appgate

iSMG
INFORMATION SECURITY
MEDIA GROUP

Faces of Fraud 2023

La Evolución del Fraude en Línea en 2023 y las Mejores Prácticas para Cerrar las Brechas

Author: ISMG

Tabla de Contenidos

Sobre esta encuesta:

Esta encuesta fue realizada por Information Security Media Group y Appgate en el segundo trimestre de 2023. En total, participaron en este estudio más de 150 instituciones financieras, principalmente de Estados Unidos y Canadá.

Sobre Appgate:

Appgate es una empresa de acceso seguro que potencia cómo las personas trabajan y se conectan al proporcionar soluciones construidas específicamente en los principios de seguridad de Zero Trust (Confianza Cero). Este enfoque de seguridad definido por las personas permite conexiones rápidas, simples y seguras desde cualquier dispositivo y ubicación a cargas de trabajo en cualquier infraestructura de TI en entornos en la nube, locales e híbridos. Appgate ayuda a organizaciones y agencias gubernamentales en todo el mundo a comenzar desde donde están, acelerar su camino hacia Zero Trust y planificar su futuro. Obtenga más información en Appgate.com.

Introducción

Bienvenidos a nuestro informe que resume la encuesta "Faces of Fraud survey 2023". Estamos muy agradecidos con nuestros colaboradores de la industria que respondieron nuestras preguntas con franqueza, lo que nos permitió ofrecer una instantánea de los fraudes que más preocupan a los servicios financieros en 2023. También podemos observar cómo la industria en su conjunto se ve afectada y le permitimos ver cómo sus colegas están priorizando formas de protegerse.

Esto incluye identificar en qué áreas están centrando sus inversiones las instituciones financieras de hoy en día en tecnologías de prevención de fraudes para el próximo año.

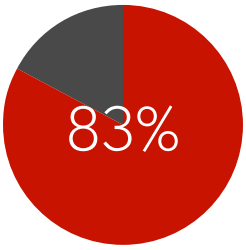
Cuando se trata de amenazas, cada nueva tecnología da lugar a nuevos fraudes a medida que los atacantes evolucionan e innovan, pero nuestras defensas cibernéticas también están evolucionando. Entonces, ¿qué debemos estar vigilando en el próximo año y cómo debemos responder?

Los datos compartidos en este informe ayudarán a informar su estrategia de prevención de fraudes para el próximo año, no solo en relación a las amenazas que enfrenta y la tecnología que implementa para prevenirlas, sino también para establecer un punto de referencia sobre lo que debería ser realista en cuanto a logros.

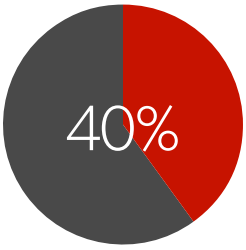
Atentamente,

TONY MORBIN
Editor Ejecutivo, EU
Information Security Media Group
Tmorbin@ismg.io

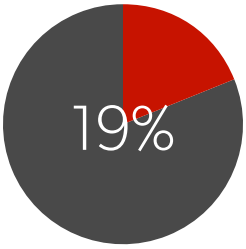
Algunos Números



83% de los encuestados afirman que los esquemas de fraude actuales están evolucionando demasiado rápido para que puedan mantenerse al día



Solamente el 40% de las organizaciones tienen la visibilidad necesaria para identificar el impacto de un ataque de phishing.



Solo el 19% de las organizaciones tienen la capacidad de identificar el fraude en tiempo real.

Resumen Ejecutivo

El fraude es un problema continuo y los atacantes ven cada avance en la tecnología como una oportunidad para explotar la creciente complejidad, las superficies de amenaza en expansión y posibles nuevas brechas en nuestras defensas.

¿Un ejemplo? Tan pronto como la inteligencia artificial generativa se volvió ampliamente utilizada, los estafadores comenzaron a explotarla para identificar vulnerabilidades, acelerar nuevos ataques y crear señuelos más convincentes, incluyendo deepfakes. También la utilizaron como una palabra clave atractiva. Y los actores de amenazas continúan explotando las complejidades creadas por infraestructuras de TI dispersas, la digitalización, la migración a la nube y el cambio hacia fuerzas de trabajo remotas y híbridas y el uso de dispositivos personales (BYOD).

La preocupación por el impacto del cambio rápido se refleja en los resultados de la encuesta "Faces of Fraud" de este año, donde los encuestados de servicios financieros afirman que la principal vulnerabilidad es que los esquemas de fraude actuales evolucionan demasiado rápido para que puedan mantenerse al día. Si bien el ritmo de cambio ha sido un problema anual en esta serie "Faces of Fraud", el número de encuestados que lo ven como su principal preocupación casi se ha duplicado, pasando del 43% en 2019 al 83% este año.

Una vulnerabilidad evidente que permite tales fraudes es la falta de visibilidad que las organizaciones tienen para poder identificar el impacto de un ataque de phishing, con un 55% diciendo que tenían visibilidad limitada y un 5% admitiendo que no tenían ninguna. Menos de la mitad, solo el 40%, afirma tener la visibilidad detallada necesaria para identificar el impacto de un ataque de phishing, lo que sugiere que esta área sigue siendo un objetivo de mejora.

La percepción de la brecha

En la encuesta de este año, las percepciones contradictorias son muy reveladoras al comparar las respuestas de los encuestados a diferentes preguntas. Por ejemplo, al calificar la capacidad de su organización financiera para identificar y mitigar el fraude, el 60% de los encuestados dicen que es superior o por encima del promedio; el 37% dice que es promedio; y el 3% lo califica como por debajo del promedio.

Sin embargo, aunque el 97% de los encuestados dicen tener una capacidad promedio o superior para detectar y mitigar el fraude, solo el 19% dice que pueden identificar un ataque de fraude en tiempo real. Incluso menos, el 11%, afirma que pueden mitigar en tiempo real. El veinte por ciento de las organizaciones que tardan más de una semana en identificar el fraude carecen de la capacidad para hacerlo o no saben si la tienen. El veintinueve por ciento de las organizaciones que tardan más de una semana en mitigar el fraude también dicen que carecen de la capacidad para hacerlo o no saben si la tienen. Es particularmente preocupante que los tiempos de mitigación hayan aumentado en comparación con encuestas anteriores de esta serie; el porcentaje de aquellos que pueden hacerlo en tiempo real ha disminuido un 3% desde 2020. Incluso teniendo en cuenta cualquier margen de error estadístico, está claro que la situación no está mejorando.

Por lo tanto, no sorprende que exista una brecha de percepción entre cuán sólida es la postura de seguridad de una organización contra el fraude en comparación con lo que la organización cree que es. La brecha ha sido notablemente consistente a lo largo de la serie de encuestas, con una confianza en las capacidades que se mantiene alta. En el Faces of Fraud survey 2021, casi tres cuartos de los encuestados dijeron que estaban seguros o muy seguros de que su alta dirección comprendía la inversión necesaria para contrarrestar y mitigar las crecientes amenazas de fraude. Y casi tres cuartos de los encuestados en la encuesta de 2020 dijeron que estaban seguros o muy seguros de que los ejecutivos C - level "lo entendían" en cuanto a las inversiones contra el fraude. Sin embargo, en ambos casos, casi la mitad de las instituciones encuestadas afirmaron tener visibilidad limitada o nula para identificar el impacto de dicho ataque.

