VU LABS

Informe 2018-2019

CIBERSEGURIDAD

en entornos digitales

corporate@vusecurity.com vusecurity.com @vusecurity /vusecurity /vusecurity

Bienvenidos al informe 2018 de ciberseguridad en entornos digitales

Con el objetivo de concientizar y poner a disposición información concreta en el campo de la seguridad informática, VU creó su propio laboratorio de investigaciones, VU Labs, el cual se constituye como una herramienta esencial para la toma de decisiones en el campo de la ciberseguridad de cualquier empresa u organización.

Durante el último año, el incremento de noticias sobre fraudes, ataques cibernéticos y amenazas en la red, que alcanzan tanto a particulares como a miembros del ámbito corporativo, ha demostrado la importancia de generar consciencia social sobre la necesidad de proteger la identidad digital de las personas, prevenir los fraudes y mantener la privacidad en el mundo online.

En vista de la cada vez mayor variedad y diversificación de amenazas, **desde VU hemos decidido analizar la ciberseguridad teniendo en cuenta la percepción de usuarios y líderes corporativos para definir tendencias, los alcances de *IoT*, la detección de potenciales riesgos y entender la visión del usuario final frente a los ataques actuales.** Para lograrlo, VU Labs realizó, por tercer año consecutivo, una encuesta a toda nuestra base de datos de América Latina, incluyendo clientes y *prospects.*

Gracias a la validación de los profesionales que conforman el laboratorio y la colaboración de organizaciones de América Latina, hoy podemos compartir con ustedes los valiosos resultados.

VU | Sebastián Stranieri
CEO de VU

Metodología de investigación

El relevamiento se realizó utilizando una encuesta auto-administrada que fue respondida vía correo electrónico por más de 600 miembros de organizaciones de 16 países, incluyendo Argentina, Bolivia, Chile, Colombia, Costa Rica, Ecuador, España, Guatemala, Italia, México, Panamá, Perú, República Dominicana y Uruguay, entre otros.

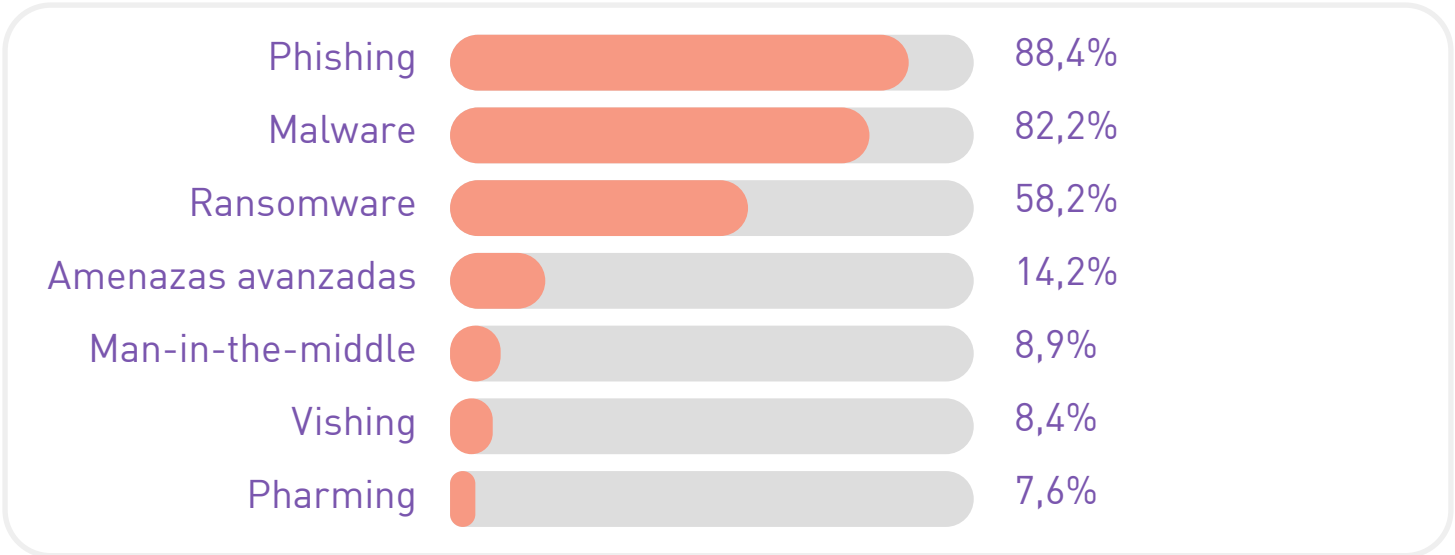
Análisis de resultados

La investigación muestra resultados sobre las metodologías de fraude más frecuentes, los problemas más usuales de ciberseguridad a nivel corporativo y el futuro de las criptomonedas y la Internet de las Cosas (*IoT*). Al mismo tiempo, provee *insights* valiosos sobre la frecuencia con la que ocurren los fraudes, si hay sectores encargados de la ciberseguridad en las empresas, y cómo reaccionan los usuarios y las compañías cuando surgen, lo que nos provee datos sobre cuánto saben sobre seguridad de la información en general.

El problema: percepción

Ataque cibernético más frecuente

Al consultarle a los participantes sobre las amenazas online que perciben como más frecuentes, el **88,4%** destaca el ***phishing*** y el **82,2%** menciona al ***malware***, mientras que el **58,2%** se refiere al ***ransomware***. La percepción se mantiene constante a través de los diferentes países encuestados.



Fraudes más frecuentes

¿Qué es el ***phishing***?

El concepto hace referencia a una metodología mediante la cual el estafador se hace pasar por una persona o una empresa de confianza en una aparente comunicación oficial electrónica, usualmente email o alguna plataforma de mensajería instantánea, para adquirir información confidencial.

¿Qué es el ***malware***?

Malware es la abreviación de *malicious software* y es un término que engloba a todo tipo de aplicación o código informático malicioso que trabaje para dañar un sistema o causar el mal funcionamiento de un programa o dispositivo. Incluye a todos los virus, troyanos ***(trojans***), gusanos (***worms***), ***keyloggers***, ***botnets*** y ***spyware.***

¿Qué significa ***man-in-the-middle***?

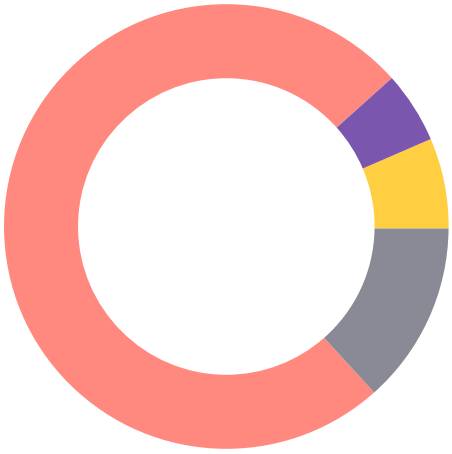
Man-in-the-middle, también conocido como ataque de intermediario, MitM o JANUS, es un ataque criptográfico en el cual el atacante intercepta mensajes entre dos víctimas sin que éstas perciban que la conexión ha sido interferida. Este tipo de ataque es particularmente común en redes WiFi sin cifrar.

¿Qué es el ***ransomware***?

Es un código que cifra la información de la computadora e ingresa una serie de instrucciones que el usuario debe seguir para recuperar el control de sus archivos, generalmente pagando una suma de dinero.

La ciberseguridad y la banca

¿Cuál es su percepción en relación a la ciberseguridad y la banca?



- **75,1%** **La inversión en soluciones es suficiente.**
- **13,3%** Deberían **seguir invirtiendo** para prevenir fraudes y **proteger la identidad digital de los usuarios.**
- **6,7%** **NO han invertido.** Los sistemas son más inseguros debido al aumento de amenazas.
- **4,9%** **NO han invertido**. Los sistemas son igual de inseguros.

