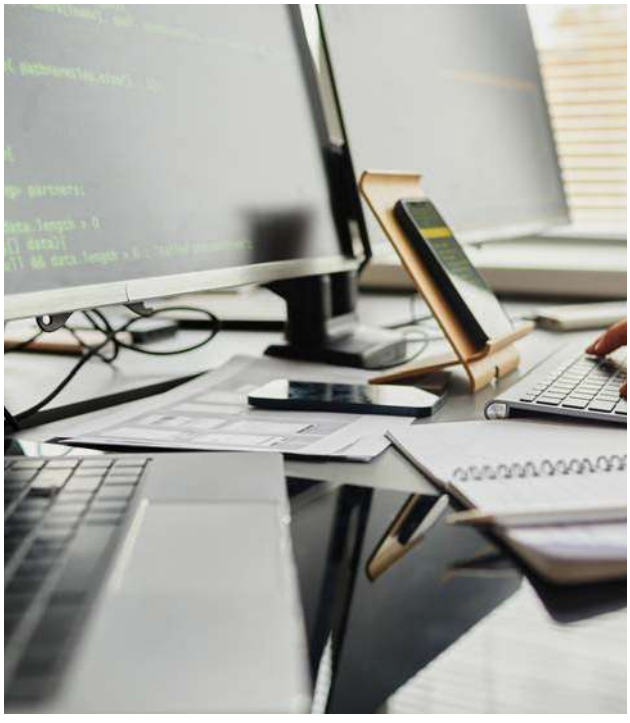
En el caso de que las organizaciones desarrollen programas que almacenan o manejan datos personales y confidenciales de forma insegura, **lo que corresponde es realizar pruebas de seguridad continuas con herramientas automatizadas y hackers éticos altamente certificados,** recomienda especialista.

Así, las organizaciones pueden identificar y reportar las vulnerabilidades presentes en sus sistemas, para que puedan remediarlas cuanto antes. “Gracias a estas pruebas, las organizaciones pueden aumentar la seguridad de su tecnología, evitar impactos por ciberataques, así como sanciones, y mantener la confianza de sus usuarios”, declara especialista.

En el caso del entorno industrial, la amenaza puede ser mayor. “El mal manejo de la privacidad y la protección de datos personales en instalaciones industriales pueden causar ciberataques con graves consecuencias en la población, ya que los cibercriminales, **con los datos adquiridos, pueden conocer contraseñas o deducirlas y así acceder a los sistemas industriales e interrumpir servicios como la distribución de agua, gas y generación eléctrica.** Por ello, es importante la visibilidad y monitoreo de toda la infraestructura crítica para poder **identificar de manera inmediata cualquier anomalía en ambientes de tecnología de las operaciones (OT) e internet de las cosas (IoT)”**, refiere especialista.

Pinal resalta que, **a medida que las amenazas se vuelven más complejas, los profesionales de la ciberseguridad deben adaptarse y aprender nuevas destrezas para defender sus entornos.** "Es necesario adoptar modelos óptimos de seguridad para proteger tanto la infraestructura crítica como los datos personales de los usuarios, así como los secretos industriales de las empresas. **Esto incluye la implementación de medidas de encriptación, autenticación y control de acceso seguro contra el robo o manipulación de los datos personales",** señala.

Para evitar consecuencias escalables, dice el ejecutivo, "es indispensable que las empresas y organizaciones tengan políticas y procedimientos para responder rápida y adecuadamente a incidentes de seguridad relacionados con los datos personales. Proteger los datos personales es [proteger] no solo al individuo, sino a la comunidad entera".



