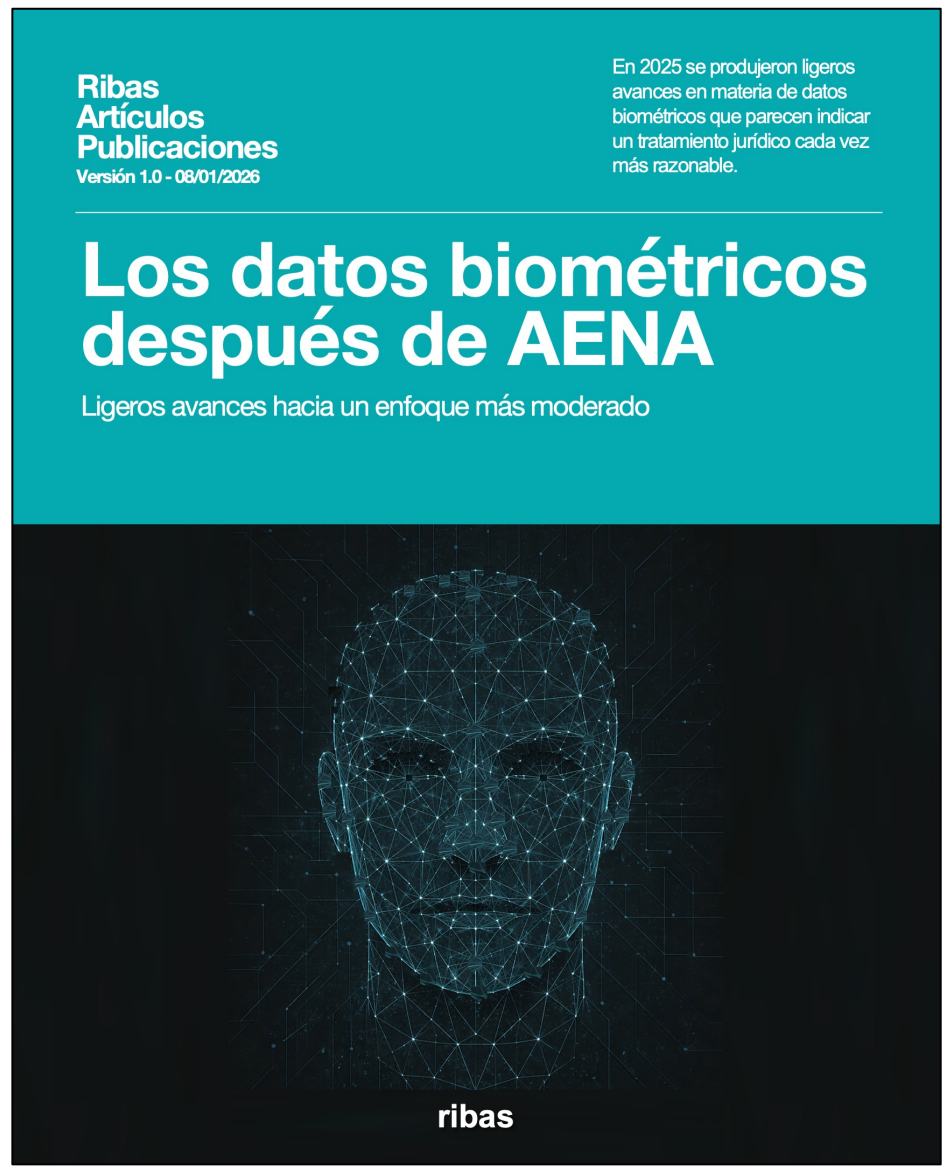
Casos de suplantación de identidad a partir de datos biométricos robados o expuestos

+1.000 millones de afectados vs. Cero denuncias

ribas

Informe completo



Accede al informe completo en este enlace:

https://lnkd.in/eE2MaMJX

ribas

Conclusión avanzada de este informe

La conclusión avanzada de este informe es que, a día de hoy, **no se ha encontrado una constancia documental, judicial ni técnica** de un caso de suplantación de identidad ejecutado con éxito mediante la reutilización de plantillas biométricas robadas a un responsable del tratamiento.

ribas

Brechas de datos biométricos más importantes

En esta tabla pueden verse los incidentes de seguridad más graves con afectación de datos biométricos y el contraste del carácter masivo del incidente con la ausencia total de quejas y denuncias por explotación de los datos y suplantación de identidad.

