Comentarios de FIDO Alliance a la Comisión para el Mercado Financiero (CMF) de Chile

Abril 2026

Comentarios Norma en Consulta - Modificación NCG N°538 sobre Medidas de Seguridad y Autenticación de Operaciones Sometidas a la Ley n°20.009

Fast Identity Online (FIDO) Alliance agradece la oportunidad de enviar comentarios a la Comisión del Mercado Financiero (CMF) de Chile sobre su *Norma en Consulta - Modificación NCG N°538 sobre Medidas de Seguridad y Autenticación de Operaciones Sometidas a la Ley n°20.009*.

Como antecedente, *FIDO Alliance* es una organización público-privada de desarrollo de estándares industriales con múltiples partes interesadas, compuesta por más de 300 empresas y agencias gubernamentales de todo el mundo, dedicada a la creación de estándares y programas de certificación para la autenticación multifactor (MFA) y la autenticación sin contraseña, así como para la verificación remota de identidad.

Nuestros más de 40 miembros del directorio, cuyos logos se incluyen a continuación, demuestran la solidez del liderazgo de *FIDO Alliance*, así como la diversidad de sus miembros. Entre ellos se encuentran empresas líderes en banca, criptomonedas, tecnología financiera y pagos, además de muchos de los proveedores de seguridad a los que recurren estas empresas para protegerse contra ataques a verificación y autenticación de identidad.

El lanzamiento de *FIDO Alliance* en 2012, y la posterior creación y adopción masiva de los estándares de autenticación FIDO durante los catorce años siguientes, ha contribuido a transformar el mercado de la autenticación, abordando las preocupaciones sobre los problemas con las contraseñas, así como la creciente vulnerabilidad al phishing de las herramientas MFA *legacy* de primera generación, como las contraseñas de un solo uso (OTP), al tiempo que ha permitido mejoras significativas en la usabilidad de la MFA.

Actualmente, los estándares FIDO se han consolidado como la mejor opción para quienes buscan implementar autenticación resistente al phishing (como *passkeys* y llaves de seguridad) que sea más segura y fácil de usar que las herramientas de autenticación tradicionales. Cuentan con el respaldo de un amplio ecosistema de más de 1000 productos certificados según los estándares FIDO, lo que garantiza que empresas de todos los tamaños puedan elegir entre una variedad de productos interoperables y basados en estándares para satisfacer sus necesidades de autenticación. Además, dado que el protocolo *FIDO Web Authentication* es un estándar W3C, todos los principales navegadores y plataformas ofrecen soporte nativo para FIDO, lo que hace que la autenticación resistente al phishing sea igual de fácil (o incluso más fácil) de implementar que las herramientas de autenticación tradicionales.

FIDO Alliance aprecia y valora el continuo esfuerzo de la Comisión para fortalecer la ciberseguridad del ecosistema financiero chileno en virtud de la Ley N° 20.009.

Comprendemos y apoyamos plenamente la preocupación de la CMF por garantizar la inclusión financiera. Es fundamental asegurar que los segmentos de la población con menor nivel de digitalización, en particular los adultos mayores, no queden excluidos de los servicios financieros debido a dificultades operativas al adoptar nuevos mecanismos de Autenticación Reforzada del Cliente (ARC).

En ese sentido, no tenemos ninguna objeción a que se mantengan las herramientas de autenticación multifactor (MFA) tradicionales, como los conjuntos de datos impresos, para aquellos segmentos de la población que no están en condiciones de adoptar enfoques de autenticación reforzada del cliente (ARF) más modernos, como *passkeys*. Los bancos deben adaptarse a las necesidades de sus clientes y toma tiempo migrar desde otras herramientas *legacy*.

