FORRESTER®

Explorando el panorama del fraude y la autenticación multicanal

Cómo la biometría potencia las estrategias actuales de autenticación y prevención del fraude

Empecemos →

RESUMEN DE OPORTUNIDADES DE FORRESTER: ESTUDIO PERSONALIZADO ENCARGADO POR NUANCE | JUNIO DE 2019

El paradigma de la autenticación y la prevención del fraude está cambiando

Las marcas se han centrado tradicionalmente en la voz en el *contact center* para autenticar a los clientes y prevenir el fraude. Sin embargo, a medida que aumentan las expectativas del cliente de realizar interacciones rápidas y fluidas, los canales digitales de autoservicio, como las aplicaciones móviles y los chats, se han disparado, y con ellas, el riesgo de fraude. A medida que las empresas trabajan para satisfacer las expectativas de experiencias digitales rápidas y sin fricción, están descubriendo la necesidad de cambiar sus estrategias de autenticación para adaptarse a trabajar en varios canales para proteger a los clientes y el negocio.

En abril de 2019, Nuance encargó a Forrester Consulting una evaluación del fraude y la autenticación. Con nuestra encuesta realizada a 561 responsables de la toma de decisiones sobre fraude y autenticación de todo el mundo, hemos tratado de entender qué canales son el objetivo, cómo están respondiendo las organizaciones, y cómo pueden mejorar las marcas.

Principales conclusiones

El fraude multicanal ya es algo habitual. A medida que los clientes acceden a servicios en varios canales, los estafadores trabajan en diferentes canales para aprovechar las vulnerabilidades. La autenticación multicanal es crítica.

Las empresas no están lo suficientemente preparadas para combatir el fraude en varios canales. A pesar de la confianza en la prevención del fraude en canales individuales, las empresas confían mucho menos en sus capacidades de prevención a través de varios canales.

Los métodos de autenticación biométrica son la clave para una estrategia multicanal moderna. Las empresas que utilizan datos biométricos en más de un canal tienden más a describir su prevención del fraude en varios canales como totalmente optimizada o casi optimizada.

A medida que la autenticación digital se dispara, surgen nuevos riesgos de fraude

Las experiencias móviles y digitales están muy demandadas, y el crecimiento de la autenticación en dichos canales es sustancial: el 67 % las empresas han observado un aumento del 10 % o más en la autenticación en sus aplicaciones móviles en 24 meses. Y a medida que las empresas cambian la forma de ponerse en contacto con los clientes, están cambiando la forma en que perciben y gestionan el riesgo de fraude:

- El 70 % está de acuerdo en que tradicionalmente los canales de voz han sido el foco de la estrategia de prevención del fraude.
- El 74 % está de acuerdo en que abrir nuevos canales para la participación del cliente ha incrementado su vulnerabilidad al fraude.
- El 87 % está de acuerdo en que ahora están centrados en la prevención del fraude en los canales digitales.

Rango de canales donde las empresas experimentan los niveles más altos de autenticación del cliente	Porcentaje de empresas que han observado un aumento de la autenticación del cliente de un 10 % o más durante los últimos 24 meses en este canal
Web	55 %
Aplicación móvil	67 %
En persona	25 %
Teléfono	28 %
Chat	54 %

Base: ejecutivos diversos con responsabilidad en la prevención del fraude y la autenticación del cliente en empresas a nivel mundial
Fuente: estudio realizado por Forrester Consulting por encargo de Nuance, abril de 2019.