Al consultarle a los encuestados con respecto a la seguridad en la banca, más del 75% considera que los bancos han invertido en soluciones de ciberseguridad y que éstas han sido efectivas para aumentar la seguridad de sus instituciones, reducir el fraude y proteger la identidad de sus clientes. Tan sólo el 11% de los encuestados considera que los bancos no han invertido en este tipo de medidas.

¿Qué acciones generan más estafas frecuentes en redes sociales?

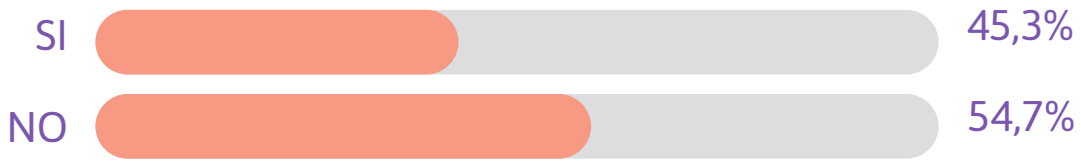
Considerando el gran impacto de las redes sociales, es importante evaluar también cuál es la percepción de los encuestados respecto a los ataques a través de dichas plataformas. Al consultar cuáles son las estafas más frecuentes, el **61,8%** considera que la modalidad principal son las ofertas falsas para unirse a nuevos grupos o participar en eventos, y las aplicaciones falsas (**50,7%**).

El problema y cómo afecta a las empresas

Los problemas más comunes de seguridad informática a nivel corporativo.

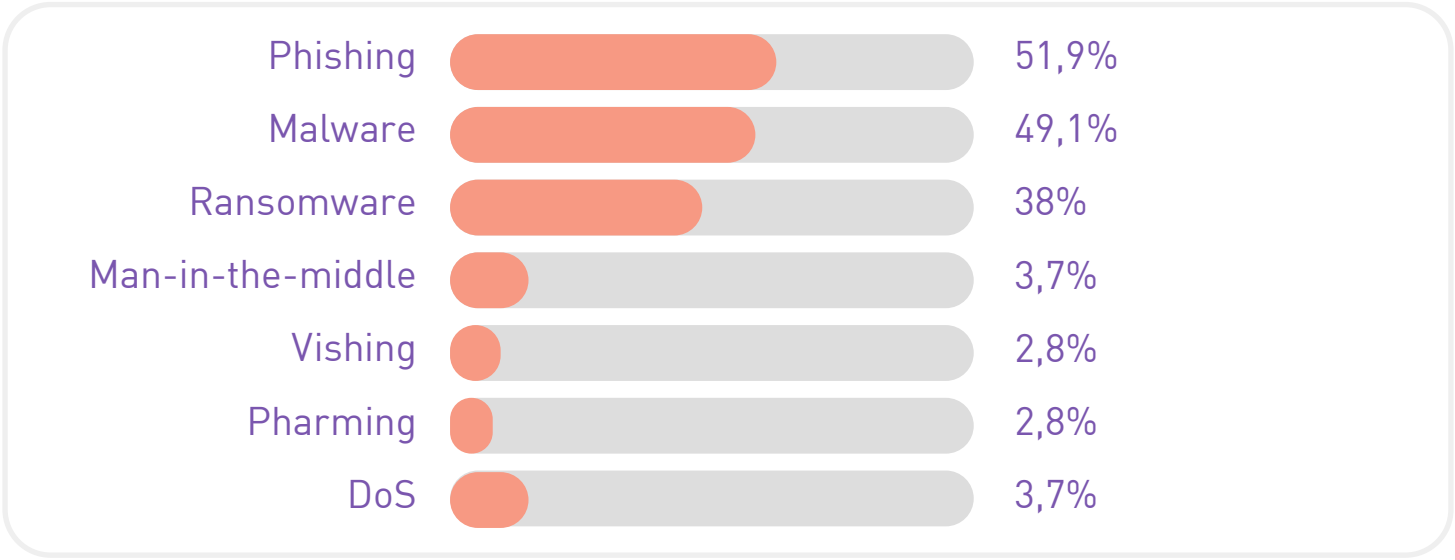
Al ser consultados sobre qué tipo de ataques son los más frecuentes en las empresas, los encuestados coincidieron en mencionar el ***phishing*, el *malware* en general y el *ransomware***, que afectan por igual a todas las industrias y todos los países, dado que todos los sectores son vulnerables a ser atacados si no cuentan con los sistemas de seguridad adecuados.

Su empresa, ¿ha sido víctima de algún tipo de ciberataque en los últimos 3 años?



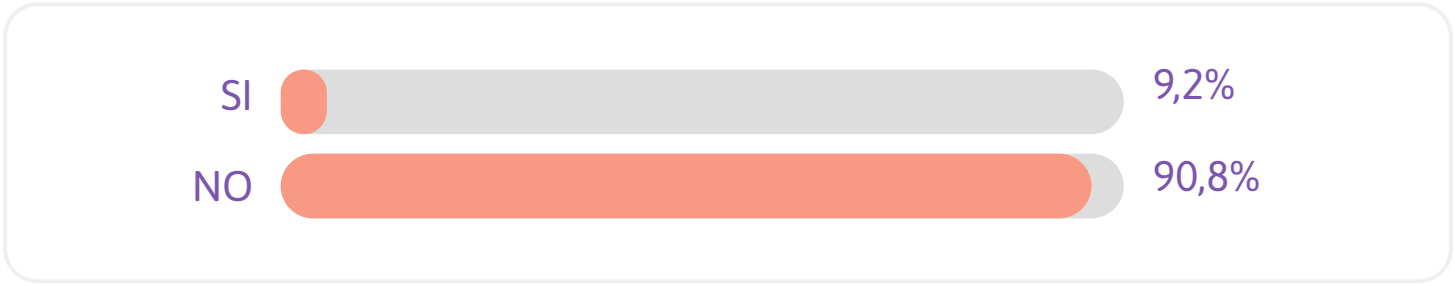
Casi la mitad (el **45,3%**) de las organizaciones participantes asegura haber sido víctima de al menos un ciberataque durante los últimos tres años.

¿Qué tipo de ciberataque cree que ha sufrido?



La percepción de los ataques más frecuentes coincide con la realidad, ya que los ataques más frecuentes en empresas de América Latina durante 2018 fueron ***phishing, malware, ransomware, man-in-the-middle, DoS, pharming y vishing.***

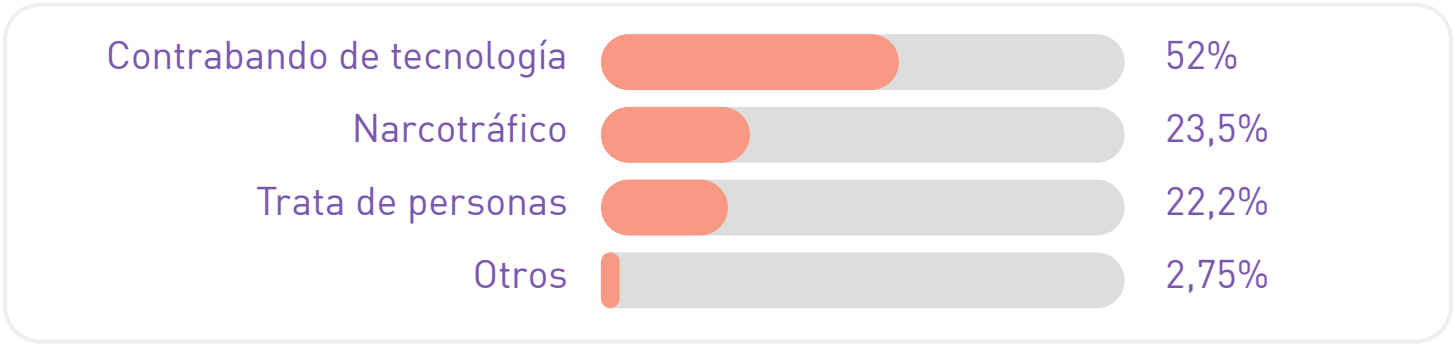
El ataque, ¿le generó pérdida de clientes?