Dicho esto, si bien entendemos la razón para preservar el uso de estas tarjetas impresas y apoyamos la decisión, queremos destacar algunos aspectos para que la consideración de CMF, y también sugerir una enmienda al texto propuesto que podría ayudar a acelerar la transición de Chile hacia métodos más seguros de ARC:

1) **El phishing se está convirtiendo en un problema cada vez mayor, y el uso de tarjetas impresas dejará a los usuarios de dichas tarjetas vulnerables a los ataques de phishing.**

   En todo el mundo, los atacantes han logrado vulnerar muchas de las herramientas *legacy* que se utilizan en autenticación como protección. Los ciberdelincuentes han ideado métodos para atacar estas herramientas mediante phishing, como códigos OTP, tarjetas impresas con códigos o aplicaciones de autenticación push, lo que ha generado una necesidad imperiosa a nivel mundial de que los consumidores adopten herramientas de autenticación más modernas y resistentes al phishing.

   Estos ataques se ven impulsados por el auge de la IA generativa, que facilita a los atacantes la creación de ataques de phishing sofisticados que engañan a un mayor número de usuarios. Todo el proceso de phishing puede automatizarse mediante modelos de lenguaje a gran escala (LLM, por sus siglas en inglés), lo que reduce el costo de los ataques en más del 95 % y, al mismo tiempo, logra tasas de éxito iguales o superiores.[1]

   Muchos de estos ataques de phishing son posibles gracias a la tecnología deepfake. Los incidentes de deepfake en el sector fintech aumentaron un 700 % en 2023 en comparación con el año anterior.[2]

   Dada esta rápida evolución de los ataques contra la autenticación, resulta imperativo que cualquier medida regulatoria gubernamental que permita el uso de métodos de autenticación *legacy* y vulnerables al phishing también tome medidas para incentivar la retirada de estas herramientas obsoletas en los próximos años.

2) **Muchos otros gobiernos están específicamente pidiendo el uso de autenticación resistente al phishing para proteger a los consumidores en los servicios financieros.**

   - El año pasado, ENISA publicó una Guía de Implementación Técnica para las organizaciones que buscan cumplir con la directiva de ciberseguridad NIS2 en la Unión Europea.[3] La nueva guía dice

[1]Consulte https://hbr.org/2024/05/ai-will-increase-the-quantity-and-quality-of-phishing-scams
[2]Consulte https://www.wsj.com/articles/deepfakes-are-coming-for-the-financial-sector-0c72d1e5
[3]Consulte https://www.enisa.europa.eu/publications/nis2-technical-implementation-guidance

específicamente: “Siempre que sea posible, utilice la autenticación multifactor (MFA) resistente al phishing” y establece una jerarquía de MFA que dice:

> *“Se recomienda el uso de (MFA) resistente al phishing. A continuación, se muestra una lista de las soluciones disponibles actualmente, ordenadas de la más fuerte a la más débil.*
>
> - *Fuerte: Resistente al phishing*
> *- sin secretos compartidos, no vulnerable a ataques de ‘attacker-in-the-middle’;*
> *- clave privada criptográfica protegida que puede registrarse de forma segura en:*
> - *un dominio, de acuerdo con los estándares Fast Identity Online (FIDO) y W3C WebAuthn;*
> - *un proveedor de confianza, que cumple con los estándares de infraestructura de clave pública y X.509 de la Unión Internacional de Telecomunicaciones.*
>
> - *MFA 'Medio', por ejemplo:*
> - *Notificaciones push, coincidencia de números o basadas en aplicación.*
>
> - *MFA de ‘último recurso’:*
> - *Código OTP enviado por mensaje de texto o correo electrónico”*

- ENISA y CERT-EU también destacaron la importancia de FIDO en una publicación de 2022 titulada “Impulsando la Ciberresiliencia de su Organización (JP-22-01)”[4], señalando:

> *“Si es posible, evite usar SMS y llamadas de voz para proporcionar códigos de un solo uso y considere la posibilidad de implementar tokens resistentes al phishing, como tarjetas inteligentes y llaves de seguridad FIDO2 (Fast IDentity Online).”*

- En Estados Unidos, el Instituto Nacional de Estándares y Tecnología (NIST) ha aconsejado a las organizaciones que prioricen autenticación resistente al phishing, señalando en sus Directrices de Identidad Digital (SP 800-63B)[5]:

> *“En todos los casos, los verificadores **DEBERÍAN** fomentar el uso de autenticación resistente al phishing en AAL2 siempre que sea posible, ya que el phishing es un vector de amenaza importante.”*

Además, el NIST señala que los "secretos de búsqueda", como las tarjetas impresas que se utilizan en Chile, "no son resistentes al phishing".