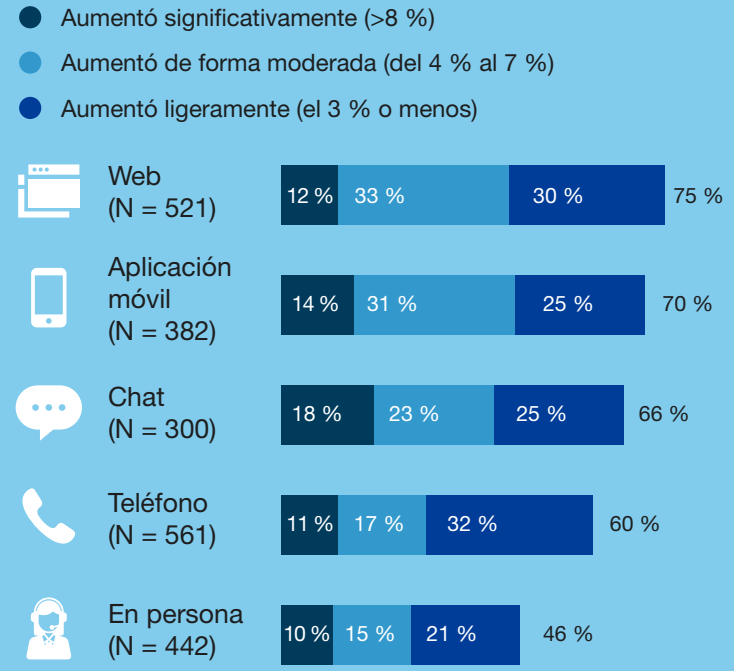
El fraude va en aumento, y no hay ningún canal seguro

Por desgracia, la rápida adopción por parte de los clientes de los servicios digitales ha dado lugar a un aumento similar del porcentaje de fraude en los canales digitales: el 45 % de las empresas experimentó un aumento del 4 % o más en el porcentaje de fraude en sus aplicaciones móviles y sitios web en los últimos 24 meses.

Entre tanto, a pesar del éxito de las estrategias de "primero en el móvil" para potenciar a los clientes expertos digitales, los canales telefónico y presencial también están creciendo tanto en términos de autenticación como de fraude en muchas empresas. Aunque el 87 % de las empresas afirman estar centradas en la prevención del fraude en los canales digitales, es evidente que los canales heredados de las empresas aún necesitan protección.

Los canales digitales son el mayor objetivo de fraude, pero los canales heredados no pueden convertirse en un punto ciego.

"¿Cómo ha cambiado el porcentaje de fraude (incluido el fraude detectado antes de que haya ocurrido y el fraude descubierto con posterioridad) durante los últimos 24 meses en los siguientes canales?"



Base: ejecutivos diversos con responsabilidad en la prevención del fraude y la autenticación del cliente en empresas a nivel mundial
Fuente: estudio realizado por Forrester Consulting por encargo de Nuance, abril de 2019.

Las empresas tienen un exceso de confianza en su capacidad para prevenir el fraude en los canales individuales

A pesar del creciente fraude, las empresas creen que su capacidad de prevención es madura: hasta un 84 % afirma que su capacidad para prevenir el fraude en cualquier canal está casi o totalmente optimizada.[1] Sin embargo, las empresas tienen un exceso de confianza, pues se basan en muchos de los mismos métodos de autenticación en los que fácilmente ocurre fraude:[2]

- **Datos de identificación personal:** confirmación de las fechas de nacimiento, códigos postales, etc.; datos que a menudo están disponibles a través de las redes sociales o que se pueden comprar en la *dark web* después de una violación de datos.
- **Autenticación basada en el conocimiento:** por ejemplo, "¿de qué color era su primer coche?"; datos cada vez menos seguros debido a las violaciones de datos de alto perfil, o bien es tan complicada que frustra a los usuarios.
- **Contraseñas:** a menudo no son lo suficientemente complejas o los usuarios las anotan en lugares poco seguros; los estafadores intentarán combinaciones de contraseñas filtradas a través de varios sitios con la esperanza de que la misma contraseña haya sido reutilizada.

"Para cada uno de los canales de la lista, seleccione las formas en que su empresa registra, autentica, y/o autoriza a los clientes en dicho canal".