De todas maneras, **sólo un 9,2% de los afectados admite haber perdido clientes como consecuencia de los ataques.** Esta tendencia se mantiene constante en todos los países.

Más de la mitad de los encuestados cree que este tipo de ataque es utilizado para financiar, en primer lugar, el contrabando ilegal de tecnología y en segundo lugar, el narcotráfico.

¿Qué cree que ayuda a financiar el ***ransomware***?

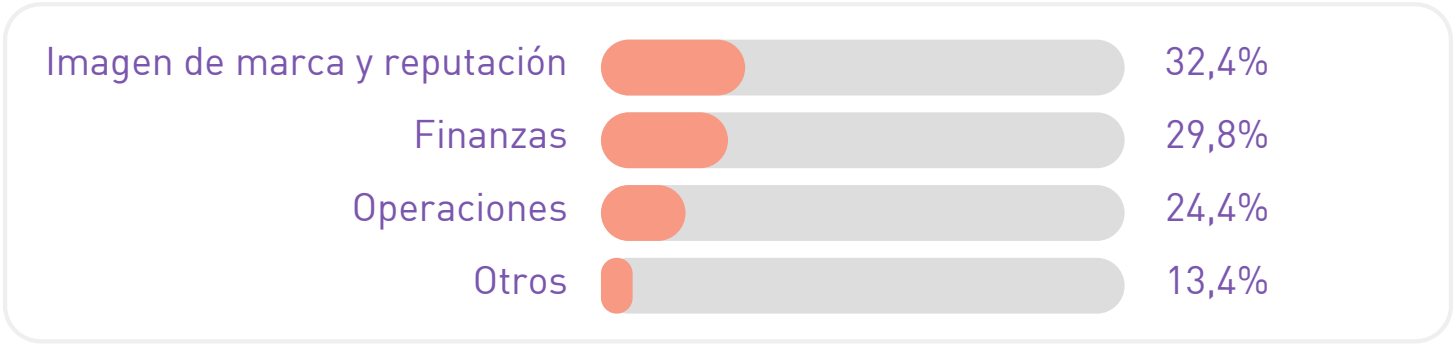


¿Cuidan los usuarios su seguridad cibernética?

Siendo el *phishing* el ataque online más frecuente, la prevención de fraude y la protección de la identidad adquieren cada vez mayor importancia. En el último año, los ataques automatizados a corporaciones fueron noticia más de una vez, al causar el robo de datos de miles de millones de usuarios alrededor del mundo.

La autenticación de doble factor de autenticación se consolida como una herramienta fundamental para proteger la identidad de los usuarios, seguida de cerca por el análisis de patrones de comportamiento, que facilita la validación de la identidad y la obtención de información adicional para verificar movimientos sospechosos e inusuales.

¿Cuál cree que es el área más afectada por una brecha en ciberseguridad?

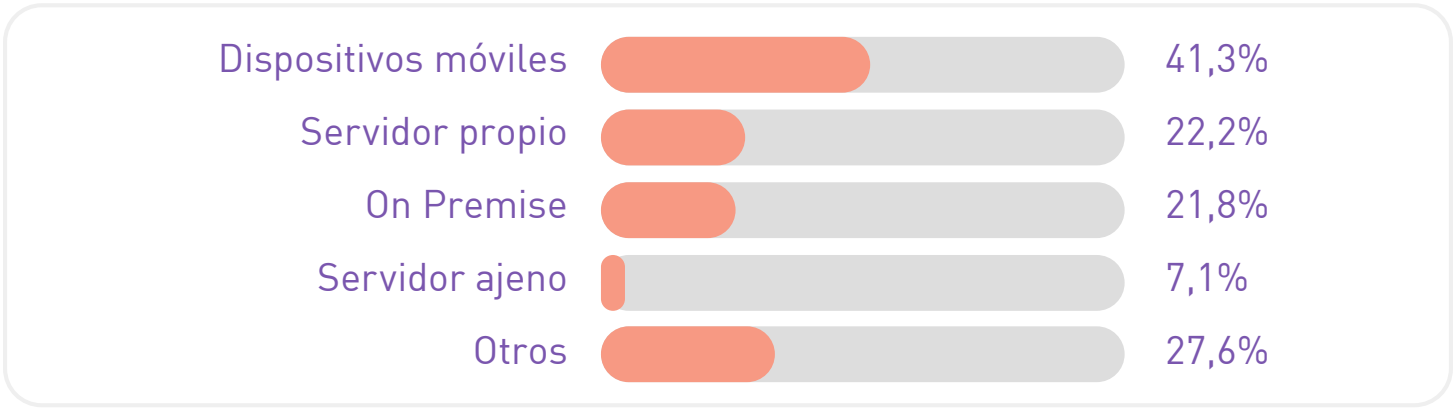


El 32,4% de los encuestados opina que la imagen de marca y reputación es el sector más afectado por las brechas de ciberseguridad. Un 29,8% piensa que este tipo de ataques afecta de manera negativa las finanzas de la compañía y finalmente, un 24,4% piensa que el impacto se hace notar sobre las operaciones.

Los únicos países donde la tendencia varía son Ecuador y Guatemala, donde se cree que los ataques tienen mayor impacto en las finanzas que en la imagen de marca.

Vulnerabilidades en las instituciones

¿Cuál considera que es la fuente de ataques cibernéticos más vulnerable de su empresa?



Los encuestados consideran que los dispositivos móviles son los más vulnerables con respecto a los ciberataques (41,3%), seguido por un servidor propio (22,2%), los equipos *on premise* (21,8%) y luego, la información en la nube en un servidor ajeno (7,1%).

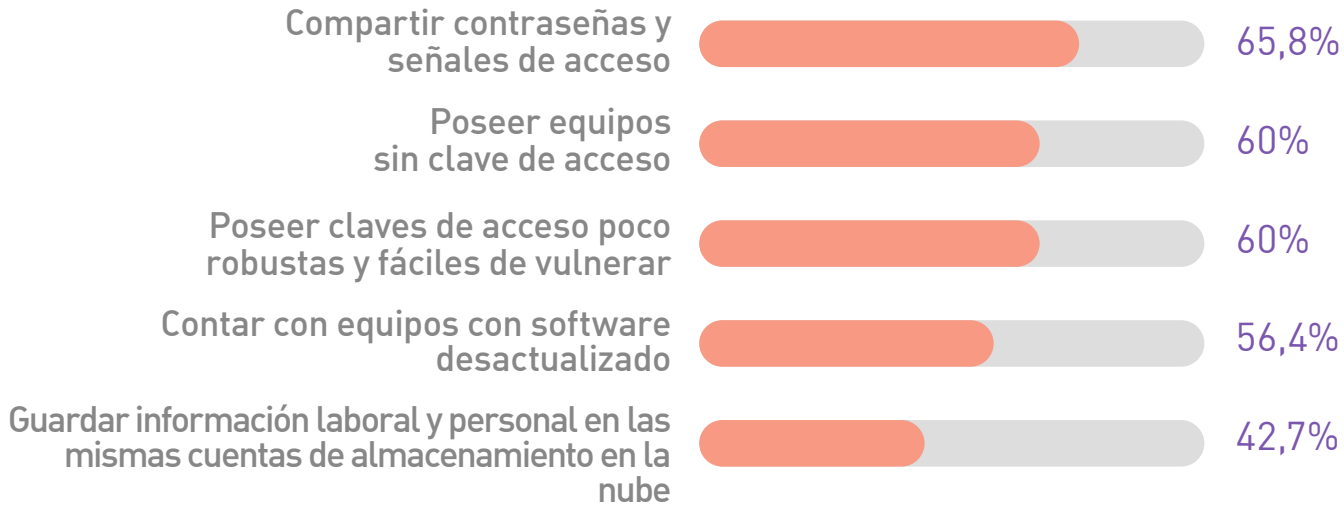
Sin embargo, esta percepción no se traslada a los hechos, ya que el 83,1% de los encuestados declara que no ha experimentado delitos cibernéticos a través de dispositivos móviles en los últimos 6 meses. Esta tendencia se mantiene en todos los países.