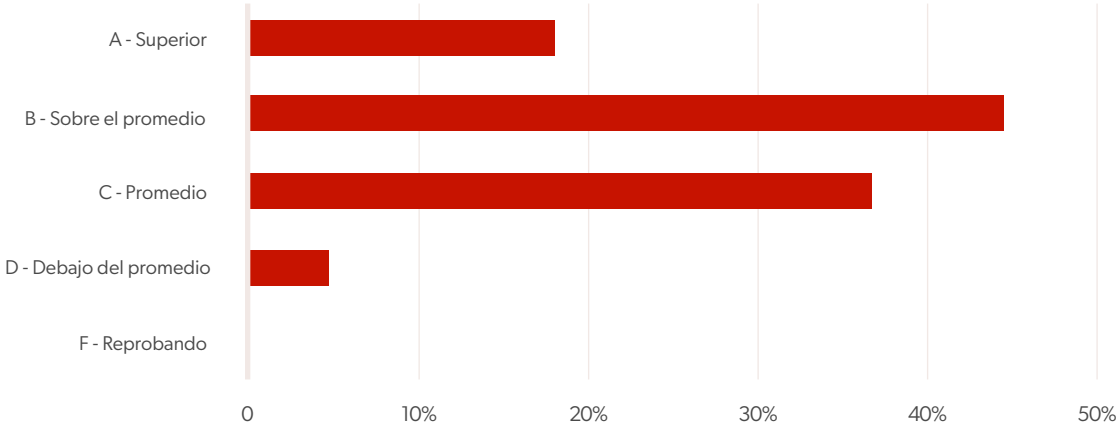
Conciencia vs. Disposición

Otra desconexión es que, aunque el 57% de los encuestados dice que los sistemas de detección y monitoreo de inteligencia de fraude tienen el impacto más significativo en la prevención de pérdidas por fraude, solo el 43% de los encuestados dice que planea invertir en sistemas de detección y monitoreo de inteligencia de fraude en los próximos 18 meses. La inferencia es que la conciencia sobre los beneficios de las herramientas modernas de prevención de fraude supera la disposición o capacidad para comprometerse a gastar en esas mismas herramientas.

También podría ser que las organizaciones financieras estén adoptando un enfoque demasiado segmentado en las herramientas de prevención de fraudes, ya que el 80% de los encuestados afirma que sus controles no se comunican entre sí en diferentes partes de la organización. Además, persiste una complacencia en la creencia de que las organizaciones ya están haciendo lo suficiente para prevenir el fraude, a pesar de que la evidencia sugiere lo contrario.

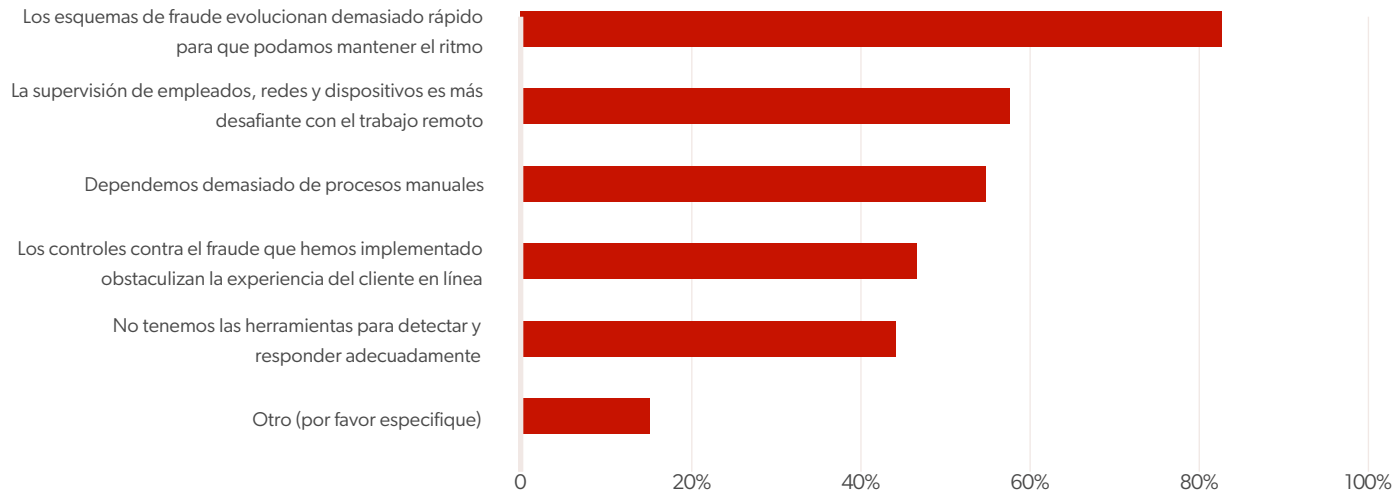
Resultados del Faces of Fraud Survey 2023

¿Qué calificación le daría a la capacidad de su organización para identificar y mitigar el fraude?



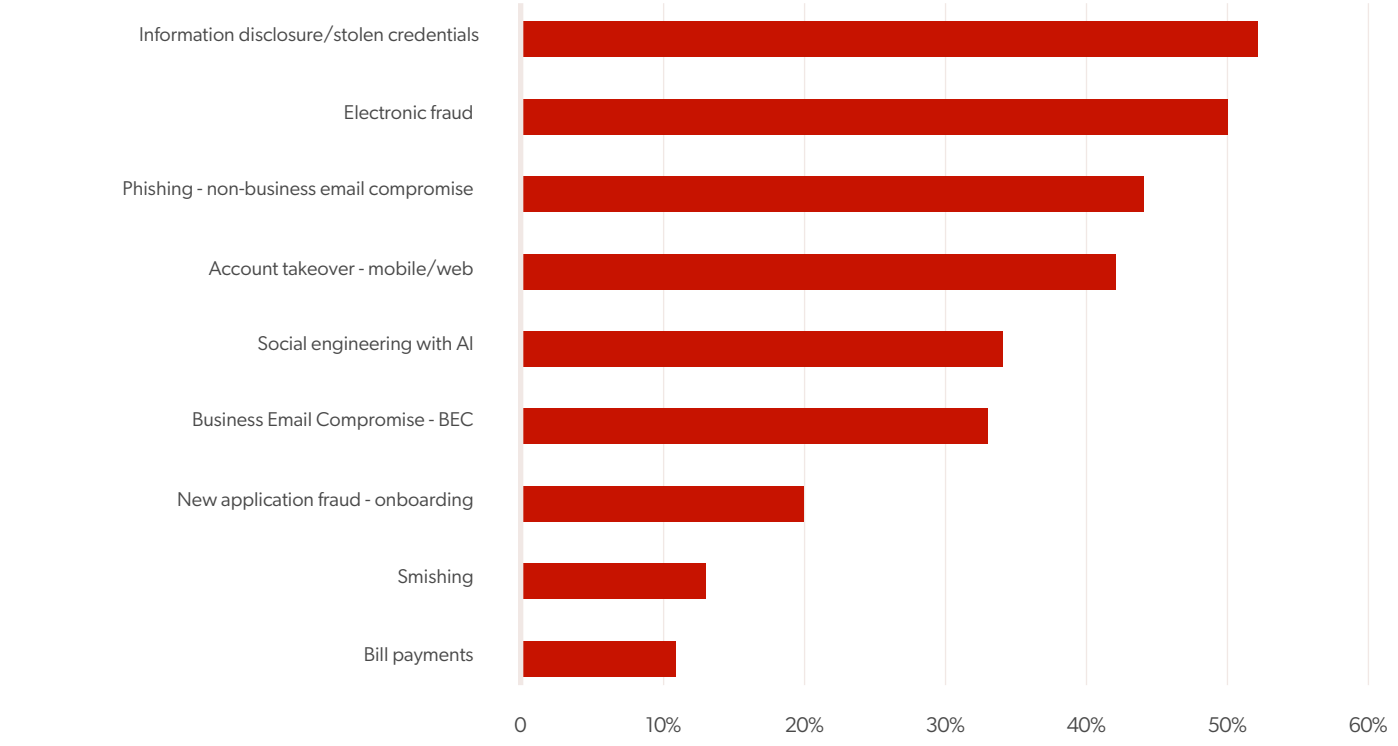
No sorprende que la mayoría de los encuestados, el 60%, piensa que su capacidad para identificar y mitigar el fraude es superior o por encima del promedio, mientras que el 37% dice que es promedio y solo el 3% dice que es inferior al promedio.

