El nuevo rostro del fraude:

Combatiendo la suplantación de identidad y las amenazas de *deepfake*

Imagínese que **una cantidad importante de dinero** fuera transferida desde la **cuenta bancaria** de su empresa con autorización de un alto ejecutivo de su organización.

Sin embargo, más adelante descubre que ha sido víctima de fraude...

Lamentablemente, esta situación es cada vez más común. En PwC, la consideramos una tendencia global en aumento, con empresas de diversos sectores industriales que están siendo víctimas de esta situación.

Según la **Encuesta Global sobre Delitos Económicos 2024** el delito cibernético, incluido el fraude de suplantación de identidad mediante tecnología *deepfake*, es el tipo de fraude más reportado en Europa Central y del Este.

Según el Global Digital Trust Insights Report **2025**, los ejecutivos del área de seguridad informan que la IA Generativa (67%) y las tecnologías en la nube (66%) han ampliado la superficie de exposición a ciberataques durante el último año. Esto significa que las empresas son más vulnerables a amenazas sofisticadas.

¿Qué es el fraude de suplantación de identidad?

El fraude de suplantación de identidad es una amenaza creciente en nuestro mundo digital, donde los delincuentes imitan a representantes legítimos de empresas para robar información confidencial o dinero.

Esto puede incluir:

Phishing

Los estafadores envían correos electrónicos engañosos haciéndose pasar por personas u organizaciones de confianza para engañar a las personas y que proporcionen información confidencial.

Compromiso del correo electrónico empresarial

Los ciberdelincuentes utilizan ingeniería social basada en correos electrónicos para defraudar a empresas haciéndose pasar por ejecutivos o empleados.

Deepfakes

Esto implica el uso de tecnología deepfake para imitar las voces o apariencias de ejecutivos, con frecuencia apuntando a empleados nuevos o con menos familiaridad con estos individuos.

Estas técnicas se han vuelto más sofisticadas con el uso de la IA y la tecnología deepfake, lo que dificulta cada vez más distinguir entre **comunicaciones genuinas** e **intentos fraudulentos.** El fraude de suplantación de identidad puede tener como objetivo a personas, empresas o incluso entidades gubernamentales, lo que con frecuencia provoca **pérdidas financieras significativas o filtraciones de datos.**

Quién:

Suplantación de ejecutivos

Los ejecutivos de alto nivel (C-suite), en particular los CEOs y CFOs, son los objetivos más comunes de los *deepfakes.*

Cómo:

Una historia creíble mediante un fraude multifactor y estructurado en múltiples niveles

Los estafadores utilizan tecnología *deepfake* para imitar las voces o apariencias de los ejecutivos, y con frecuencia emplean estos recursos para engañar a empleados de menor rango o menos familiarizados con dichos ejecutivos, manipulándolos para que eludan los controles.

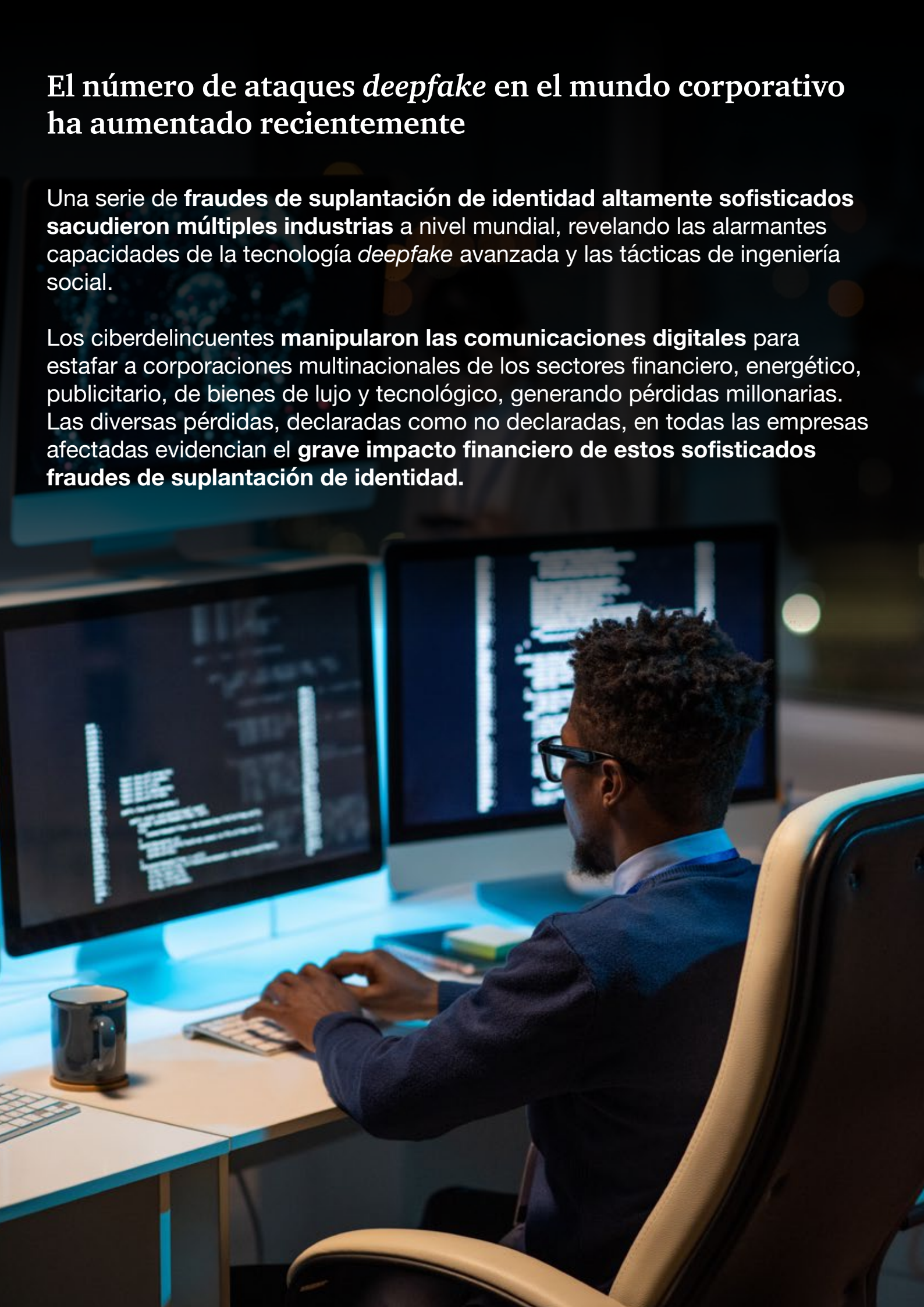
Los estafadores combinan *deepfakes* con técnicas tradicionales de phishing o ingeniería social. Por ejemplo:

- Los ataques dirigidos suelen comenzar mediante WhatsApp, antes de pasar a las videollamadas con tecnología *deepfake*.
- Las notas de voz o videollamadas falsas suelen ir acompañadas de correos electrónicos de phishing para simular un proceso de autenticación multifactor.
- Los estafadores aprovechan la falta de verificación cruzada durante las interacciones remotas, especialmente en reuniones virtuales y llamadas de voz.

El número de ataques *deepfake* en el mundo corporativo ha aumentado recientemente

Una serie de **fraudes de suplantación de identidad altamente sofisticados sacudieron múltiples industrias** a nivel mundial, revelando las alarmantes capacidades de la tecnología *deepfake* avanzada y las tácticas de ingeniería social.

Los ciberdelincuentes **manipularon las comunicaciones digitales** para estafar a corporaciones multinacionales de los sectores financiero, energético, publicitario, de bienes de lujo y tecnológico, generando pérdidas millonarias. Las diversas pérdidas, declaradas como no declaradas, en todas las empresas afectadas evidencian el **grave impacto financiero de estos sofisticados fraudes de suplantación de identidad.**



La estrategia de la estafa

01

Preparación y recopilación de información

Los estafadores recopilan meticulosamente información pública disponible sobre el CEO y el CFO locales de la empresa. Esto incluye videos de entrevistas, grabaciones de voz de llamadas anteriores y datos personales obtenidos de la página web de la empresa y de los perfiles en redes sociales de los altos ejecutivos.

02

Preparación tecnológica

Con los datos recopilados, los delincuentes emplean algoritmos avanzados de IA para crear videos *deepfake* convincentes y clones de voz del director ejecutivo. También desarrollan cuentas de correo electrónico y perfiles de mensajería falsos que imitan fielmente los del equipo ejecutivo.

03

Generación de confianza

Los estafadores envían un correo electrónico a un gerente de finanzas de nivel medio, aparentemente enviado por el asistente del CEO. El mensaje menciona un próximo proyecto confidencial y está vinculado superficialmente a eventos actuales dentro de la organización. Este primer contacto tiene como objetivo generar credibilidad sin levantar sospechas inmediatas y suele ir acompañado de una solicitud para firmar un acuerdo de confidencialidad. Durante los días siguientes, los estafadores intercambian varios correos electrónicos con el gerente de finanzas, proporcionando detalles creíbles sobre el supuesto proyecto y ganándose poco a poco su confianza. Los estafadores también pueden hacerse pasar por consultores reales o abogados externos de firmas reconocidas, lo cual aporta credibilidad adicional a la historia.

04

Clonación de voz

Una vez establecida la confianza, los estafadores organizan una llamada de voz entre el gerente financiero y el "director ejecutivo" usando su clon de voz generado por IA. Durante la llamada, el falso director ejecutivo habla sobre la urgencia de una adquisición altamente confidencial.