Personalmente, ¿ha experimentado delitos cibernéticos a través de sus dispositivos móviles durante los últimos 6 meses?

Al profundizar con respecto a cuáles son los comportamientos de los usuarios que vuelven inseguros a los dispositivos móviles, **lideran el ranking el compartir contraseñas y claves de acceso,** poseer equipos sin clave de acceso y el uso de contraseñas poco robustas.

Todo esto refuerza el concepto de que la seguridad depende del usuario y el uso que éste le dé a la tecnología.

¿Qué tipo de comportamiento de los usuarios con dispositivos móviles considera que genera mayores posibilidades de violación de seguridad?

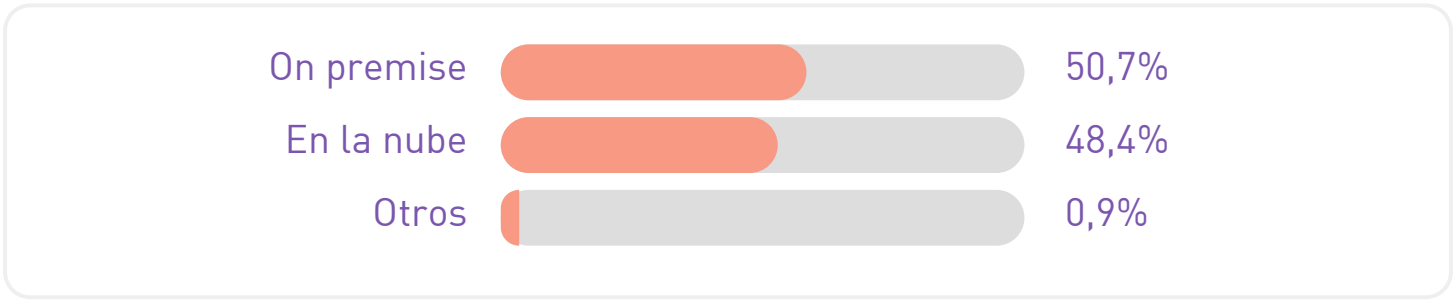


Métodos de prevención

Almacenamiento seguro

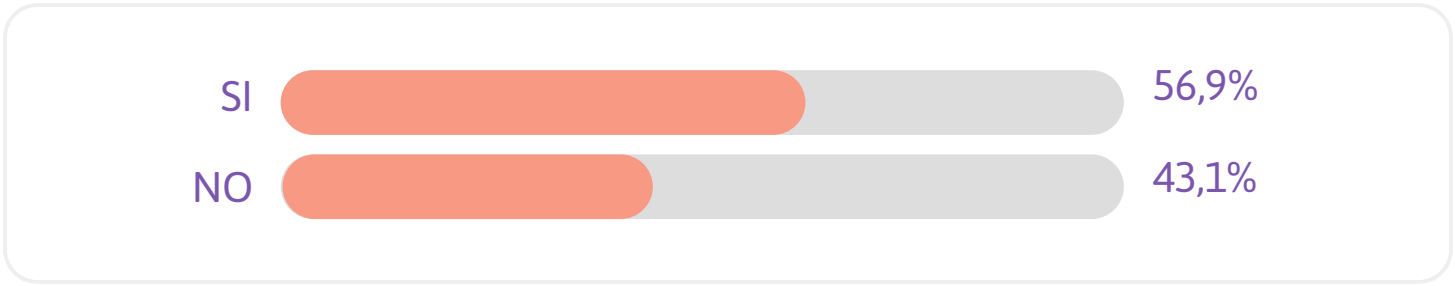
Respecto a los métodos seguros de almacenamiento, **las respuestas están divididas en partes prácticamente iguales: el 50,7% considera que es más seguro guardar información *on premise*, mientras que el 48,4% confía más en la nube.** Nuevamente, no existen diferencias significativas en las respuestas en los diferentes países.

¿Qué metodología de almacenamiento considera que tiene más control y seguridad?



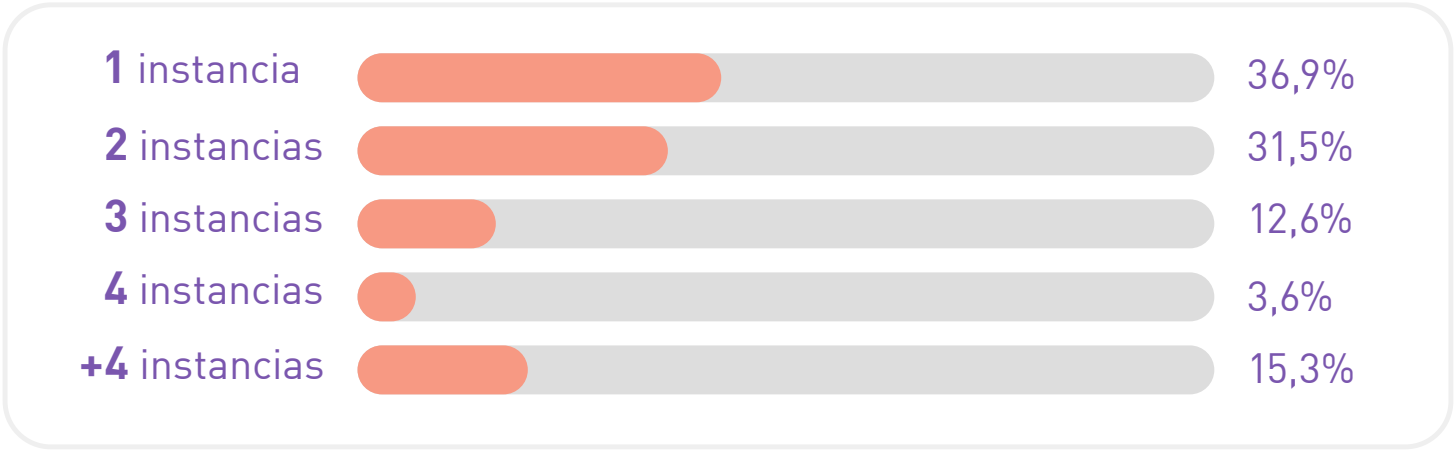
Esta respuesta es coherente con la decisión de los ejecutivos sobre dónde guardar la información sensible, ya que el 56,9% de los encuestados declara que no guardan información crítica en la nube.

¿Tiene información crítica guardada en la nube?



