VU LABS

CIBERSEGURIDAD
en entornos digitales

INFORME
2016 - 2017

600 Organizaciones latinoamericanas participantes

18 Países representados

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

Bienvenido al informe sobre CIBERSEGURIDAD en América Latina y Caribe

VU Labs, es una herramienta anual brindada por 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.

Como se puede observar en los medios, las noticias acerca de ataques, fraudes y amenazas a través de la red son cada vez más frecuentes. Esto afecta tanto a particulares como al ámbito corporativo; ninguno está ajeno a este tipo de situaciones. Este contexto ha despertado la conciencia social respecto a la importancia que tiene proteger la información y la privacidad en un mundo online.

La variedad y diversificación de amenazas es cada vez mayor. Frente a ello, desde VU abordamos la temática de la ciberseguridad considerando la opinión de usuarios y líderes de empresas, marcando tendencias, alcances de IoT, detección de peligros y la percepción de los usuarios frente a los ataques actuales.

Para ello realizamos una encuesta a toda nuestra base de datos de América Latina, incluyendo clientes y *prospects*. Luego, los datos estadísticos y de tendencias fueron validados en su totalidad por los expertos que conforman VU Labs.

Antes de compartir los resultados, queremos agradecer todas las organizaciones de toda América Latina que contribuyeron a este informe, con el aporte de datos e información que constituyen el timón de las perspectivas aquí presentadas.

Esperamos que la información resulte de interés y les sea de utilidad.

Sebastián Stranieri, **CEO de VU**

Metodología de la Investigación

El relevamiento se llevó a cabo a través de una encuesta auto-administrada, que fue respondida vía correo electrónico por más de 600 organizaciones de **18 países de América Latina.**

Las preguntas fueron abiertas, invitando al desarrollo de sus respuestas por parte del universo participante, clientes y *prospects* de VU de entre 25 y 60 años, con un porcentaje similar de público femenino y masculino.

Países representados en el informe

Argentina	Bolivia	Panamá	Rep. Dominicana
Uruguay	Perú	Costa Rica	México
Chile	Ecuador	Nicaragua	
Paraguay	Colombia	El Salvador	
Guatemala	Venezuela	Honduras	

Análisis de resultados

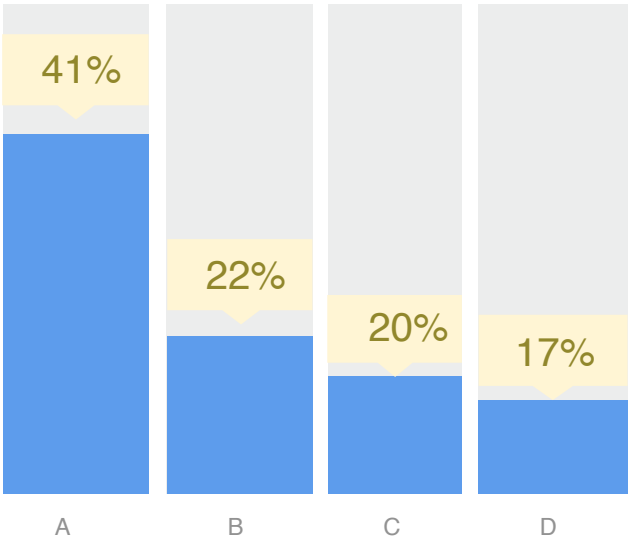
El informe expuso resultados sobre las metodologías de fraude más frecuentes, los problemas más comunes de seguridad informática a nivel corporativo y el futuro de los bitcoins. También brinda *insights* interesantes sobre la frecuencia con la que ocurren los fraudes, quién es el responsable dentro de la empresa cuando éstos surgen, cómo reaccionan los usuarios y cuánto deberían saber sobre ciberseguridad.

Metodología de fraude más frecuente

Al consultarle a los participantes sobre la metodología de fraude más frecuente, el 41% de los encuestados destacaron el *phishing*, como se puede ver en el gráfico a continuación.

¿Qué entendemos por *phishing*?

El término se refiere a la suplantación de identidad; un ciberdelito que se comete mediante el uso de un tipo de ingeniería social, caracterizado por intentar adquirir información confidencial de forma fraudulenta.