¿Cuáles cree que son las tres principales vulnerabilidades en sus defensas contra el fraude?



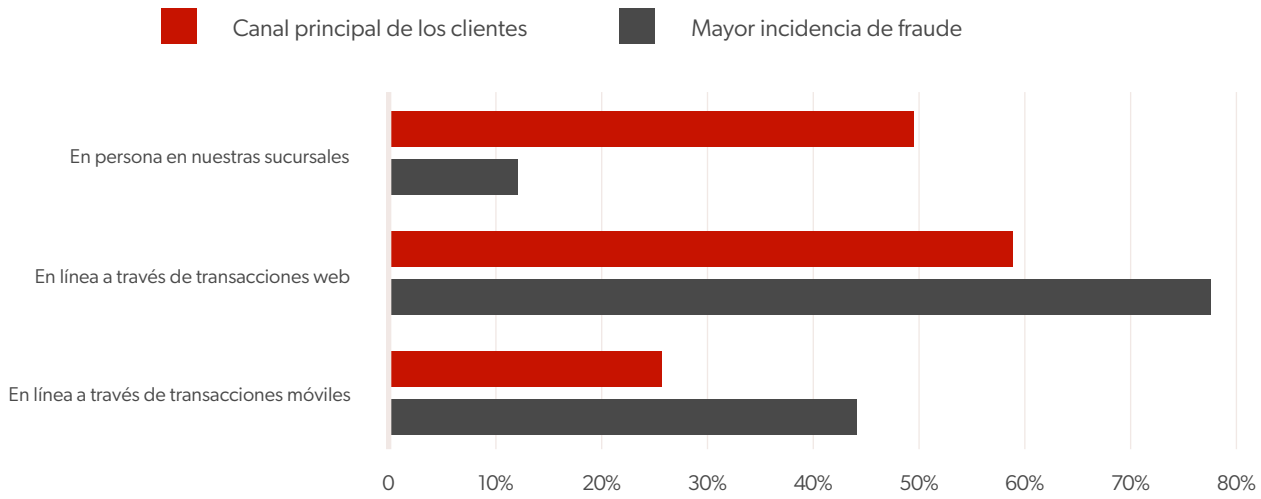
La principal vulnerabilidad para los encuestados es que los esquemas de fraude actuales evolucionan demasiado rápido para que puedan mantenerse al día, con un 83%. En segundo lugar, con un 57%, se encuentra el problema relacionado de cómo la supervisión de empleados, redes y dispositivos se ha vuelto más desafiante con fuerzas de trabajo remotas. Y el 55% de los encuestados dice que están preocupados por una dependencia excesiva de procesos manuales.

Por favor seleccione los tres esquemas de fraude más preocupantes para su institución en el próximo año.



El esquema de fraude más preocupante para las instituciones durante el resto de 2023 y 2024 es la divulgación de información/credenciales robadas, con un 52%, seguido de cerca por el fraude electrónico con un 50%. El phishing (sin compromiso de correo electrónico empresarial) ocupa el tercer lugar con un 44%, seguido por la toma de control de cuentas (móviles/web) con un 42%.

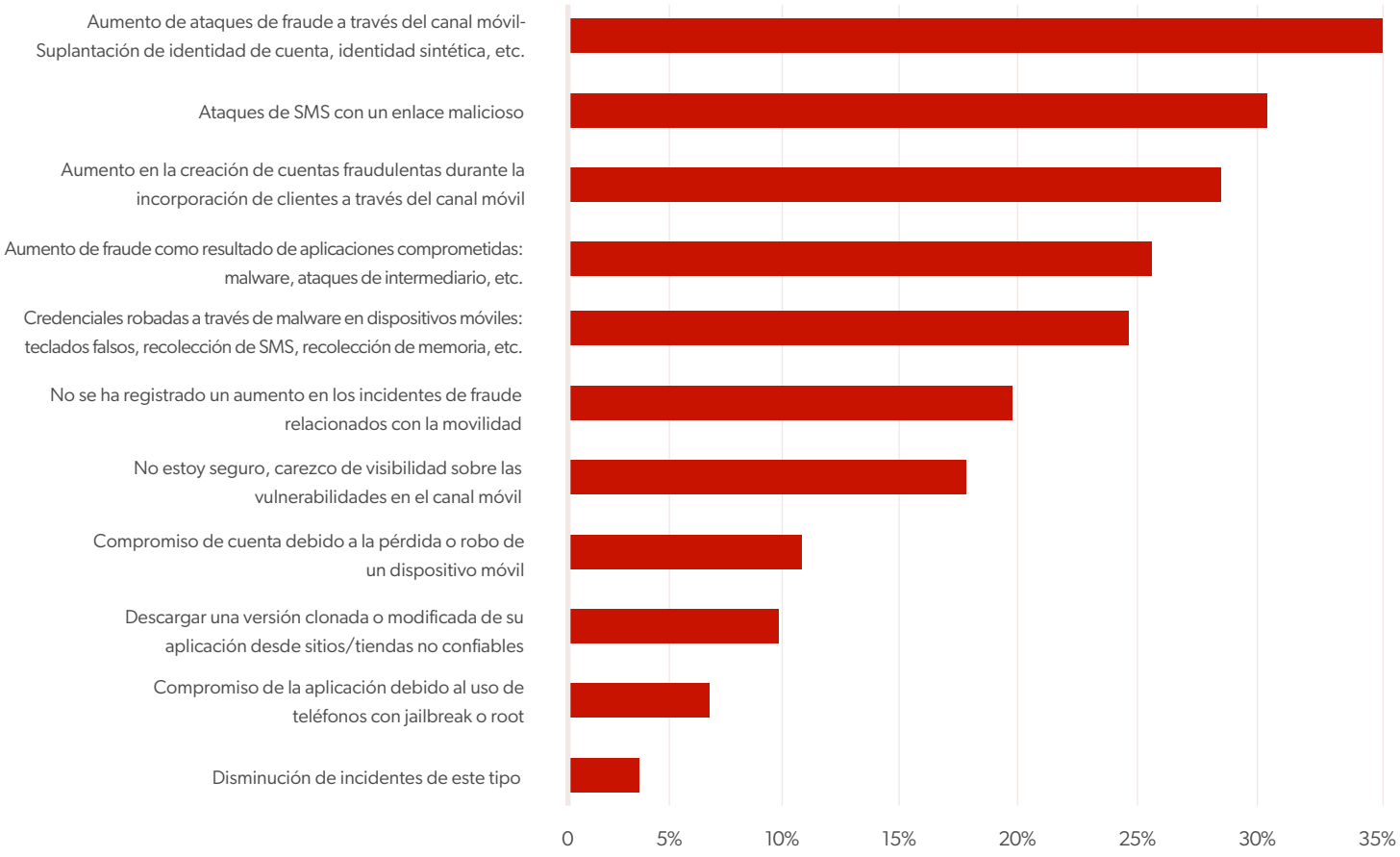
Hoy en día, ¿cuál es el canal principal que utilizan sus clientes para realizar negocios con su institución? ¿Cuál es el canal con la mayor incidencia de fraude?