Privacidad y gestión del riesgo

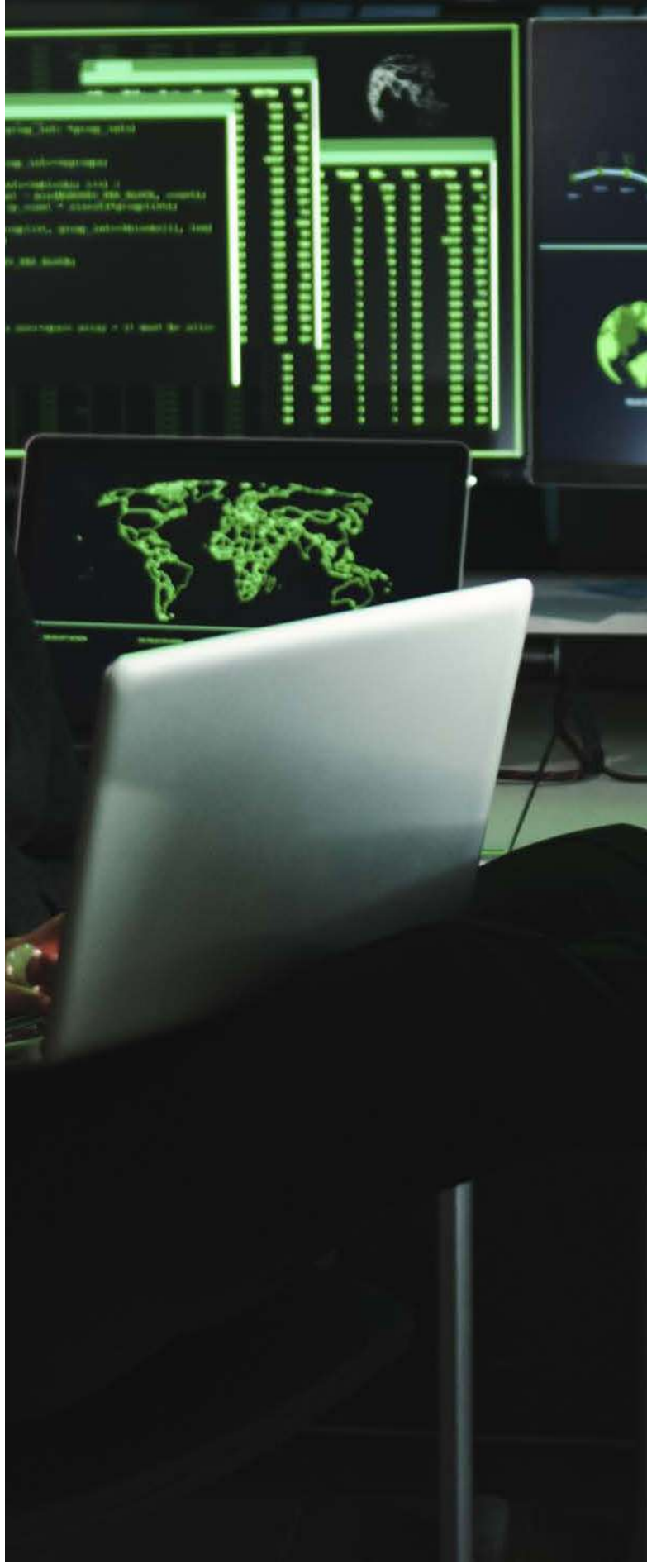
Dentro del sector financiero, uno de los más regulados respecto a la protección y privacidad de los datos por la gran cantidad de información que maneja de cada uno de sus clientes, la recomendación es **adoptar modelos de control dentro de estrategias de gestión del riesgo y prevención del fraude.**

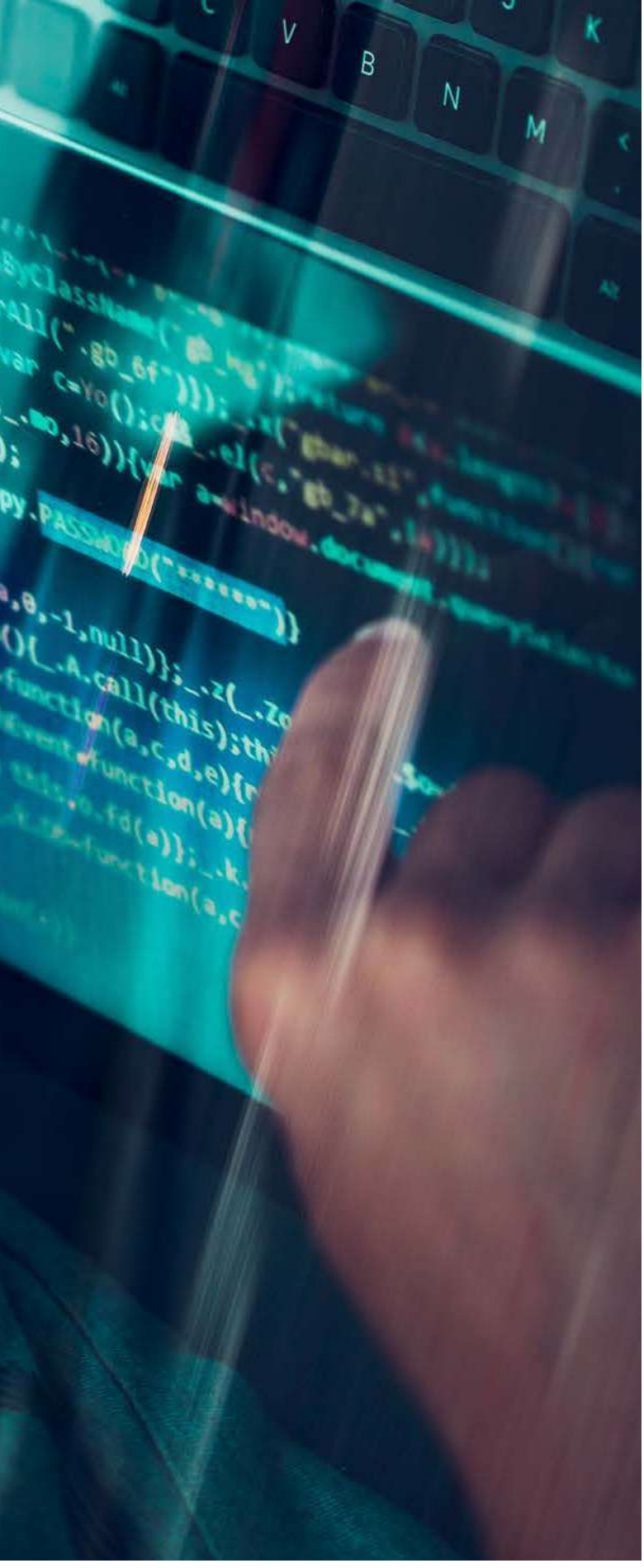
La idea es usar **"soluciones que les permitan a los profesionales del riesgo y a sus equipos detectar y prevenir los posibles peligros que puedan presentarse durante la ejecución de transacciones"**, especialmente en las empresas que forman parte del sector de procesamiento de pagos, aconseja especialista.