A - *Phishing*

B - Aprovechamiento de la vulnerabilidad del sistema

C - Incitación a la fuga en punto de venta

D - Instalación de malware

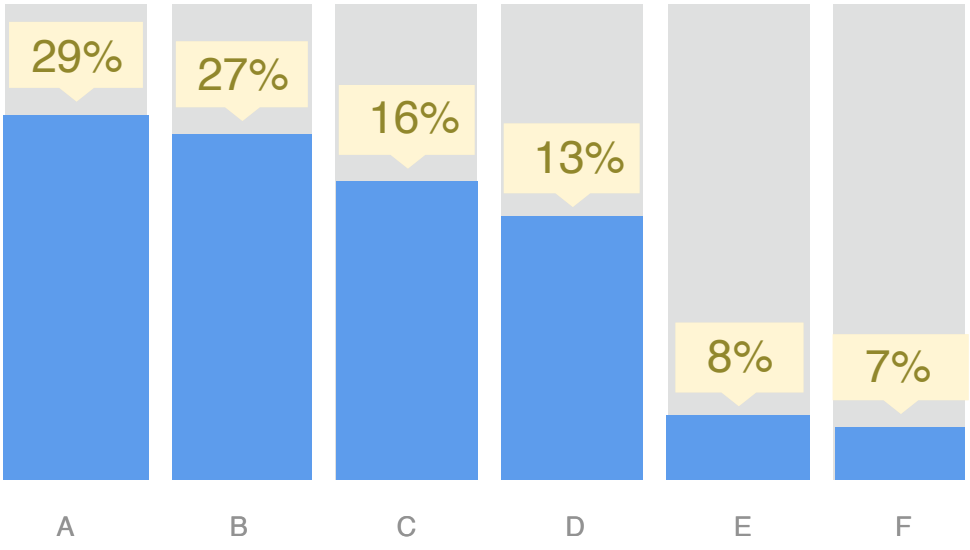
Problemas más comunes de seguridad informática a nivel corporativo

Al ser consultados sobre qué sectores, podrían ser víctimas de *phishing,* los encuestados expresaron que, debido a las características de la web, todos los sectores son vulnerables a ser atacados si no se cuenta con barreras de protección adecuadas. Un alto número coincidió con que los delitos son cada vez más sofisticados, los ciberdelincuentes se encuentran más preparados, disponen de mejores herramientas y tienen un mercado mucho más amplio para delinquir.

En este escenario, el 29% de los participantes destacó que el sector gubernamental es el más propenso a sufrir este tipo de ataques, además del popularmente conocido sector Banca y Finanzas. Lo sigue, inmediatamente con el 27%, Telecomunicaciones y luego Salud con el 16%, y Educación con el 13%.

Sectores víctimas de *phishing*

Al consultarle a las personas sobre el tipo de metodología de fraude más recurrente, en su mayoría (41%), los encuestados destacaron el *phishing*, como se puede ver en el gráfico a continuación:



A - Gobierno

B - Telecomunicaciones

C - Salud

D - Educación

E - Minería

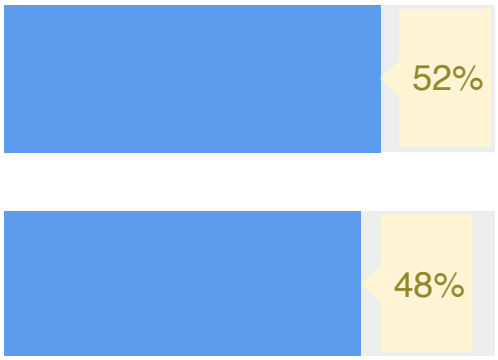
F - Construcción

El futuro de los bitcoins

El siguiente aspecto que se consideró dentro del relevamiento fue el futuro de los bitcoins y su proliferación en América Latina. Esta nueva modalidad de pago genera múltiples beneficios para el usuario, entre los que se destacan que los pagos realizados a través de los bitcoins son irreversibles y seguros, ya que la transacción se realiza de forma directa.

En este caso, las respuestas de los encuestados se encuentran divididas: el 52% considera que esta moneda virtual se popularizará e incrementará su uso, mientras que el 48% restante está en desacuerdo.

¿El Bitcoin proliferará en la región?