Los encuestados dicen que el canal principal que utilizan los clientes para realizar negocios con su organización son las transacciones en línea, con un 44%. También afirman que este canal tiene la mayor incidencia de fraude, con un 58%, lo que supera ampliamente el uso. Parece que los gestores de riesgos, ya sea que lo sepan o no, están aceptando el potencial de niveles más altos de actividades fraudulentas a cambio de un aumento en el volumen de negocios a través de los canales en línea.

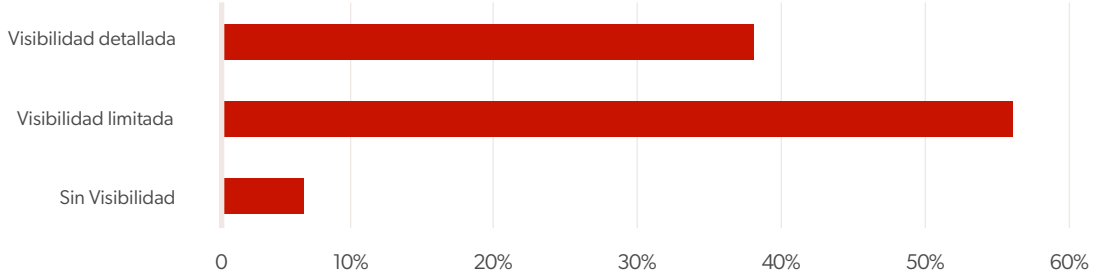
En contraste, los encuestados dicen que los negocios en persona en las sucursales representan el 37% del uso, pero solo el 9% del fraude. Las transacciones móviles ocupan el tercer lugar en términos de uso, con un 19%, pero el segundo lugar en fraude, con un 33%.

En el último año, ¿ha experimentado alguno de los siguientes incidentes de fraude específicamente relacionados con el canal móvil?



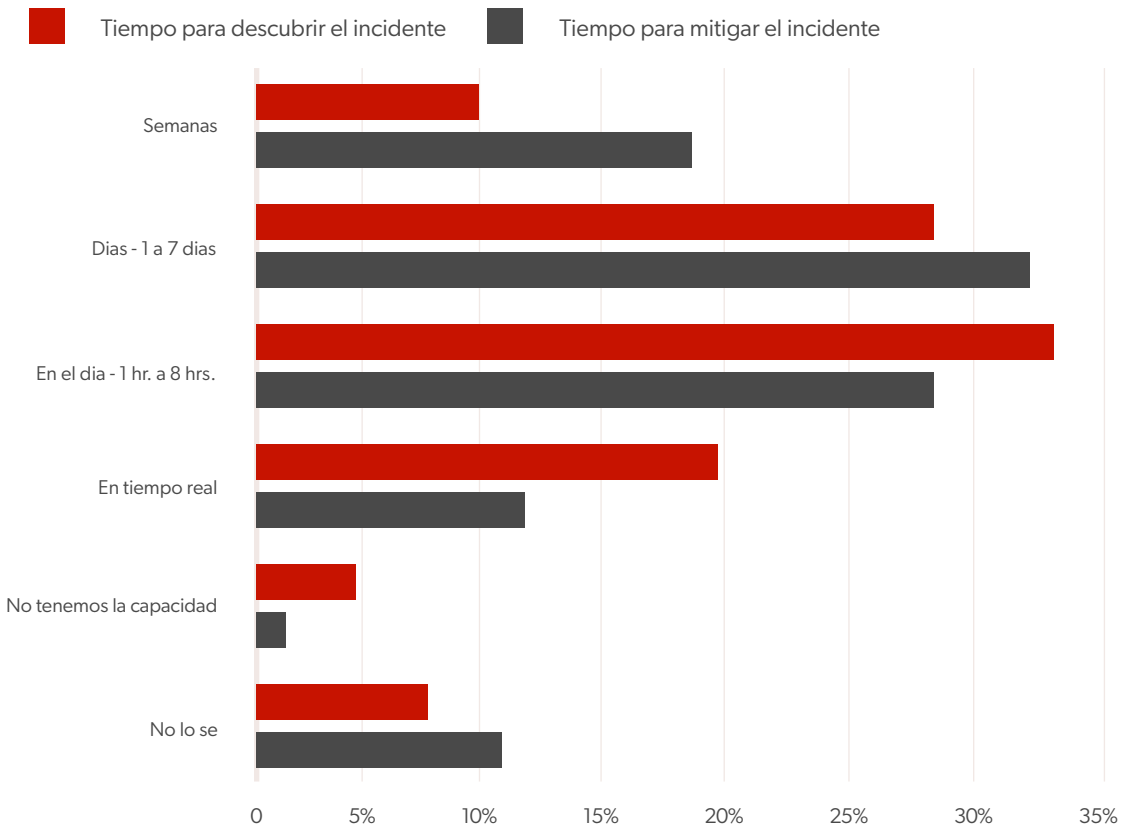
Aunque no hubo un método de ataque destacado, el 35% de los encuestados informa un aumento en los incidentes de fraude a través del canal móvil (suplantación de identidad de cuenta, identidad sintética, etc.), el 30% dice que los ataques de SMS con un enlace malicioso están en aumento, y el 28% informa un aumento en la creación de cuentas fraudulentas (incorporación de clientes) a través del canal móvil.

¿Cuánta visibilidad tiene su organización cuando se trata de identificar el impacto de un ataque de phishing?



La mayoría de las organizaciones, un 62%, afirman tener visibilidad limitada o nula cuando se trata de identificar el impacto de un ataque de phishing, y solo el 38% asegura tener visibilidad detallada. Los resultados sugieren que esta área sigue siendo un punto de mejora.

En promedio, ¿cuánto tiempo estima que le lleva a su organización descubrir/mitigar un incidente de fraude una vez que ocurre?

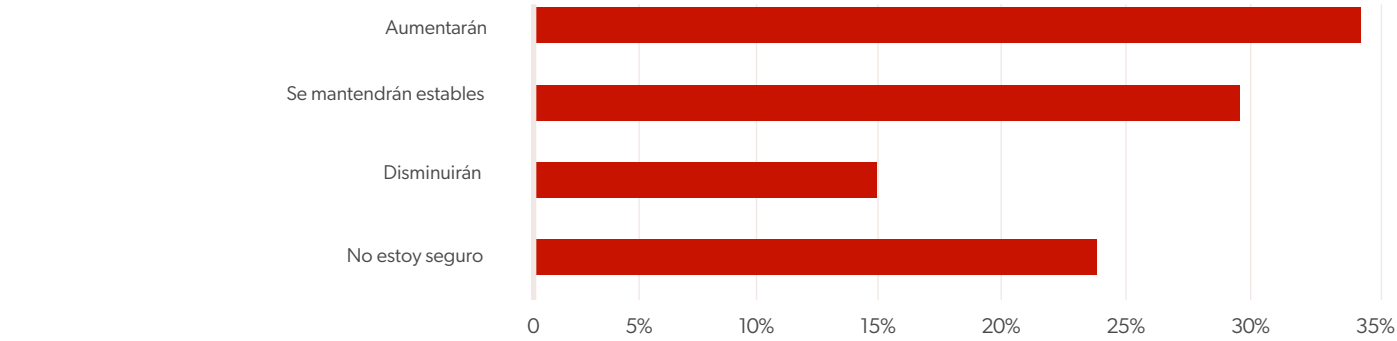


Diecinueve por ciento de los encuestados dicen que pueden descubrir un incidente de fraude en tiempo real. Eso representa un aumento del 7% desde 2019 y una disminución del 3% desde 2020. Once por ciento de los encuestados dicen que pueden mitigar el fraude en tiempo real.