Cinco métodos de autenticación principales: los métodos más arriesgados están en blanco

TELÉFONO

Verificación de identidad
Datos de identificación personal
Autenticación basada en el conocimiento
Autenticación basada en el riesgo
Contraseñas

WEB

Contraseñas
Verificación de identidad
Datos de identificación personal
Autenticación basada en el conocimiento
Contraseña de un solo uso (OTP) basada en software

APLICACIÓN MÓVIL

Contraseñas
Verificación de identidad
Datos de identificación personal
Autenticación basada en el conocimiento
Contraseña de un solo uso (OTP) basada en software

EN PERSONA

Verificación de identidad
Datos de identificación personal
Autenticación basada en el conocimiento
Biometría de huella dactilar
Biometría facial

Base: ejecutivos diversos con responsabilidad en la prevención del fraude y la autenticación del cliente en empresas a nivel mundial
Fuente: estudio realizado por Forrester Consulting por encargo de Nuance, abril de 2019.

El fraude multicanal es la mayor amenaza

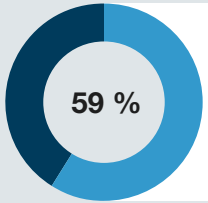
Aunque la mayoría de las empresas creen tener los canales individuales bajo control, los estafadores actúan en todos los canales, explotando las vulnerabilidades de cada uno. Por ejemplo, el fraude sin tarjeta (por ejemplo, utilizar un número de tarjeta de crédito robado sin una tarjeta física) es una vieja táctica, pero sigue siendo eficaz en el canal telefónico, mientras que la apropiación de cuenta (por ejemplo, al piratear contraseñas) es eficaz en los sitios web y aplicaciones móviles.

Como resultado, el 82 % de las empresas aceptan que la autenticación a través de todos los canales es cada vez más importante para la prevención del fraude. Sin embargo, sólo el 59 % definen su sistema de prevención del fraude multicanal como casi o totalmente optimizado; está, por lo tanto, mucho menos maduro que en cualquier canal individual. Las empresas no están suficientemente preparadas para combatir el carácter cambiante del fraude.

"¿Qué tipo de fraude ha sido más común en cada canal durante los últimos 24 meses?"

Canal	Tipo de fraude más común
Aplicación móvil y web	Apropiación de cuenta
Teléfono	Fraude sin tarjeta
Chat	Robo de identidad
En persona	Fraude de identidad sintética

Sólo el 59 % describe la capacidad de su empresa para evitar el fraude en todos los canales como casi o totalmente optimizada.



Por debajo de la madurez promedio de cualquier canal individual (81,2 %)

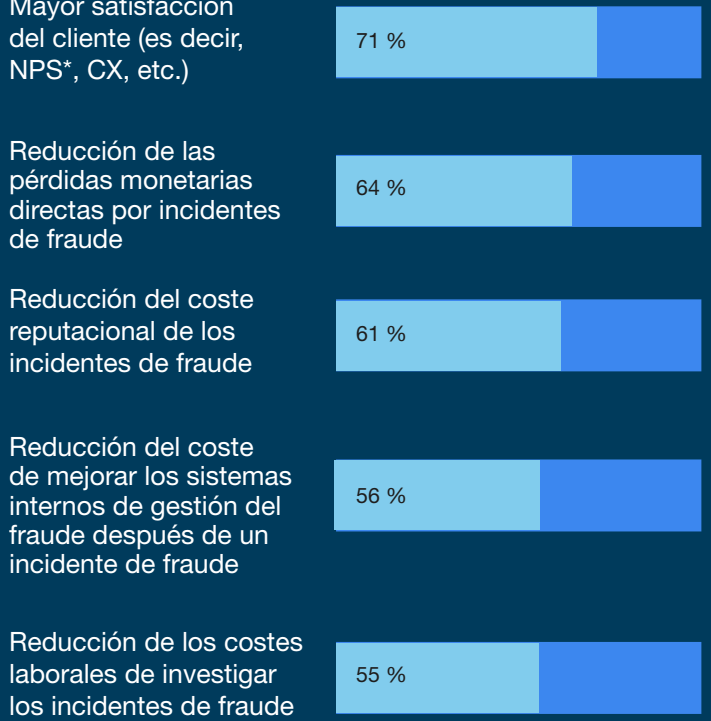
Base: 561 ejecutivos con responsabilidad en la prevención del fraude y la autenticación del cliente en empresas a nivel mundial
Fuente: estudio realizado por Forrester Consulting por encargo de Nuance, abril de 2019.