Sobre el 43,1% que sí guarda información crítica en la nube, varían mucho las instancias de la nube que utilizan. En su mayoría, utilizan una (36,9%) o dos instancias (31,5%), mientras que sólo el 12,6% utiliza tres. **Por su parte, el 15,3% declara emplear más de 4 instancias.**

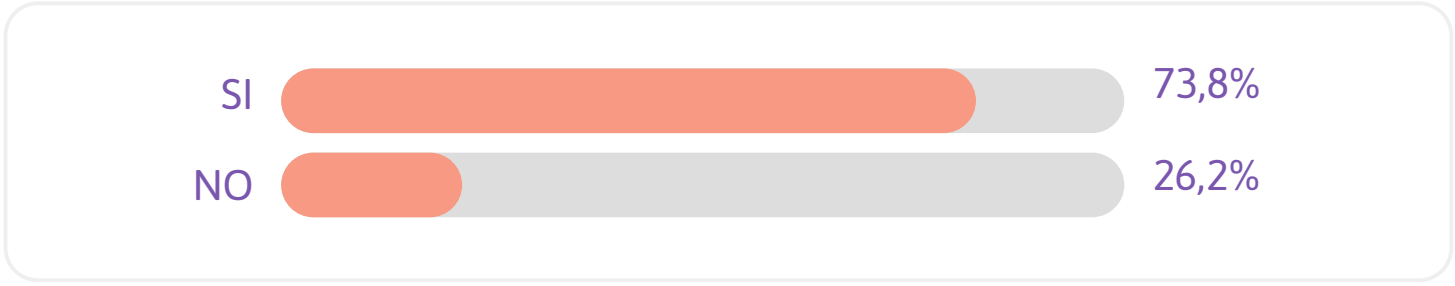
En caso de que la respuesta sea afirmativa, ¿cuántas instancias de la nube utiliza?



Ciberseguridad como protección

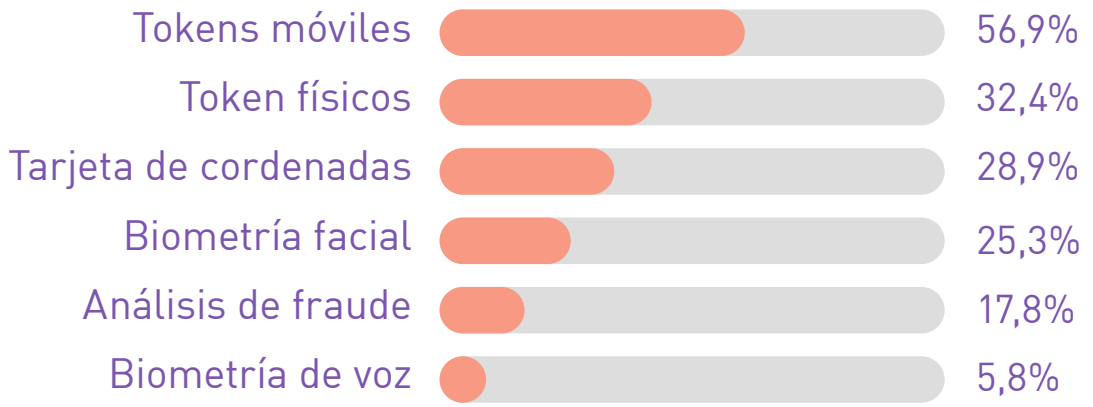
Para prevenir fraudes y proteger la identidad de sus empleados y clientes, el 73,8% de los encuestados afirma que invierte en soluciones de ciberseguridad para su empresa. La tendencia se mantiene a través de todos los países con excepción de Uruguay, en donde el 87% de los encuestados confiesa invertir en este tipo de soluciones; Ecuador, donde el 65% lo hace; y Bolivia, donde el invierte el 54% de los encuestados.

Su empresa, ¿invierte en soluciones de ciberseguridad?



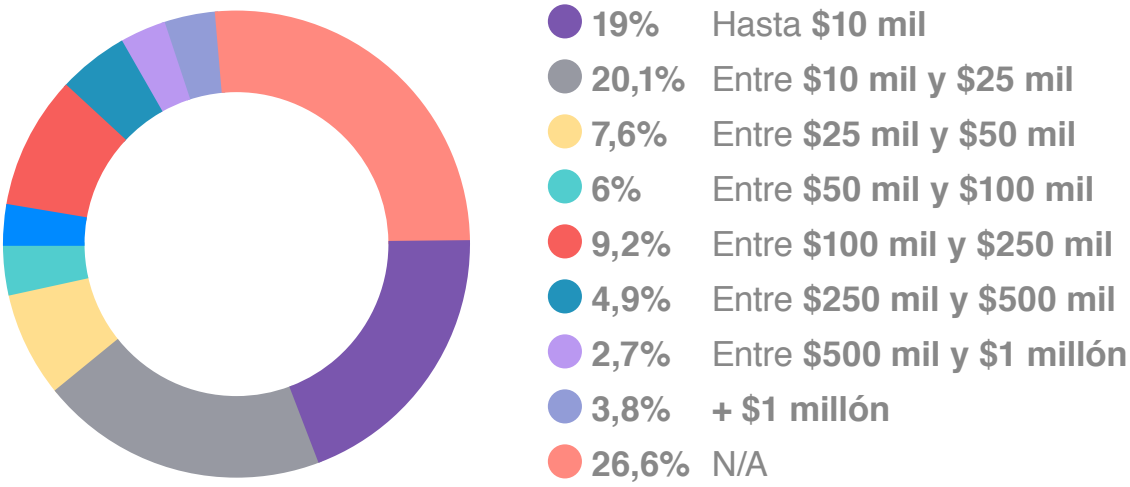
A la hora de proteger la información confidencial de las empresas, los métodos de autenticación robusta más elegidos por los ejecutivos son los tokens móviles (56,9%), los tokens físicos (32,4%) y las tarjetas de coordenadas (28,9%). Las prácticas más modernas demuestran más resistencia a la hora de ser implementadas, ya que sólo el 25,3% de los encuestados emplea biometría facial, el 17,8% utiliza análisis de fraude y tan sólo el 5,8% adopta biometría de voz para proteger la identidad digital de las personas.

¿Qué métodos de autenticación robusta utiliza a la hora de proteger la identidad digital de las personas?