Casi la mitad de los encuestados dicen que les lleva más de un día identificar el fraude. Aunque los porcentajes de intradía y de 1 a 7 días disminuyeron, los números de 'más de una semana' aumentaron desde 2019 y 2020. Además, al evaluar los tiempos de mitigación de años anteriores en general, los tiempos de mitigación aumentaron, lo que significa que a las instituciones les está llevando más tiempo.

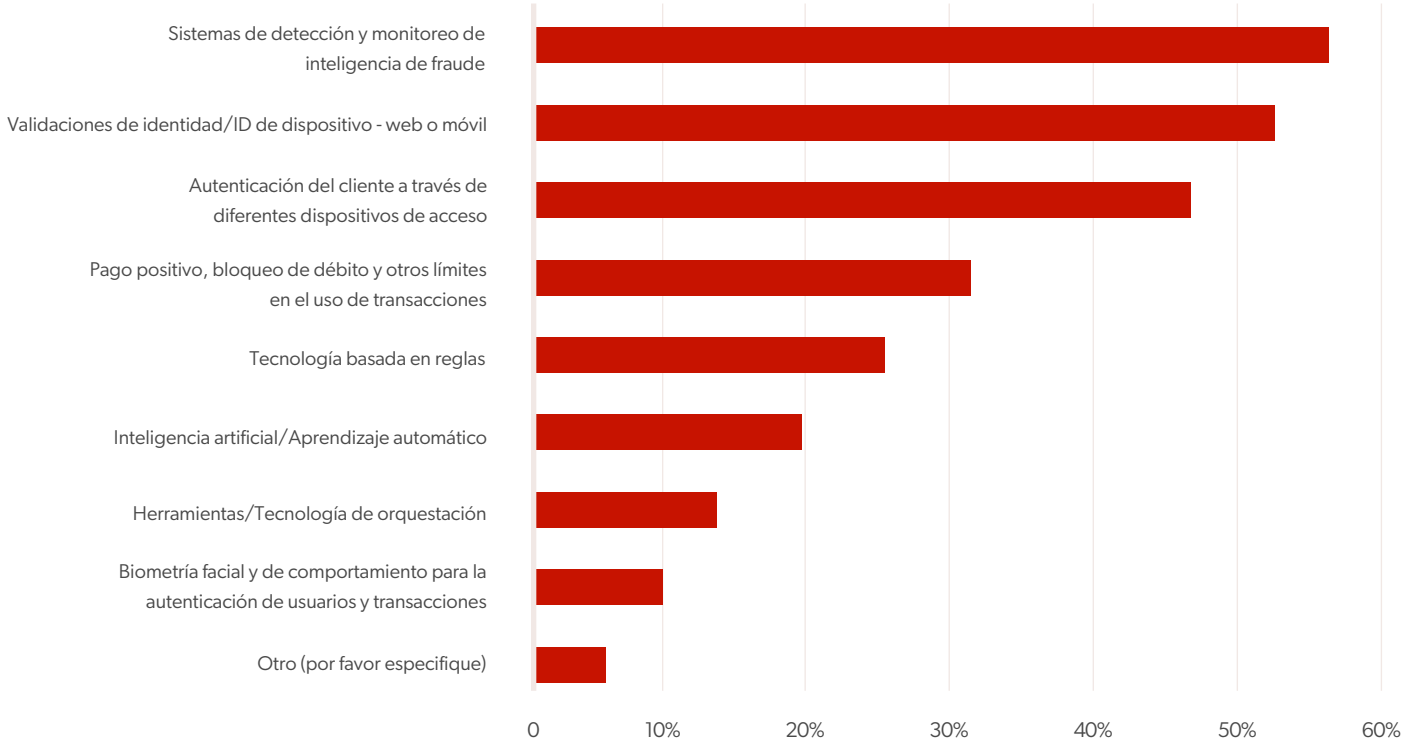
Sin embargo, el 97% de los encuestados dice que su capacidad para detectar y mitigar el fraude es promedio o superior. Por lo tanto, hay una desconexión entre sus percepciones y la realidad.

Considerando los últimos 12 meses en relación con las pérdidas por fraude y su postura actual contra el fraude, ¿cómo prevé que serán sus pérdidas monetarias por fraude durante los próximos 12 meses?



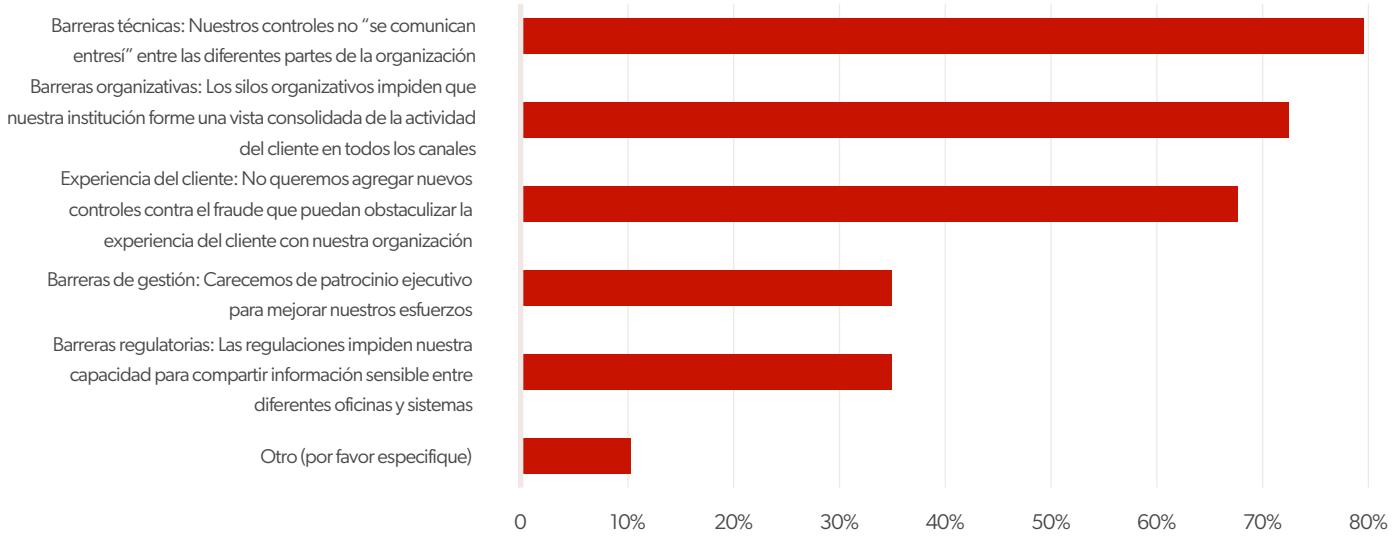
El treinta y cuatro por ciento de los encuestados esperan que las pérdidas monetarias por fraude aumenten durante los próximos 12 meses, mientras que el 29% espera que se mantengan estables y solo el 14% pronostica una disminución.

¿Qué tecnologías tuvieron el impacto más significativo en la prevención de pérdidas por fraude?