La prevención del fraude multicanal mejora la experiencia del cliente

A medida que las empresas trabajan en la prevención del fraude multicanal, ven la mejora de la experiencia del cliente como un resultado clave. Como es de esperar, supera cualquier beneficio de reducción de costes, probablemente debido al vínculo bien establecido entre experiencia del cliente y crecimiento de los ingresos.[3] La mejora de la experiencia del cliente se deriva de las experiencias de autenticación multicanal que tienen estas características:

- **Efectivas:** limitan las falsas aceptaciones y los falsos rechazos, incluso a medida que los clientes se mueven a través de los distintos canales.
- **Fáciles:** métodos de autenticación que no son frustrantes o engorrosos y que son consistentes en los distintos canales.
- **Con impacto emocional:** a los clientes les gustan las experiencias; por ejemplo, la confianza es una emoción especialmente importante que asociar a la autenticación.[4]

"¿Qué beneficios se obtendrían mediante una mejor prevención del fraude multicanal?"



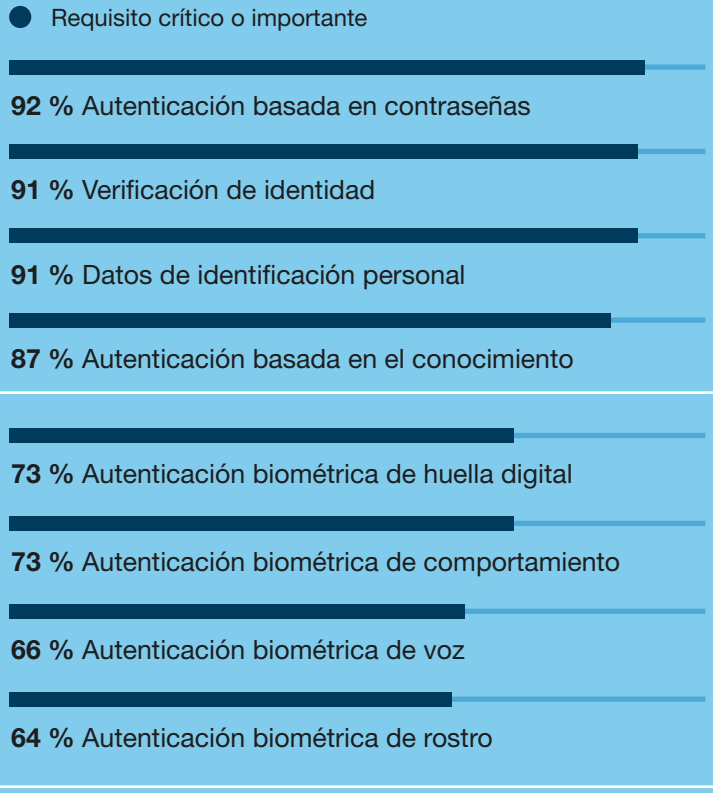
Base: 561 ejecutivos con responsabilidad en la prevención del fraude y la autenticación del cliente en empresas a nivel mundial
*Nota: Net Promoter y NPS son marcas de servicio registradas, y Net Promoter Score es una marca de servicio, de Bain & Company, Inc., Satmetrix Systems, Inc. y Fred Reichheld.
Fuente: estudio realizado por Forrester Consulting por encargo de Nuance, abril de 2019.

La biometría ayuda a las empresas a equilibrar la seguridad y la experiencia del cliente

Para mejorar la autenticación multicanal, prevenir el fraude y beneficiarse de una mejor experiencia de cliente, las empresas están evaluando métodos de autenticación heredados y emergentes. A pesar de los inconvenientes claros, las empresas todavía creen que las contraseñas, los datos de identificación personal y la autenticación basada en el conocimiento previenen el fraude. Sin embargo, también perciben el valor de la biometría. Al basarse en características innatas, estos métodos no añaden fricción a la interacción.[5] Además, la biometría puede identificar a los impostores independientemente de los conocimientos o habilidades de ingeniería social que posean. Las empresas que utilizan la biometría en varios canales:

- Es menos probable que dependan de contraseñas y datos de identificación personal en aplicaciones móviles, webs y teléfono (hasta 24 puntos).
- Es más probable que describan su prevención del fraude en cada canal como optimizada (hasta 20 puntos).
- Es más probable que describan su prevención del fraude multicanal como totalmente optimizada o casi optimizada (hasta 9 puntos).