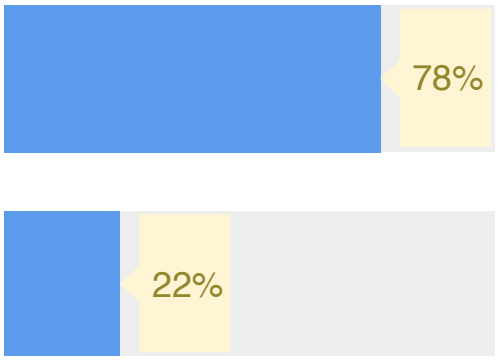


En esta misma línea se consultó cómo es percibida el bitcoin. El protocolo ***blockchain*** favorece el intercambio de un valor entre dos partes de una forma rápida y eficaz, sin la necesidad de un ente regulador.

Es por su atractivo, que la industria financiera ha puesto los ojos en esta tecnología, que puede suponer una gran oportunidad para generar nuevos servicios bancarios más ágiles, de menor costo y más favorables para sus clientes. Esta tecnología es tanto una ventaja como una amenaza para el sector bancario y financiero, de acuerdo a la estrategia que sigan y el grado de conocimiento que tengan para aprovechar este panorama favorable.

Inicialmente, uno de los primeros impactos más notables sería la reducción de costos. Por el simple hecho de que los bancos compartieran un *shared ledger*, se conseguirían importantes ahorros, así como agilidad en algunos de los procesos sin la necesidad de validación.

¿Qué representa el Bitcoin?

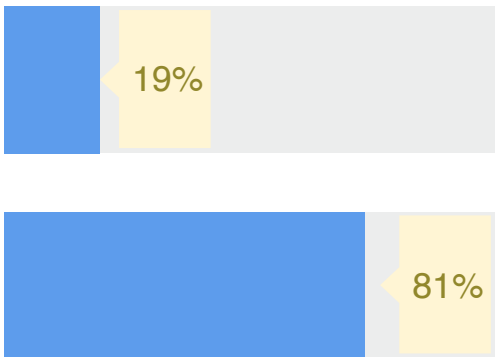


Para el 78% de los encuestados, representa una oportunidad, mientras que para el 22% sería una amenaza.

Ciberdelitos Móviles

Al tratar el tema fraudes, en la encuesta se consultó si habían sufrido algún ciberdelito a través de dispositivos móviles el último año.

¿Ha experimentado delitos a través de dispositivos móviles?



Ante estas consultas, sólo el 19% indicó haber experimentado un ciberdelito en el último año, mientras que el 81% respondió no haberlo experimentado.

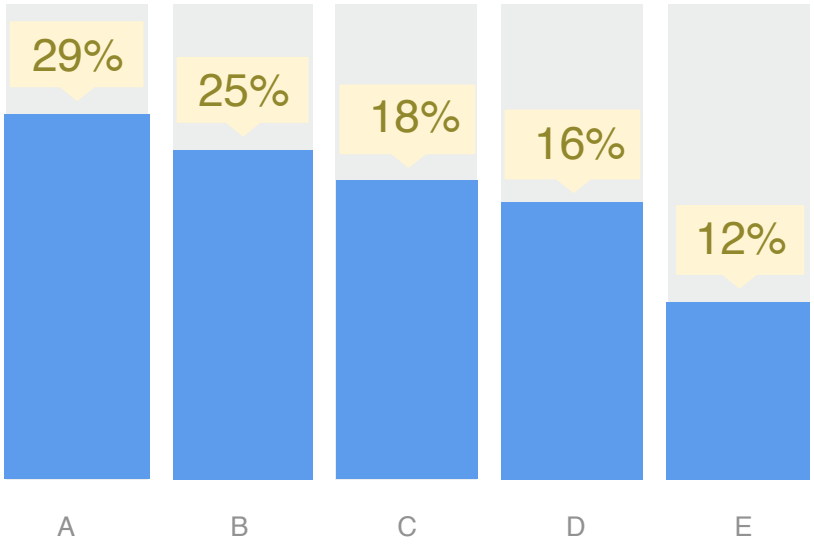
¿Cuidan los usuarios su seguridad cibernética?

Hoy los ataques son personalizados, automatizados y a nivel masivo, con mayor velocidad de reacción de los atacantes, con identidades falsas relacionadas, donde el perfil del usuario malintencionado realmente resista una investigación amateur y el origen del hackeo sea cada vez más complejo de visualizar.

La autenticación de doble factor pisa cada vez más fuerte, como herramienta fundamental para proteger los sistemas de este tipo de situaciones, seguida por el análisis de patrones de comportamiento de los usuarios facilitando la validación de la identidad y la obtención de información adicional para chequear movimientos sospechosos.