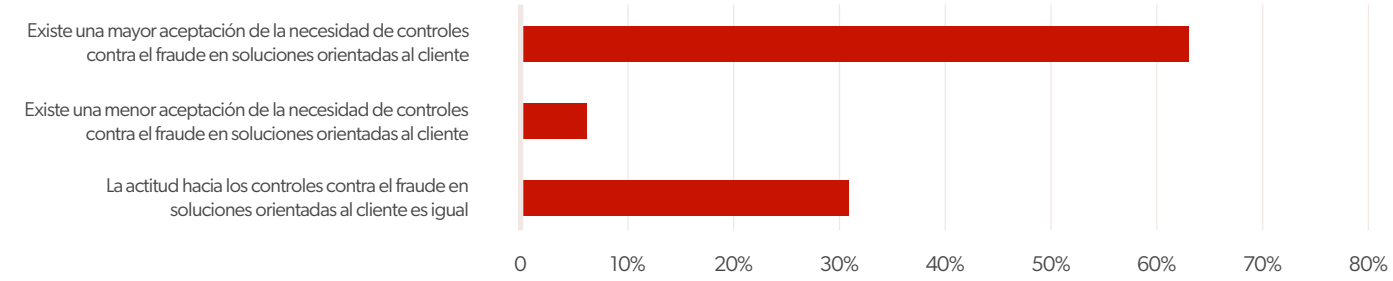
Los sistemas de detección y monitoreo de inteligencia de fraude encabezan la lista de las tecnologías que tienen el impacto más significativo en la prevención de pérdidas por fraude, con un 57%. La validación de identidad/el ID de dispositivo (web o móvil) ocupa el segundo lugar con un 53%, y la autenticación del cliente a través de diferentes dispositivos de acceso ocupa el tercer lugar con un 47%.

Por favor seleccione las tres barreras principales de su organización para mejorar la prevención del fraude.



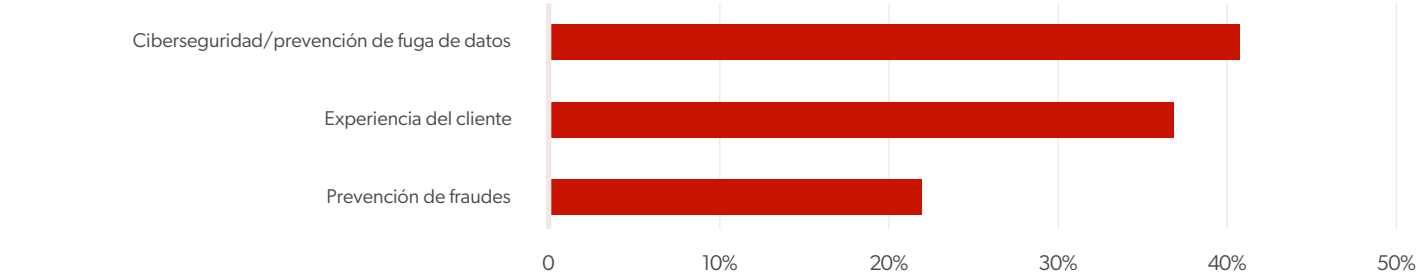
La principal barrera para mejorar la prevención de fraudes son las barreras técnicas, según el 80% de los encuestados. Le siguen las barreras organizativas con un 73%, y la experiencia del cliente con un 68%.

En su institución, ¿cómo ha cambiado la actitud hacia los controles contra el fraude en comparación con la experiencia del cliente?



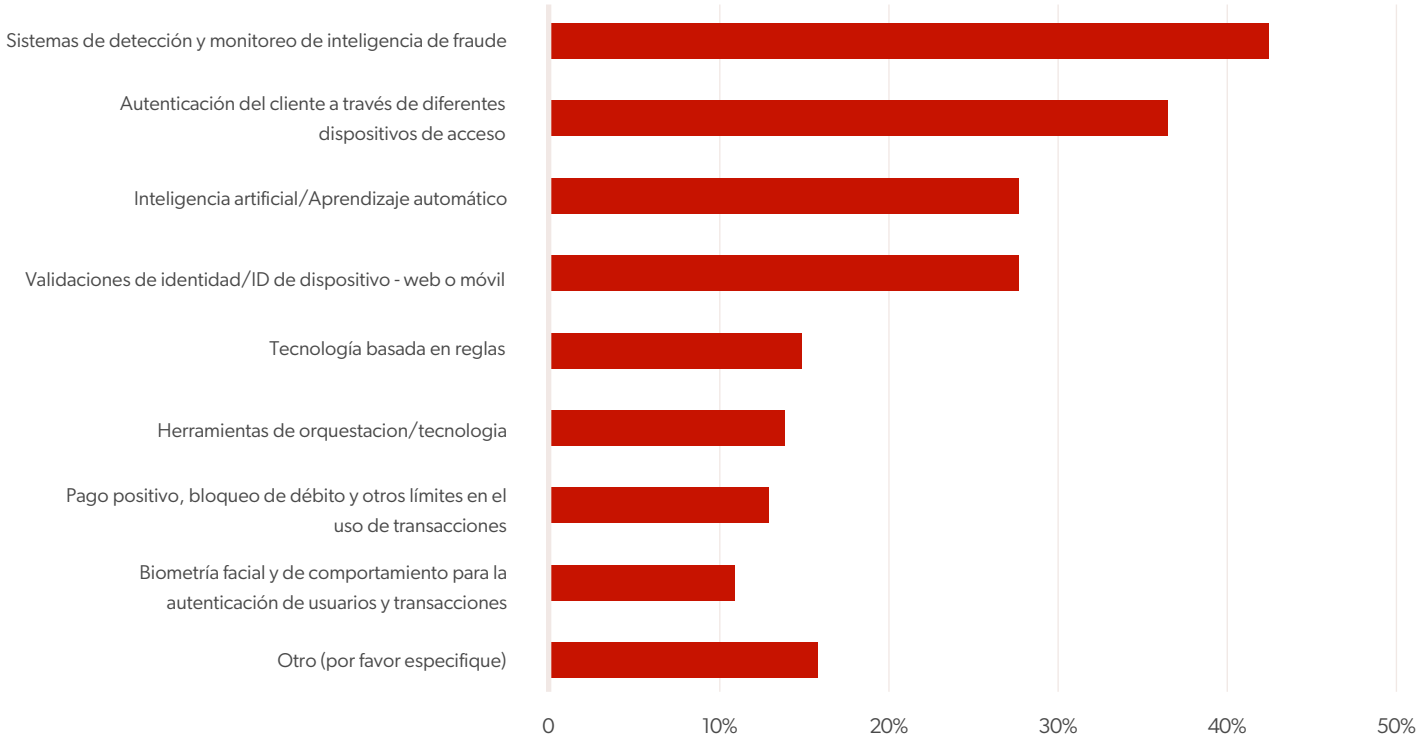
La mayoría de los encuestados, un 63%, dicen que hay una mayor aceptación de la necesidad de controles contra el fraude en soluciones orientadas al cliente, en comparación con el 31% que dice que la actitud se mantiene igual y solo el 6% que dice que hay una menor aceptación.

En su opinión, ¿cuál de estos tiene la mayor prioridad para su institución en soluciones orientadas al cliente hoy?



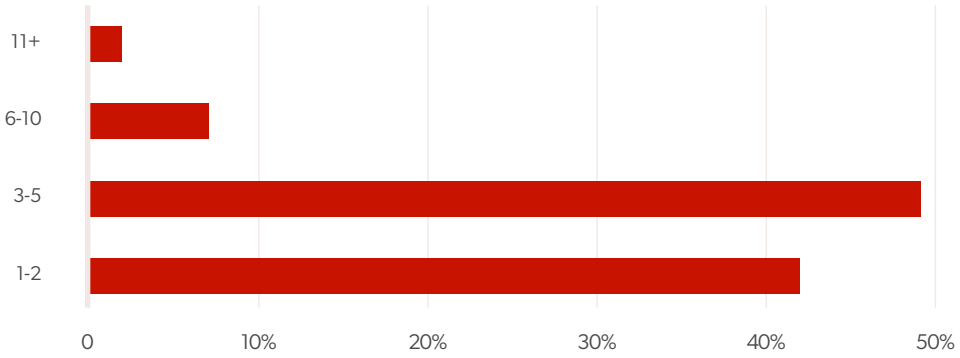
Cuando se les preguntó cuál es la mayor prioridad para su institución en soluciones orientadas al cliente en la actualidad, el 41% de los encuestados respondió ciberseguridad/prevención de brechas de datos. La experiencia del cliente ocupó el siguiente lugar con un 37%, seguido de la prevención de fraudes con un 22%.