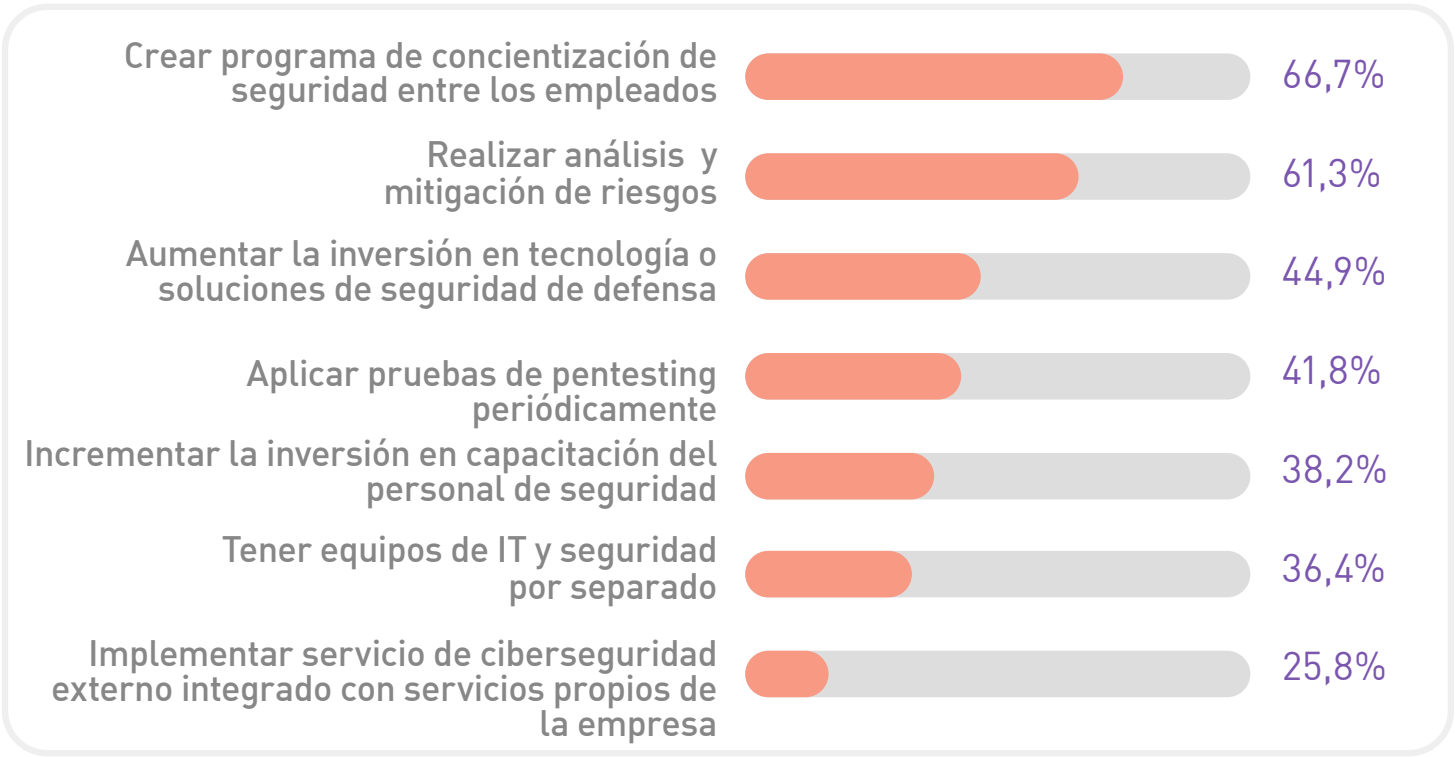


Si bien el porcentaje de empresas que invierten en ciberseguridad es alto, destinan presupuestos muy acotados en esta área. El 26,6% invierte entre $10.000 y $25.000 dólares, mientras que el 19% destina menos de $10.000 dólares. Lo sorprendente es que un 20,1% de los encuestados desconoce cuánto invierte su empresa en este rubro.

En caso de que la respuesta sea positiva, ¿cuánto invierte su empresa en ciberseguridad por año?



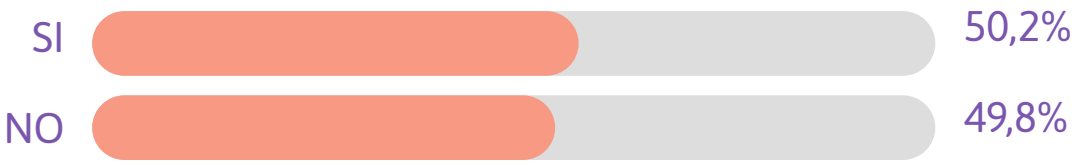
¿Cuál es la mejor estrategia para reducir el riesgo de ataques y mejorar la ciberseguridad?



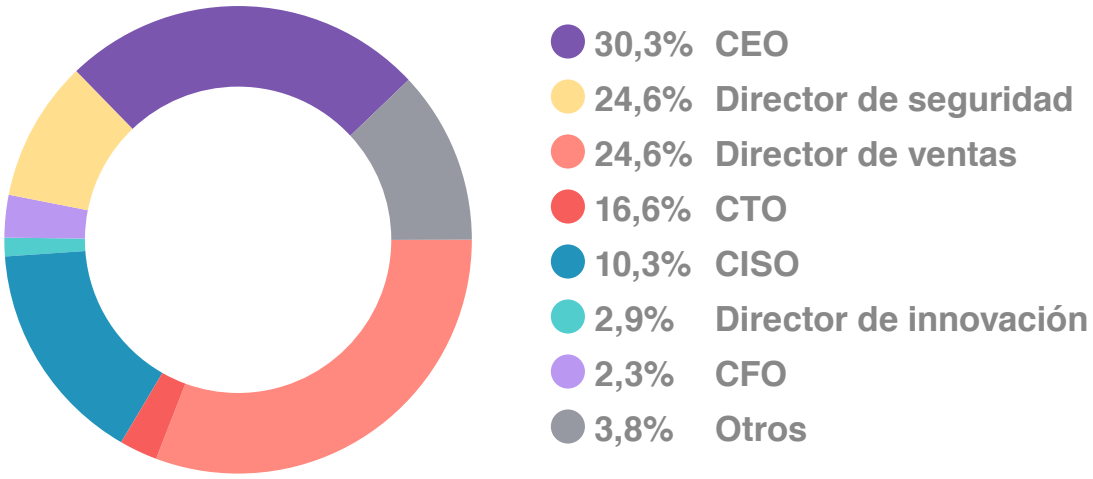
Recursos destinados a la ciberseguridad

En el informe de VU Labs también se cuestionó a los ejecutivos en relación a los recursos humanos destinados a la ciberseguridad dentro de la empresa. En este caso, la mitad de las empresas encuestadas cuenta con un sector de ciberseguridad. Sin embargo, en esta respuesta hubo grandes discrepancias entre los distintos países: en Bolivia, el 86% de las empresas no cuenta con un sector de ciberseguridad. En el caso de Costa Rica es el 63% y en Guatemala, el 60% tampoco cuenta con dicho sector.

¿Cuenta su empresa con un sector de ciberseguridad?

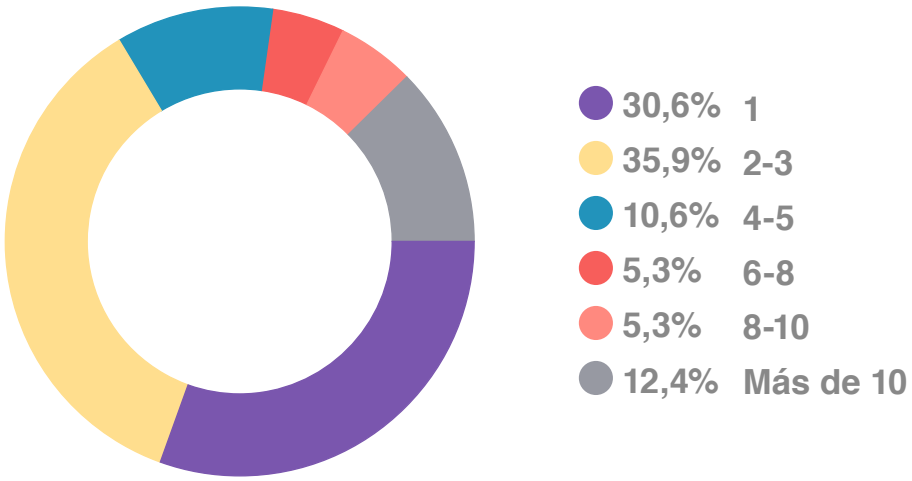


¿De quién depende este sector?



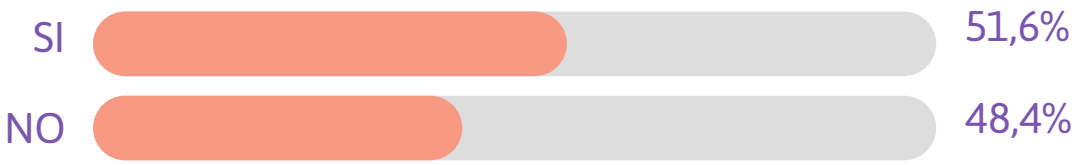
Según los resultados, se puede ver que no existe un consenso entre las empresas sobre de quién debería depender dicho departamento. En el 30,3% de los casos depende del CEO, en el 24,6% de los casos depende del Director de seguridad, en el 16,6% de los casos depende del CTO y en el 10,3% de los casos depende del Chief Information Security Officer (CISO).

¿Por cuántas personas está integrado el departamento de ciberseguridad?