Al consultar respecto al comportamiento de los usuarios frente a la telefonía móvil, el 29% de los encuestados indicó que el que genera más posibilidades de violación de seguridad es compartir contraseñas y claves de acceso. Ahora la gran pregunta es, si los usuarios conocen este riesgo, ¿por qué toman esta conducta? Simplemente, porque suelen estar desbordados por la cantidad de usuarios y contraseñas, que las anotan, comparten, y repiten, con el objetivo de no olvidarlas.

¿Qué comportamientos vuelven a los usuarios más vulnerables en la red?



A - Compartir contraseñas y claves de acceso

B - Uso de equipo sin clave de acceso

C - Archivo de información laboral y personal en las mismas cuentas de almacenamiento online

D - Falta de actualización de los equipos

E - Almacenamiento de archivos online

La contraseña está en desuso, y pronto será reemplazada al 100% por un método de autenticación que no requiera de este mecanismo de seguridad", asegura Sebastián Stranieri, CEO de VU. "Incluso, muchas compañías de seguridad, incluyendo VU, están desarrollando soluciones para ayudar a los usuarios a administrar y almacenar sus contraseñas de manera segura", continuó.

Responsabilidad ante un fraude

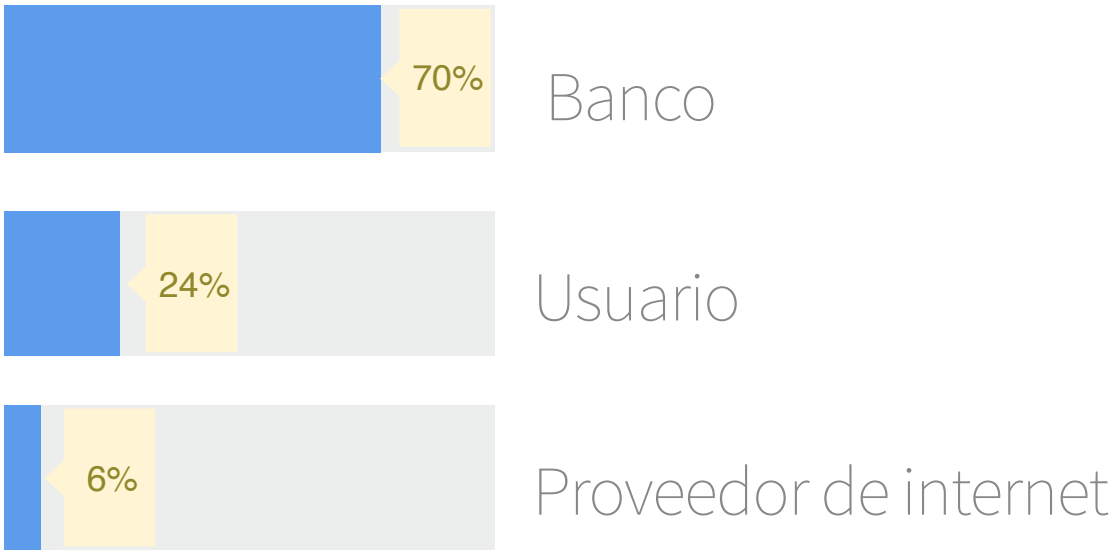
El incremento de estafas electrónicas ha reabierto el debate acerca de la responsabilidad por dichas defraudaciones. Frente a la consulta respecto a quién sería responsable ante una situación de fraude cibernético bancario, el 70% de los encuestados indicó – sin lugar a dudas – que sería el mismo banco.

En la actualidad, es la propia víctima la que se ve obligada a realizar una denuncia ante la institución bancaria.

Pero ¿quién debería ser el verdadero responsable? La falta de inversiones en tecnología y de revisiones periódicas favorecen y dan lugar a que los ciberdelincuentes ataquen y se apoderen del patrimonio de los usuarios del sistema bancario.

De acuerdo al relevamiento, mientras que el 70% apuntó al banco, el 24% indicó que el responsable es el usuario y solo el 6% señaló al proveedor de Internet.