¿En cuáles de las siguientes tecnologías planea invertir en los próximos 18 meses?



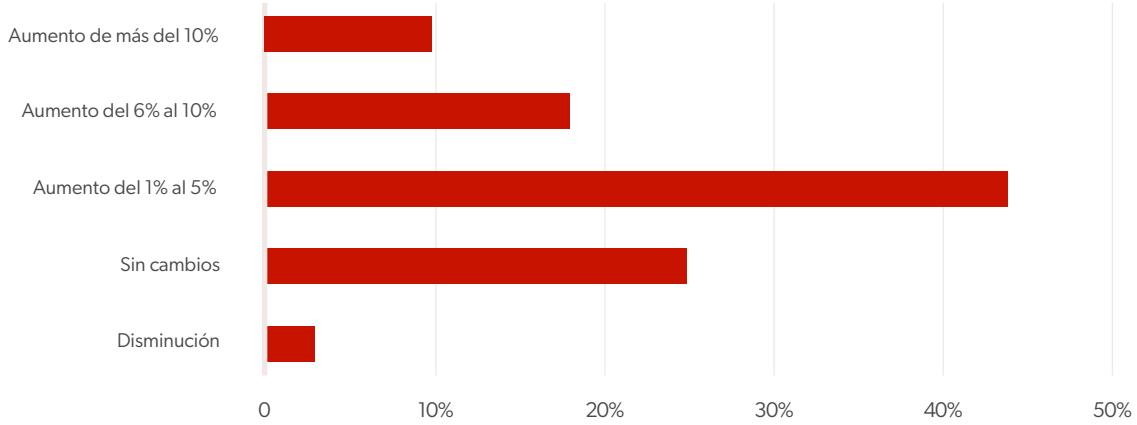
El cuarenta y tres por ciento de los encuestados dicen que planean invertir en sistemas de detección y monitoreo de inteligencia de fraude en los próximos 18 meses. Le siguen la autenticación del cliente a través de diferentes dispositivos de acceso con un 37%, y las validaciones de identidad/ID de dispositivo (web o móvil) y la inteligencia artificial/aprendizaje automático, ambos con un 28%.

¿Cuántos proveedores diferentes compra para satisfacer sus necesidades de prevención de fraude?



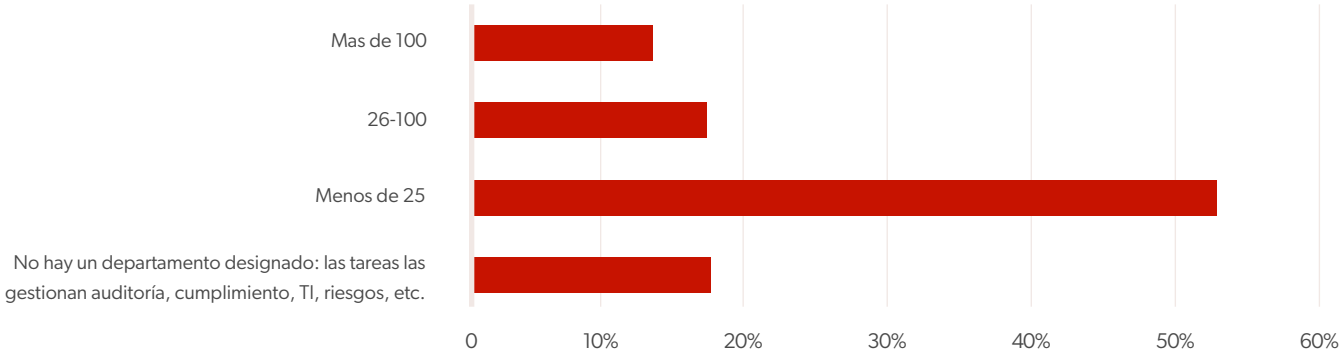
El cuarenta y nueve por ciento de los encuestados dicen que utilizan de tres a cinco proveedores, y el 42% dicen que utilizan uno o dos. Solo el 9% dicen que utilizan seis o más.

¿Cómo espera que cambie su presupuesto dedicado a la prevención de fraudes en el próximo año?



El cuarenta y cuatro por ciento de los encuestados dicen que su presupuesto dedicado a la prevención de fraudes aumentará en un 1% a un 5% en el próximo año. El veinticinco por ciento pronostican que no habrá cambios, el 18% espera un aumento del 6% al 10%, y el 10% espera un aumento de más del 10%. Solo el 3% espera una disminución.

¿Cuán grande es el departamento de su organización asignado a la prevención y detección de fraudes?



La mayoría de los encuestados, el 53%, dice que su departamento asignado a la prevención y detección del fraude está formado por menos de 25 personas. El diecisiete por ciento dice que no tiene un departamento designado, el 17% informa que tiene entre 26 y 100 personas y solo el 13% dice que tiene más de 100 personas.

Conclusiones

Visibilidad

La preocupación más grande que se desprende de los datos es que solo el 19% de los encuestados logra identificar en tiempo real el impacto de un fraude de phishing, y los tiempos de respuesta están aumentando. Esto significa que las empresas se están volviendo más lentas en su capacidad para identificar que han sido afectadas por el fraude. La mitigación en tiempo real es aún menor, con solo un 11%.

Un factor contribuyente significativo es que el 56% de los encuestados dice que tienen una visibilidad limitada cuando se trata de identificar el impacto de un ataque de phishing, y el 6% admite que no tienen visibilidad.

Herramientas y silos

Los encuestados reconocen los beneficios que se pueden obtener mediante la implementación de sistemas de detección y monitoreo de inteligencia de fraude, que lideran la lista de tecnologías con el impacto más significativo en la prevención de pérdidas por fraude, con un 57%. Sin embargo, solo el 43% de los encuestados tiene planes de invertir en sistemas de detección y monitoreo de inteligencia de fraude en los próximos 18 meses.

Otro problema es que la implementación de herramientas parece estar ocurriendo de manera fragmentada, ya que el 80% afirma que sus controles no se comunican entre sí, siendo esta la principal barrera para mejorar la prevención de fraudes. Se requiere un enfoque integral.

Las entidades necesitan superar sus barreras técnicas y organizativas. Esto ha sido una tendencia constante en el informe desde 2020. Los silos están impidiendo que las instituciones adopten un enfoque de múltiples capas. Sin ello, se vuelve muy difícil mantenerse al día con la velocidad a la que evoluciona el panorama del fraude.

La preocupación por los procesos manuales, que implica la necesidad de automatización, sigue creciendo, pero esto puede verse como un desarrollo positivo que probablemente impulse la automatización en el futuro.

Un enfoque holístico

Necesitamos adoptar un enfoque integral para combatir el fraude. No podemos analizar las partes o componentes de forma aislada. Las organizaciones deben ser alentadas a aprovechar los sensores que tienen en cada una de las partes: usuario, dispositivo, transacción/evento, para crear una evaluación única y continua de la sesión.

Aunque es de esperar un lapso de tiempo entre la conciencia de la solución y su implementación, la brecha entre la percepción del rendimiento y la evidencia del rendimiento es una característica persistente de esta serie de encuestas. Parece haber una falta de conciencia/benchmarking del rendimiento de sus pares y cierta dosis de complacencia.