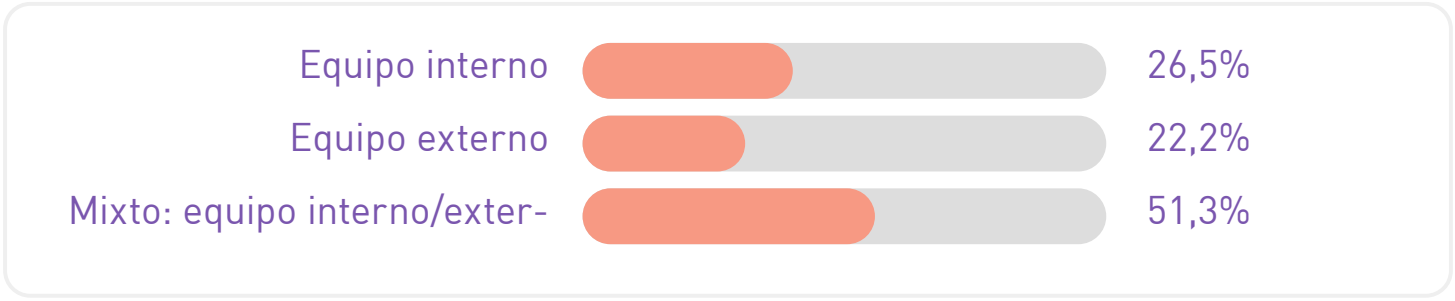
En la mayoría de los casos, se puede observar que suelen ser departamentos integrados por una (30,6%) o dos personas (35,9%). En tan sólo el 10,6% de los casos está integrado por cuatro o cinco personas y en el 12,4% de los casos, el departamento tiene más de diez. personas.

¿Realiza tareas de *pentesting* en su empresa?



Al consultar sobre las tareas que realiza en relación a la ciberseguridad, menos de la mitad (48,4%) realiza *pentesting* (hacking ético) en su empresa.

Si la respuesta es afirmativa, ¿de qué forma realiza las tareas?



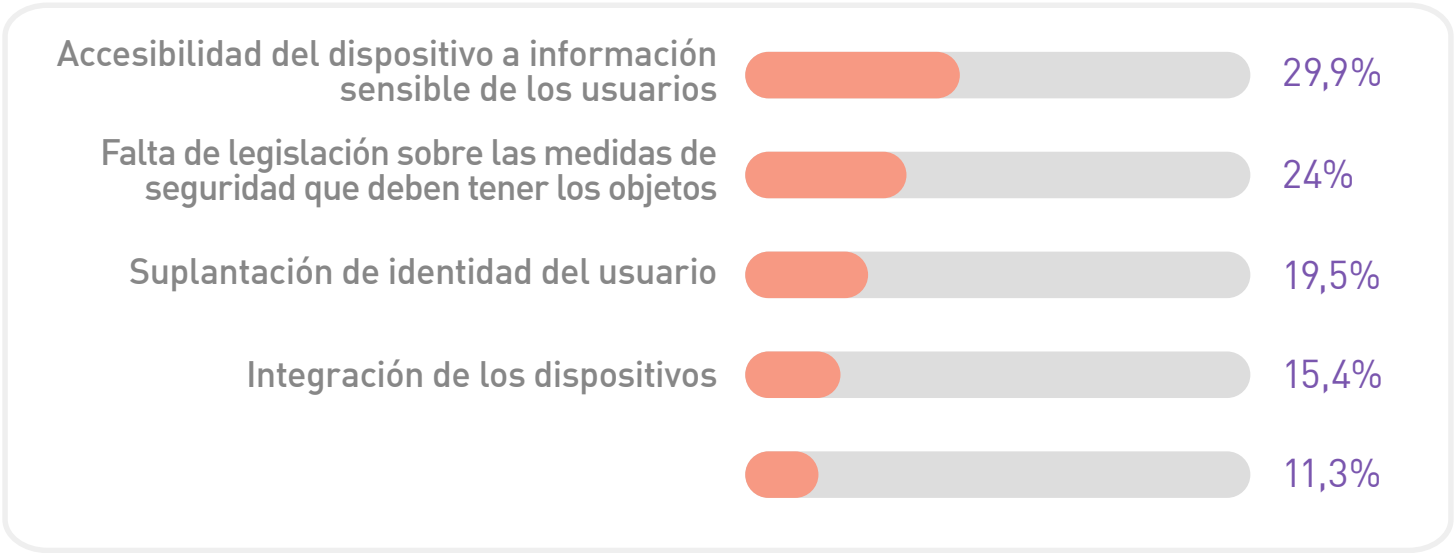
De aquellas empresas que realizan *pentesting*, el 51,3% utiliza equipos mixtos compuestos por miembros internos y externos, mientras que el 26,5% emplea a su equipo interno para dicha actividad y el 22,2% contrata un equipo externo.

Tendencias

Internet de las Cosas (IoT)

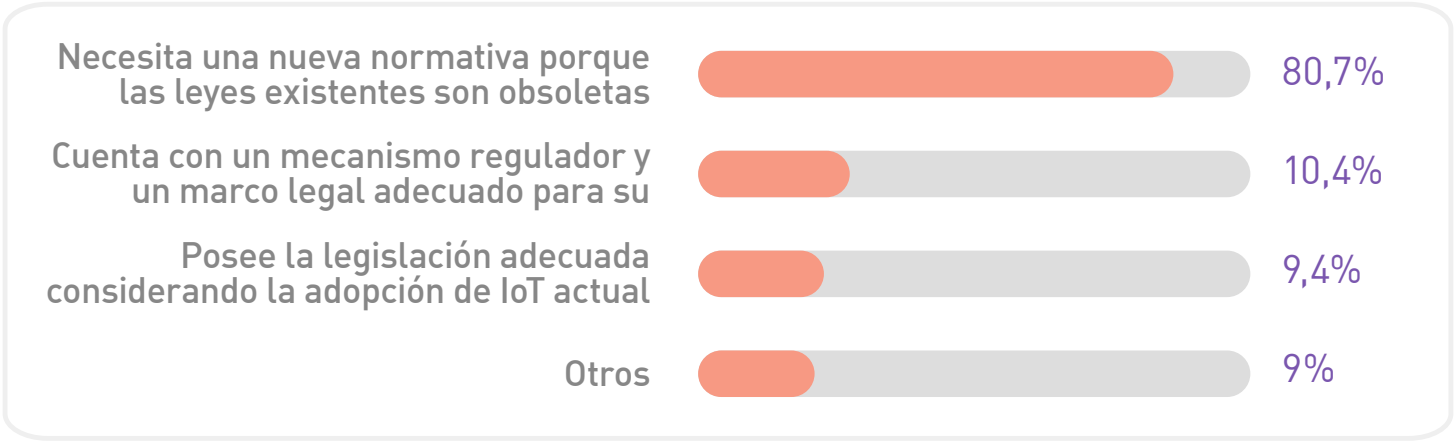
Desde VU Labs también se evaluó el impacto respecto a las distintas tendencias como Internet de las Cosas (IoT) y los pagos móviles.

¿Cuál considera que es el principal riesgo de la evolución de la Internet de las Cosas (IoT)?



En relación al riesgo que conllevan los dispositivos interconectados, el 29,9% de los encuestados considera que el principal riesgo tiene que ver con la accesibilidad del dispositivo a información sensible de los usuarios. Luego, el 24% hace referencia a la falta de legislación con respecto a las medidas de seguridad que deben tener dichos dispositivos. Por otro lado, el 19% percibe la suplantación de la identidad del usuario como un riesgo, seguido por el 15,4%, que ve el peligro en la integración de los dispositivos o la gestión de la confidencialidad de los datos (11,3%).