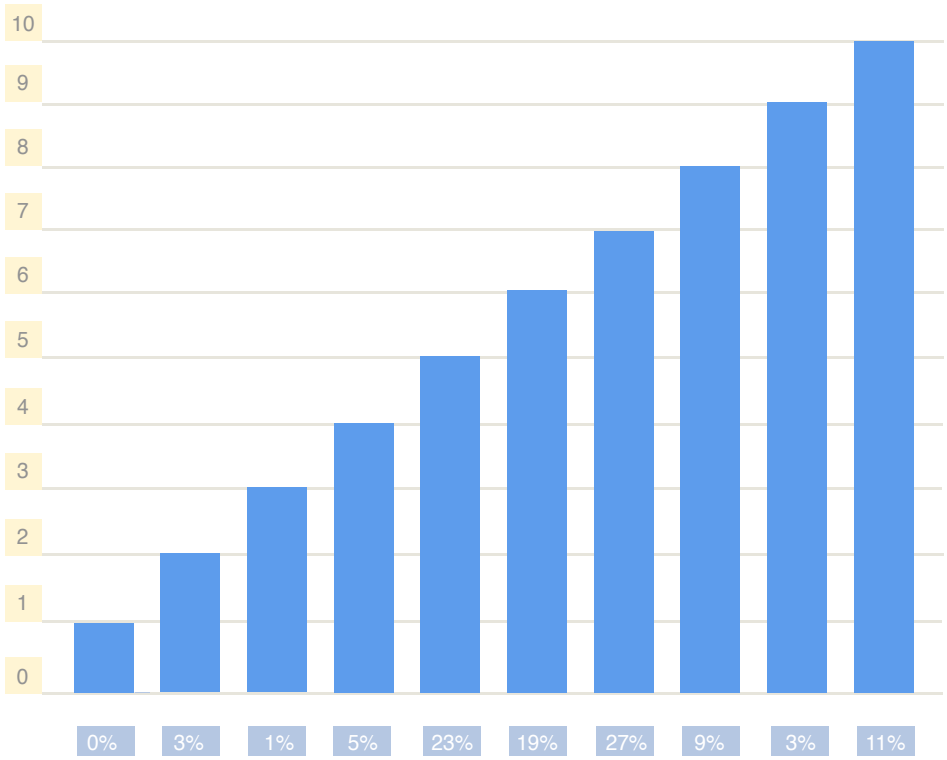
¿Ante un caso de fraude, quién sería el responsable?



¿Qué hay que saber para estar seguros?

Al consultar acerca de cuánto debe saber una persona que no es especialista en informática para estar seguro en el mundo digital, en una escala del 1 al 10, siendo 1 escaso o nulo conocimiento, y 10 mucho conocimiento, 50% de los encuestados dieron una valoración superior a 7 puntos en relación a su necesidad de mantenerse informados acerca de prácticas para mantenerse seguros.

¿Cuánto debe saber una persona para estar seguro?



*En una escala del 1 al 10, siendo 1 escaso o nulo conocimiento, y 10 mucho conocimiento.

Según el Reporte Anual de CISCO de Ciberseguridad 2017, "muchas organizaciones están confiando en muchas soluciones de diferentes vendedores".

Esta táctica suma a la complejidad y confusión de las redes de seguridad a medida que la Internet se hace más rápida y aumenta el número de dispositivos conectados y el tráfico.

"Las organizaciones deben buscar la sencillez y la integración si quieren protegerse".

Por su parte, el Reporte de Inteligencia de seguridad de Microsoft 2016 destaca que "en las computadoras que ejecutan software de seguridad en tiempo real, la mayoría de los intentos de malware para infectar computadoras se bloquean antes de que tengan éxito".

Estos dos reportes demuestran que es indispensable mantener los equipos actualizados con las últimas versiones y patches de seguridad. Además, es conveniente que se tomen el tiempo para hablar con expertos de ciberseguridad, investigar y evaluar las diferentes opciones disponibles en el mercado para mantener su información y sistemas seguros.

Para acceder a la encuesta completa, por favor ingrese al siguiente link:
http://www.vusecurity.com/campaign/2016-encuesta/index.php

Para acceder al informe anterior, por favor ingrese al siguiente link:
http://www.vusecurity.com/sharing/docs/VU_Informe_seguridad_la tam_2015.pdf

Acerca de VU

Es una compañía especialista en el desarrollo de software de Ciberseguridad, con foco en la prevención del fraude y el robo de identidad. Su misión es entregar experiencias digitales sin fricción y seguras tanto para Ciudadanos, como compañías. Es la única empresa de la región alineada a las buenas prácticas en materia de autenticación internacional, miembro de FIDO Alliance, OATh y OIC. Fundada en 2007, cuenta con oficinas en Argentina, Chile, Uruguay, Ecuador, Colombia, Costa Rica, México y Perú.

www.vusecurity.com

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.

VU LABS