Esperamos que los lectores de esta encuesta reconozcan cómo las expectativas de una prevención del fraude de alto rendimiento han seguido aumentando, y si ven que se están quedando atrás en las mejores prácticas, se levantarán a la ocasión al enfocarse en la identificación en tiempo real del impacto del phishing y al adoptar un enfoque integral para implementar tecnologías de prevención del fraude.

Análisis de la encuesta

Discusión de la Encuesta Faces of Fraud de Appgate con Mike Lopez, Vicepresidente Senior de Appgate

MIKE LOPEZ
Vicepresidente Senior, Appgate

Percepción vs. Realidad

TONY MORBIN: ¿Qué destacó para ti en los resultados de la encuesta y cómo se compara eso con lo que generalmente encuentras en el mercado?

MIKE LOPEZ: Una de las cosas que me llamó la atención fue la respuesta en relación a los plazos para identificar y mitigar el fraude. Solo el 19% de los encuestados dijo que pueden identificar el fraude en tiempo real. Eso no solo destaca estadísticamente para mí, sino que la abrumadora mayoría de los encuestados dijo que creen que su capacidad para identificar y mitigar el fraude es, o bien promedio o superior. Esa es una tendencia que hemos visto consistentemente desde que hicimos esto con ISMG durante más de cinco años. Es una desconexión entre la percepción de la efectividad de la postura de fraude de la organización y la realidad en términos de la capacidad real para identificar y mitigar el fraude.

El Mayor Desafío

MORBIN: ¿Cómo se alinean las respuestas de los encuestados sobre cuáles son las mayores vulnerabilidades en sus defensas contra el fraude con lo que estás observando?

LOPEZ: Desde 2019, el mayor desafío que los encuestados ven es la rapidez con la que evoluciona el fraude y la velocidad con la que los atacantes modifican sus ataques para mantenerse al día con las tecnologías emergentes implementadas por las instituciones financieras. Este año, el 83% de los encuestados dijo que esa es su mayor vulnerabilidad. Eso representa un aumento desde el 55% en 2020, y es algo en lo que las instituciones financieras deben centrarse.

Hay múltiples razones por las cuales esto es un problema, y está incorporado en las respuestas. Uno de ellos es el hecho de que todavía hay una abundancia de procesos manuales en funcionamiento en las instituciones financieras. La segunda parte, que es el mayor contribuyente a esto, es la falta de orquestación no solo entre las tecnologías implementadas por las instituciones financieras y los encuestados, sino también entre las unidades de negocio en sí.

> *"Todavía se están creando silos significativos entre estos componentes que están obligando a que se ejecuten procesos manuales, y eso está permitiendo que los estafadores y los adversarios se mantengan un paso por delante de las propias instituciones."*

Todavía se están creando silos significativos entre estos componentes que están forzando a que se ejecuten procesos manuales, y eso está permitiendo que los estafadores y adversarios se mantengan un paso por delante de las propias instituciones.

Un Enfoque Holístico

MORBIN: ¿Cuando se trata de los ataques que preocupaban a los encuestados, estás de acuerdo con sus prioridades?

LOPEZ: La mayor amenaza en este momento desde la perspectiva de los encuestados es definitivamente el canal en línea. Pero parte del problema es que el aspecto de los silos de datos está impidiendo que las instituciones tomen decisiones adecuadas de manera efectiva. Destacan constantemente el equilibrio entre los controles de mitigación anti-fraude y la experiencia del cliente. Y en ese proceso, se centran en esos silos, lo que crea programas ineficaces que afectan directamente a la experiencia del usuario. Deberían adoptar un enfoque holístico.

Mejor Orquestación

MORBIN: Me sorprendió la falta de visibilidad informada para identificar el impacto de un ataque de phishing. ¿Fueron los encuestados particularmente deficientes en este sentido?

LOPEZ: Por lo general, ya sea en las cooperativas de crédito más pequeñas o en las instituciones financieras más grandes, existe una división entre quién es responsable del fraude y quién es responsable de la ciberseguridad. Y por lo general, los controles contra el phishing caen bajo el lado de la ciberseguridad. Esa información no se está transmitiendo a la unidad de fraude para que puedan correlacionar sus pérdidas por fraude. Eso es problemático.

Automatización y Inteligencia Artificial

MORBIN: Los encuestados informaron sobre las tecnologías que creen que tienen el mayor impacto en la prevención de pérdidas por fraude. ¿Tienen razón?

LOPEZ: En última instancia, la tecnología es el camino a seguir. Debe continuar invirtiendo en automatización y ser capaz de incorporar la mayor cantidad de puntos de datos posible. La orquestación debe ser considerada. No puede mirar factores individuales o sensores de forma aislada. Necesita un enfoque holístico. Si va a mantenerse por delante de los adversarios, no puede tener puntos únicos para la detección. Debe analizar los patrones de usuario, los patrones de dispositivo y los patrones de transacciones de manera conjunta para avanzar de manera efectiva hacia un programa que sea eficaz. Debe invertir en automatización, inteligencia artificial y biometría del comportamiento. Esto sin duda ayudará a solidificar su postura.

> *Si vas a mantener ventaja sobre los adversarios, no puedes depender de puntos únicos para la detección. Necesitas analizar los patrones del usuario, los patrones del dispositivo y los patrones de transacciones de manera conjunta para avanzar eficazmente hacia un programa que sea efectivo.*

Un Puntaje de Riesgo Colectivo

MORBIN: ¿Vio reflejadas esas necesidades en lo que las empresas informaron como las tecnologías en las que planean invertir en los próximos 18 meses?

LOPEZ: Están acertando en todo en lo que deberían invertir. Están considerando sistemas de detección y monitoreo, que representaron el 43% de las respuestas. También están considerando la autenticación del cliente y la validación de la identidad, ya sea en el lado del usuario o en el lado del dispositivo, lo cual fue el 37%. El porcentaje restante se destina a la inteligencia artificial/aprendizaje automático, por lo que están enfocándose en todo de manera correcta. El punto clave es cómo pueden hacer que cada uno de esos componentes se comunique entre sí. Necesitan obtener un puntaje de riesgo colectivo que incorpore el riesgo del dispositivo, el riesgo del usuario, la identidad del usuario y la inteligencia artificial o el aprendizaje automático en torno a la transacción o las sesiones mismas, para tener un solo puntaje de riesgo en lugar de mirar cada uno de esos componentes de nuevo de manera aislada.

Sobre ISMG

Information Security Media Group (ISMG) es la organización mediática más grande del mundo dedicada exclusivamente a la seguridad de la información y la gestión de riesgos. Cada una de nuestras 36 propiedades mediáticas proporciona educación, investigación y noticias específicamente diseñadas para sectores verticales clave, que incluyen la banca, la atención médica y el sector público; geografías que abarcan desde América del Norte hasta el sudeste asiático; y temas como la prevención de brechas de datos, la evaluación del riesgo cibernético y el fraude. Nuestra serie anual de cumbres globales conecta a profesionales de seguridad senior con líderes de la industria para encontrar soluciones prácticas para los desafíos urgentes de ciberseguridad.

(800) 944-0401 • sales@ismg.io

BANK INFO SECURITY® · CU INFO SECURITY® (Just for Credit Unions) · GOV INFO SECURITY® · HEALTHCARE INFO SECURITY®

infoRisk TODAY · CAREERS INFO SECURITY® · Data Breach TODAY (Prevention. Response. Notification.) · CyberEd.io

CIO.inc · DeviceSecurity.io · PaymentSecurity.io · FraudToday.io

CYBER THEORY · CyberEdBoard · Xtra mile LIFECYCLE MARKETING · GREYHEAD

ISMG
INFORMATION SECURITY
MEDIA GROUP

902 Carnegie Center • Princeton, NJ • 08540 • www.ismg.io