- Asimismo, en Estados Unidos, la Agencia de Seguridad de Infraestructuras y Ciberseguridad (CISA) emitió un aviso[6] haciéndose eco de las preocupaciones de ENISA, señalando lo siguiente:

> *“No todos los métodos de MFA son igualmente seguras. Algunos son vulnerables al phishing, a los ataques de "bombardeo de mensajes", a la explotación de vulnerabilidades del protocolo del Sistema de Señalización 7 (SS7) y/o a los ataques de intercambio de tarjeta SIM. Estos ataques, de tener éxito, podrían permitir a un atacante acceder a las credenciales de autenticación MFA o eludirla y acceder a los sistemas protegidos por MFA.”*

[4]Consulte https://www.enisa.europa.eu/publications/boosting-your-organisations-cyber-resilience
[5]Consulte https://pages.nist.gov/800-63-4/sp800-63b.html
[6]Consulte https://www.cisa.gov/news-events/alerts/2022/10/31/cisa-releases-guidance-phishing-resistant-and-numbers-matching

La guía de CISA continúa señalando:

> *"Si bien cualquier método de autenticación multifactor (MFA) es mejor que ninguno y reducirá la superficie de ataque de una organización, la MFA resistente al phishing es el estándar de oro y las organizaciones deberían priorizar su migración"*. También señala que *"la única autenticación resistente al phishing ampliamente disponible es la autenticación FIDO/WebAuthn"*, aunque indica que la MFA basada en PKI también es resistente al phishing, si bien no está tan ampliamente disponible.

- Asimismo, en Estados Unidos, una circular[7] del 11 de agosto de 2022 de la Oficina de Protección Financiera del Consumidor (CFPB) establece lo siguiente:

> *"Las soluciones de autenticación multifactor (MFA) que protegen contra el robo de credenciales, como las que utilizan el estándar Web Authentication (FIDO) compatible con los navegadores web, son especialmente importantes."*

- También hacemos notar un informe de 2023 de la Junta de Revisión de Seguridad Cibernética (CSRB)[8] sobre los ataques asociados con el Grupo LAPSUS$ declaró:

> *"En la última década, el énfasis en la autenticación multifactor (MFA) ha impulsado la adopción de soluciones más seguras para mejorar la resistencia frente a ataques, en particular el phishing. La adopción de la MFA por parte de empresas y consumidores ha supuesto un avance beneficioso respecto al uso exclusivo de contraseñas para la autenticación. Sin embargo, la revisión del Consejo concluyó que los tipos de MFA que se utilizan actualmente en el ecosistema en línea no son suficientes para que la mayoría de las organizaciones o consumidores se protejan contra el tipo de ataques descritos en este informe.*
>
> *En particular, la entrega de códigos OTP y las notificaciones push mediante SMS y llamadas de voz (e incluso correo electrónico) son vulnerables a la ingeniería social y a los ataques de suplantación de SIM, y el ecosistema de atacantes es capaz de explotar fácilmente estas debilidades. Un lucrativo mercado criminal de suplantación de SIM permite el acceso a los servicios de telefonía móvil de las víctimas mediante el pago, centrándose en el secuestro de mensajes SMS y llamadas de voz. Los SMS no fueron diseñados para transmitir información confidencial como los códigos OTP, y su uso generalizado con este fin incentiva a los delincuentes a realizar ataques de suplantación de SIM, fraude de portabilidad y técnicas similares.*
>
> *Los desarrolladores de aplicaciones web y móviles deberían aprovechar las soluciones compatibles con Fast IDentity Online (FIDO)2, basadas en hardware e integradas de forma predeterminada en los dispositivos de los usuarios. El uso de estos tokens integrados debería facilitar la integración con aplicaciones y servicios web, aprovechando estándares como WebAuthn y tecnologías como Passkeys."*

3) *FIDO Alliance* está invirtiendo en iniciativas de experiencia de usuario (UX) para facilitar el uso de *passkeys* a todos los segmentos de la población.