Las empresas aún consideran que las formas de autenticación antiguas son importantes, pero muchas perciben el valor de la biometría



Base: 561 ejecutivos con responsabilidad en la prevención del fraude y la autenticación del cliente en empresas a nivel mundial
Fuente: estudio realizado por Forrester Consulting por encargo de Nuance, abril de 2019.

Conclusión

Las empresas libran una lucha permanente para proporcionar servicios cuándo, dónde y cómo sus clientes prefieren. Esto ha generado un cambio necesario en el modo en que las empresas perciben la autenticación y la prevención del fraude. Tanto los clientes legítimos como los estafadores se mueven libremente a través de los canales, y las empresas necesitan un moderno conjunto de herramientas de autenticación que pueda equilibrar las necesidades de seguridad con las exigencias de la experiencia del cliente. Herramientas emergentes como la biometría están cobrando importancia, no sólo por su notoria seguridad en comparación con los métodos antiguos, sino por su capacidad para facilitar y mejorar la experiencia de cliente. Las empresas que utilizan biometría en más de un canal están comenzando a aplicar la prevención del fraude multicanal.

Directora del proyecto:
Emma Van Pelt,
consultora de impacto en el mercado

Contribuyó a la investigación:
Grupo de investigación
de seguridad y riesgo de Forrester

Metodología

Este resumen de oportunidades fue encargado por Nuance. Para crear este perfil, Forrester Consulting aprovechó las investigaciones existentes del grupo de investigación de seguridad y riesgo de Forrester. Complementamos esta investigación con preguntas de la encuesta personalizada a 561 responsables de la toma de decisiones sobre fraude y autenticación de todo el mundo. La encuesta personalizada comenzó y se terminó en abril de 2019.

NOTAS FINALES

RETORNO 1. Un programa de prevención del fraude optimizado se define como un programa continuo y eficaz, integrado, proactivo, y por lo general, automatizado.
RETORNO 2. Fuente: "Top Cybersecurity Threats In 2018", Forrester Research, Inc., 27 de noviembre de 2017.
RETORNO 3. Fuente: "The US Customer Experience Index, 2018", Forrester Research, Inc., 19 de junio de 2018.
RETORNO 4. Fuente: "Drive Growth With Customer Trust And Build Brand Resilience", Forrester Research, Inc., 25 de septiembre de 2018.
RETORNO 5. Fuente: "Best Practices: Behavioral Biometrics", Forrester Research, Inc., 5 de mayo de 2018.

ACERCA DE FORRESTER CONSULTING

Forrester Consulting presta servicios de consultoría basados en análisis objetivos e independientes para ayudar a los directivos a cosechar éxitos en sus empresas. Con un alcance muy extenso que va desde una breve sesión de estrategias hasta proyectos personalizados, los servicios de Forrester Consulting le ponen en contacto directo con analistas que elaboran informes especializados sobre los retos específicos de su empresa. Para obtener más información, acceda a forrester.com/consulting.

Demografía

REGIONES

- Europa: 55 %
- América: 36 %
- Australia: 9 %

CARGO

- Ejecutivo de alto nivel: 39 %
- Vicepresidente: 24%
- Director: 37 %

NÚMERO DE EMPLEADOS

- Entre 500 y 999: 1 %
- Entre 1000 y 4999: 54 %
- Entre 5000 y 19 999: 29 %
- 20 000 o más: 16 %

SECTOR

Está representada una variedad de industrias, entre las que se incluyen servicios financieros, minoristas, telecomunicaciones, manufacturación, tecnología, servicios profesionales, envíos y salud.

FORRESTER®