Según su criterio, la expansión de IoT en América Latina:

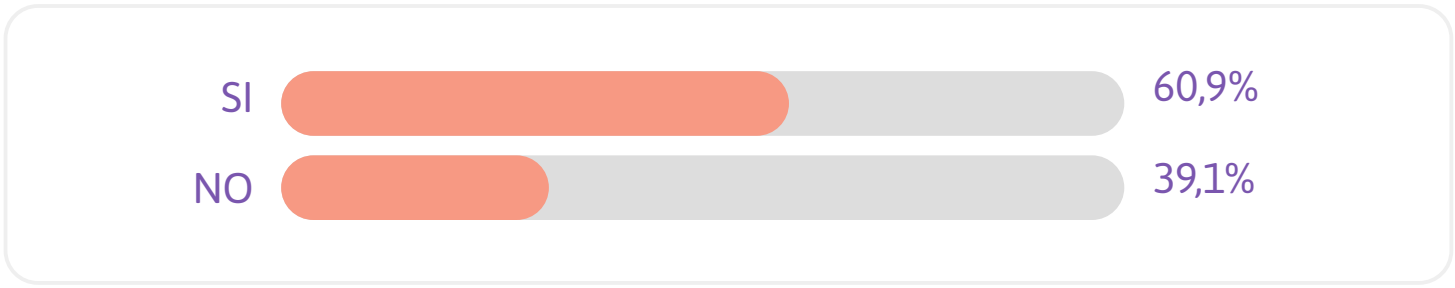


Con respecto a la expansión de IoT en América Latina, la respuesta es casi unánime en todos los países. El 80,7% de los encuestados considera que las leyes que regulan y normalizan las medidas de seguridad quedan obsoletas frente a la rápida expansión de los objetos hiperconectados, por lo que es necesario construir una nueva normativa.

Dinero móvil

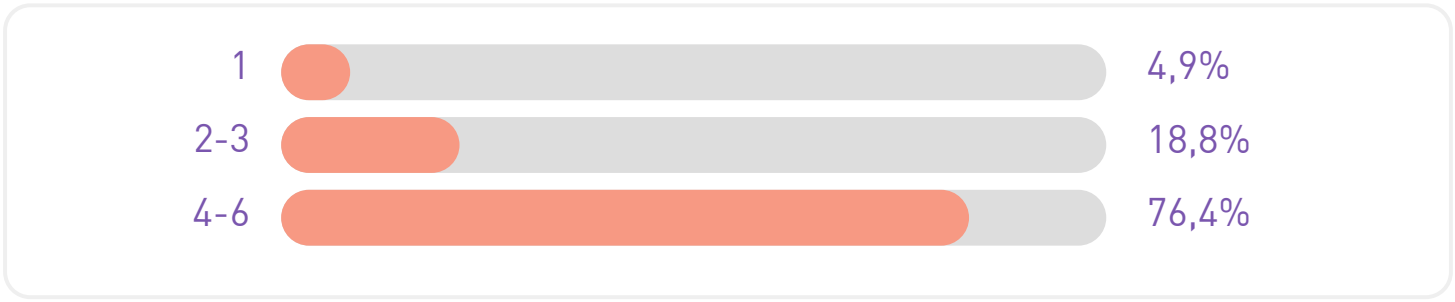
En el último tiempo, se ha visto cómo se ha propagado el uso de dinero móvil y digital en toda Latinoamérica.

¿Cree que el dinero digital (pagos móviles, criptomonedas, etc.) va a remplazar al dinero físico?



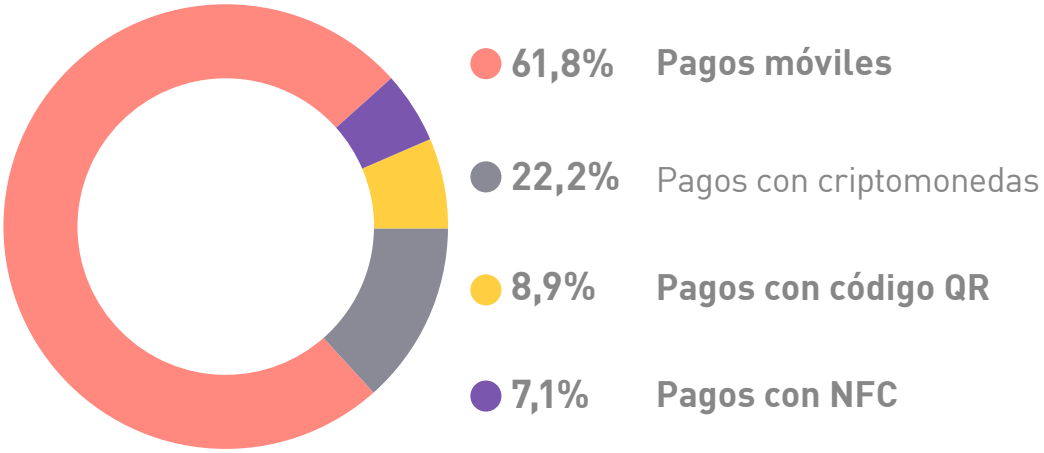
Al consultar a los ejecutivos si creen que el dinero digital (pago móviles, criptomonedas, etc.) va a reemplazar al dinero físico, el 60,9% respondió afirmativamente.

Si su respuesta fue positiva, ¿en cúanto tiempo cree que lo hará?



Sin embargo, la gran mayoría (76,4%) prevé que esto tomará entre cuatro y seis años, mientras que el 18,8% considera que esto pasará en de los siguientes dos o tres años. Sólo un 4,8% piensa que este cambio se dará dentro del próximo año.

¿Cuál cree que es el dinero digital que más se propagará?



Al especificar cuál es el medio de pago digital que más se propagará, un 61,8% estima que serán los pagos móviles, seguido por los pagos con criptomonedas (22,2%), los pagos con código QR (8,9%) y por último, el pago con NFC (7,1%).

Conclusión

Para nosotros es sumamente importante realizar, a través de VU Labs, este análisis sobre la situación de la ciberseguridad y sus amenazas tanto para ciudadanos como para empresas. El aporte de clientes y prospectos de todo América Latina nos ayuda a tener una buena perspectiva de lo que está pasando para poder adaptar nuestras soluciones de forma adecuada, mantenernos a la vanguardia de los cambios y así poder ofrecer servicios que ayuden a proteger la identidad del ciudadano, prevenir fraudes y fomentar la inclusión financiera. Desde ya, muchas gracias a todos los que participaron y esperamos poder seguir compartiendo tendencias del sector con ustedes cada año.

VU LABS

Acerca de VU

VU es una compañía multinacional enfocada en prevención de fraude y protección de la identidad. Provee soluciones de autenticación robusta de la identidad de los ciudadanos mediante la combinación de los controles tradicionales de ciberseguridad con geolocalización, machine learning, reconocimiento de documentos de identidad y el análisis del comportamiento del usuario, lo que da como resultado soluciones modulares de prevención del fraude, que incluyen reconocimiento de voz, reconocimiento facial y otras opciones de autenticación. Más de 80 clientes en 18 países de América Latina, incluyendo gobiernos, bancos y empresas de retail, integran la tecnología de VU en sus plataformas existentes para proteger la información confidencial. Entre los clientes se encuentran Banco Santander (Fortune 500), el Banco de la República de Uruguay (NYSE), Prisma, Falabella (Forbes 2000) y Globant (NYSE). Es la única compañía de la región alineada con las buenas prácticas de autenticación internacional como parte del Tech Accord, Endeavor, la Alianza FIDO, Open Authentication Alliance (OATH) y Open Connectivity Foundation (OCF).

Acerca de VU LABS

VU Labs es el laboratorio de investigaciones de seguridad de VU que persigue el objetivo de concientizar y poner a disposición datos estadísticos en el campo de la seguridad, constituyendo de esta forma una “llave en mano” esencial para la toma de decisiones en el campo de la ciberseguridad de cualquier corporación.

corporate@vusecurity.com vusecurity.com @vusecurity /vusecurity /vusecurity

© 2019 VU LABS