05

Engaño por videoconferencia

Los estafadores realizan una videollamada falsa, haciéndose pasar por el director ejecutivo y el director financiero, para discutir el acuerdo secreto y enfatizar la necesidad de no divulgar información.

06

Solicitud de transferencia de fondos

Con la confianza y la urgencia establecidas, los estafadores solicitan la transferencia de una suma significativa a una cuenta específica, aparentemente para asegurar el acuerdo de adquisición.

Vemos numerosos casos de *deepfake* donde los profesionales se preguntan cómo pudo ocurrir este fraude a pesar de todos los controles y salvaguardas existentes. La retrospectiva puede ser muy útil, pero lo cierto es que esto está sucediendo y **las organizaciones están teniendo que aprender a las malas.**

Naturalmente, los casos denunciados son solo la punta del iceberg. Hay casos no denunciados y casos en los que los estafadores no logran su objetivo gracias a la **solidez de los controles** o, aún más importante, a la **vigilancia del personal.**

Si usted es víctima de un fraude de suplantación de identidad, ¿qué debe hacer?

Debe actuar con rapidez. Las preguntas que una empresa debería plantearse en caso de ser víctima de un fraude de suplantación de identidad son:

¿Cómo obtuvo el estafador información confidencial que fue utilizada contra la empresa?

¿Estuvo alguien dentro de la empresa involucrado en el fraude?

¿Qué medidas de seguridad fallaron y cómo puede la empresa garantizar que este tipo de fraude no vuelva a ocurrir?

Pasos esenciales clave que debe tomar la gerencia en respuesta a un ataque

1. Respuesta inmediata

- Aislar el incidente tomando medidas para limitar su propagación e influencia.

2. Investigar y evaluar

- Evaluar el alcance y determinar la magnitud de la violación.
- Realizar una investigación forense/cibernética que incluya entrevistas, inteligencia corporativa, descubrimiento electrónico, análisis transaccional y cualquier otra medida apropiada.
- Analizar la naturaleza del ataque, identificar vulnerabilidades y sospechosos y comprender cómo se produjo la suplantación de identidad.
- Determinar el alcance de la violación, incluidos qué sistemas, datos y cuentas se han visto comprometidos.

3. Recuperación

- Rastrear dónde se transfirió el dinero y buscar opciones legales para su recuperación.
- Evaluar si se trata de un evento asegurado según su póliza de seguro.

4. Remediación:

- Limitar el daño, eliminar la amenaza y restablecer las operaciones normales.
- Configurar sistemas de monitoreo para detectar cualquier signo de actividad maliciosa residual.
- Mejorar los controles que puedan haber fallado o brindar capacitación a los miembros del equipo.
- Recuperar cualquier dato perdido o comprometido de las copias de seguridad.

¿Cómo puede defender su organización del fraude de suplantación de identidad?

Evaluación del riesgo de suplantación de identidad

- **Análisis e identificación de amenazas:** realizar un análisis exhaustivo de incidentes pasados, tendencias del sector y posibles actores de amenazas. Evaluar la probabilidad de intentos de suplantación de identidad mediante la revisión de puntos de acceso, canales de comunicación e interfaces de usuario que podrían ser explotados.
- **Evaluación de vulnerabilidad:** revisión exhaustiva de los sistemas, procesos y controles de su organización para identificar posibles debilidades.
- Realizar la debida diligencia de los datos **revisando la información disponible públicamente** sobre la gerencia clave y la empresa (en particular, datos de audio/voz).

Preparación y gestión de crisis de ciberseguridad

- **Los incidentes ocurren inevitablemente** y, si no se responde adecuadamente, conducen a una crisis con un impacto potencialmente devastador.
- **Preparación para la respuesta a incidentes:** revisar los procedimientos de su organización destinados a la respuesta a incidentes y la gestión de crisis, y realizar un ejercicio depreparación para practicar de forma segura.
- **Gestión de crisis, respuesta a incidentes y resiliencia:** activar los planes preparados, tomar el control del incidente para contener el daño y proceder a la erradicación de amenazas y volver a la normalidad de manera resiliente.

Capacitación y concienciación

- **Capacitación y talleres de concientización sobre tecnologías *deepfake:*** Estos pueden organizarse como parte de capacitaciones internas o conferencias.
- **Mayor concienciación:** esto debería informar a los empleados sobre la posibilidad de falsificar contenido multimedia. El objetivo es mejorar la seguridad organizacional, mitigar los riesgos de seguridad y aumentar la concienciación.
- **Prevención del fraude:** los empleados comprenden cómo se crean las *deepfakes* y aprenden a reconocerlas.

Descubra cómo podemos ayudar a su organización a defenderse contra el fraude de suplantación de identidad

Contáctenos

Alexander García
Socio
alexander.garcia@pwc.com

Juan Victor Nizama
Gerente senior
juan.nizama@pwc.com