A través de nuestro Grupo de Trabajo de Experiencia de Usuario (UXWG), la Alianza desarrolla y

[7] https://www.consumerfinance.gov/compliance/circulars/circular-2022-04-insufficient-data-protection-or-security-for-sensitive-consumer-information/
[8] https://www.cisa.gov/sites/default/files/2023-08/CSRB_Lapsus%24_508c.pdf

perfecciona continuamente directrices de diseño[9] basadas en investigación exhaustiva del consumidor. El objetivo de estas iniciativas es ayudar a las partes interesadas, como instituciones financieras, a implementar flujos de autenticación que eliminen las dificultades tecnológicas, transformando los procesos de seguridad tradicionalmente complejos en interacciones sencillas y cotidianas, como el uso de la huella dactilar o el reconocimiento facial que ya utilizan para desbloquear sus propios dispositivos personales.

Además, *FIDO Alliance* proporciona a la industria herramientas y recursos prácticos, como guías de implementación y manuales de despliegue especializados disponibles en *Passkey Central*[10], para que las organizaciones puedan auditar y optimizar sus interfaces de usuario de forma independiente. Estas inversiones continuas en experiencia de usuario y capacitación tienen como objetivo garantizar que todas las personas puedan usar *passkeys* fácilmente.

Finalmente, FIDO Alliance está a disposición para colaborar con el gobierno chileno, la CMF y las instituciones financieras en el desarrollo y apoyo de campañas de educación pública. Al generar conciencia sobre los riesgos de la autenticación legacy y los beneficios de los métodos modernos resistentes al phishing, como las passkeys, podemos incentivar a los consumidores a transiciónar hacia estas tecnologías más seguras, garantizando un ecosistema financiero digital seguro e inclusivo en Chile.

Cambios propuestos al texto (Sección V)

Para equilibrar la protección del usuario con la inclusión financiera, y para garantizar que la excepción transitoria no se convierta en un desincentivo estructural para que los emisores inviertan en mejor tecnología y usabilidad (UX), proponemos enriquecer la redacción de los párrafos penúltimo y último del reglamento propuesto (Sección V), añadiendo los textos resaltados:

> "La inclusión de clientes en los grupos a que se refiere el párrafo anterior solo podrá realizarse luego de que el emisor haya realizado sus mejores esfuerzos por proveer alternativas a estos clientes, **priorizando la provisión de métodos de autenticación altamente utilizables y resistentes al phishing (como *passkeys* o llaves de seguridad físicas)**, y será posible exclusivamente respecto de clientes vigentes a la fecha de emisión de esta normativa, a los que además deberá informar de los riesgos que conlleva la mantención de los medios de autenticación que vienen utilizando."

Además, sugerimos modificar el mandato de presentación de informes en el último párrafo para fomentar la innovación continua:

> "(...) Además, deberán enviar una actualización semestral del número de clientes que hayan dejado de ser parte de estos grupos, los que no podrán volver a ser incluidos en los mismos, **incluyendo un informe sobre las nuevas tecnologías de autenticación resistentes al phishing evaluadas o implementadas para reducir progresivamente la población exenta**."

Agradecemos la consideración de la CMF a nuestros comentarios y sugerencias. Si tiene alguna pregunta sobre nuestra presentación, o si desea obtener más información sobre los estándares y programas de certificación de FIDO, por favor comuníquese con nuestro Director Ejecutivo, Andrew Shikiar, andrew@fidoalliance.org, con nuestro Director para Latinoamérica, Diego Zavala, diego@fidoalliance.org, o con nuestro asesor de políticas públicas, Jeremy Grant, jagrant@venable.com.

[9]Consulte https://www.passkeycentral.org/design-guidelines/
[10]Consulte https://www.passkeycentral.org/