"La industria financiera requiere contar con soluciones que consideren normativas tales como PCI-DSS, las cuales tienen como objetivo el manejo seguro de los datos de los clientes. Estas normativas existen para ayudar a reducir el fraude relacionado con transacciones de tarjetas o dispositivos digitales, no solo se convierten en mandatorias para ciertos escenarios, sino [que son] necesarias para operar de manera segura", declara especialista.

En el caso de las fintech, estas han optado progresivamente por el análisis de nuevas fuentes de datos alternativos confiables, que incluyen información de SIM cards, flujos de llamadas y mensajes de texto, banca abierta, registro de pagos en efectivo, cuentas en redes sociales e historial de viajes. “El manejo adecuado y seguro de estas fuentes ha favorecido la oferta de servicios mucho más asequibles y dirigidos a una base de clientes más diversa sin aumentar el riesgo de impagos. A partir de ello, **muchas fintechs han logrado construir un perfil crediticio más preciso, reducir el fraude y avanzar con la inclusión financiera en toda Latinoamérica”**, expone especialista, una plataforma de toma de decisiones con IA.

Especialista señala que la recolección y el almacenamiento de datos personales sensibles siempre conlleva un riesgo potencial de ciberataques y un posible robo de información. “Por eso, es esencial que las instituciones financieras adopten fuentes confiables de datos financieros y medidas de seguridad para proteger la privacidad de sus clientes y evitar el aumento del fraude en sus ofertas crediticias. (…) Por su parte, las personas deben prestar especial atención al manejo que le dan a la información personal que exponen en el mundo digital, ya que ésta puede poner en riesgo sus cuentas bancarias o afectar su score crediticio”, concluye.





Cómo cumplir las regulaciones de privacidad de datos

Prepararse para las normativas sobre protección de datos existentes puede parecer complicado, **te dejamos algunas recomendaciones para facilitar este cumplimiento:**

1. **Identificar qué marcos regulatorios afectan a una empresa**, de modo que los responsables de seguridad puedan determinar qué soluciones se necesitan para cumplir las normativas.
2. **Realizar una evaluación de riesgos** para identificar brechas en su postura de seguridad, comprender sus procesos de seguridad actuales y, en caso de que exista algún desfase o brecha, priorizar su resolución en función de su gravedad.
3. **Trazar una hoja de ruta** con los pasos a seguir en cada etapa según las prioridades identificadas en la evaluación de riesgos.
4. **Realizar copias de seguridad.** Las copias de seguridad protegen a las empresas contra fugas y pérdidas de datos, datos dañados y otros problemas relacionados.
5. **Formar a los empleados en la protección de datos**, ya que es la manera de asegurarse de que el error humano no interfiera en el cumplimiento normativo de la compañía.

"El Día de la privacidad de datos representa una oportunidad para que las organizaciones y las personas aumenten su conciencia sobre la privacidad y la protección de datos, se difundan las mejores prácticas y se discuta por qué es importante la privacidad", subrayan en WatchGuard Technologies.

Recomendaciones para usuarios

Porque la educación en ciberseguridad como usuarios es un eslabón clave, especialista recomienda reducir el nivel de exposición de los usuarios en las redes:

- Minimice la información personal que expone en sus redes sociales;
- Mantenga su computadora y dispositivos móviles con las últimas actualizaciones del sistema; y
- Active el antivirus y firewall en las computadoras personales y de la familia.
- Piense dos veces antes de dar clic: Sea consciente de dónde hace clic, especialmente en los enlaces o archivos adjuntos de los mensajes sms o emails.
- Utilice una VPN para añadir una capa adicional de seguridad entre su dispositivo e internet.
- Mantenga el software actualizado con regularidad para evitar fallos de seguridad.
- Utilice un DNS de confianza, para asegurarse de que la información que recibe de internet es segura.
- Borre las cookies de los principales navegadores web. Las cookies pueden representar un riesgo para la privacidad debido a la cantidad de información que pueden contener, como identificación personal para ayudar a completar formularios automáticamente en los navegadores. Si prefiere proteger su privacidad cuando se trata de cookies, es posible que desee eliminarlas.
- Utilice un gestor de contraseñas para crear contraseñas únicas y garantizar la privacidad de la identidad digital.
- Active la autenticación multifactor (MFA), para que sea obligatorio identificarse a través de varios pasos de verificación y credenciales para poder acceder a datos.

Fuente de información: computerweekly.com