Las autoridades de control consideran la ausencia de quejas y denuncias como un indicador importante en la decisión de archivar la investigación de una brecha de seguridad, incluso en el caso de que los datos hayan sido publicados.

Caso	Datos comprometidos	Quejas o denuncias por suplantación de identidad
OPM (EE.UU., 2015)	5,6 millones de huellas dactilares	No constan
Biostar 2 (2019)	27,8 millones de patrones biométricos dactilares y faciales	No constan
Aadhaar (India, 2023-24)	815 millones de huellas dactilares	No constan Hubo fraudes cometidos con huellas clonadas de otros registros públicos, pero no directamente de este incidente.
Oracle Cloud (2025)	6 millones de registros con identificadores biométricos	No constan

Comparativa entre tres métodos de suplantación de identidad: riesgo percibido y riesgo real

En esta tabla pueden verse las diferencias entre tres métodos de suplantación de identidad. Puede apreciarse una gran discrepancia entre el riesgo percibido por el público en general y el riesgo real.

Característica	**Robo al responsable (Exfiltración BBDD)**	**Obtención en redes sociales (OSINT)**	**Ingeniería Social (Vishing/Phishing)**
Origen del dato	Responsable del tratamiento	Redes sociales	La víctima
Naturaleza del dato	Plantilla matemática (Hash / Vector).	Imagen / Video	Datos suministrados por la víctima.
Estado técnico	Dato "muerto” (requiere ingeniería inversa).	Dato "vivo" (listo para procesar con IA).	Dato "en tiempo real" (máxima calidad).
Tasa de suplantación	0% conocida. No hay denuncias.	Alta (~70%). Crecimiento exponencial.	Extrema (~95%). El usuario "da permiso".
Denuncias reales	0 por suplantación (solo por privacidad).	Miles de denuncias (Deepfakes).	Millones de denuncias (Estafas).
Tipo de suplantación	Inyección de datos	Presentación	Presentación
Dificultad	Alta	Baja	Media
Escalabilidad	Baja (Múltiples barreras)	Muy alta (Se puede automatizar)	Individual (Muy laboriosa).
Uso de IA	Gran dificultad (Minimización de datos)	Clave. Permite crear Deepfakes.	Auxiliar. Mejora guiones y voces.
Interoperabilidad	Nula. El código robado no sirve en otro sistema.	Total. Una foto sirve para cualquier app.	Total. La víctima actúa en el sistema real.
Coste del ataque	Muy alto (hackear infraestructura).	Muy bajo (herramientas de IA gratis).	Variable (tiempo y manipulación).
Barreras de seguridad	Cifrado y algoritmos propietarios.	Ninguna. Datos publicados en RRSS.	La psicología y confianza humana.
Riesgo percibido por los usuarios y el público en general	Riesgo alto debido al desconocimiento	Riesgo bajo debido al desconocimiento	Riesgo bajo debido al desconocimiento
Riesgo real	Muy bajo o inexistente	Muy alto	Muy alto

ribas

Dificultades de la suplantación a través del robo de datos

El proceso de suplantación de identidad basado en el robo y el uso de datos biométricos tiene las siguientes dificultades.

Barreras de acceso	1. Segmentación de red y separación de servidores. 2. Firewalls. 3. Autenticación y privilegios.
Barreras de salida	1. Sistemas DLP. 2. Servidores Proxy y filtros de salida. 3. Datos señuelo.
Barrera de la irreversibilidad	1. Hash o vector matemático. 2. Proceso unidireccional. 3. Es matemáticamente imposible reconstruir la cara.
Barrera de la incompatibilidad	1. Cada fabricante utiliza su propio algoritmo. 2. Los datos no son compatibles con otros sistemas.
Barrera de la prueba de vida	1. Los sistemas actuales no aceptan imágenes estáticas. 2. Los sensores buscan pruebas que demuestren que el usuario que desea autenticarse es un usuario vivo. 3. A partir del hash no pueden generarse pruebas de vida.
Barrera del cifrado	1. Para usar un dato robado se debe inyectar el hash. 2. Los sistemas actuales rechazan los ataques de inyección.
Barrera de la inyección de datos	1. Para usar un dato robado se debe inyectar el hash. 2. Los sistemas actuales rechazan los ataques de inyección
Barrera de la autenticación multifactor	1. El dato biométrico va asociado a otro factor. 2. No puede haber autenticación 1:1 sin el otro factor.
Barrera de la caducidad	1. El patrón biométrico puede ser cancelado o revocado. 2. En caso de robo se pueden invalidar todos los hashes.
Barrera de la minimización	1. Los patrones utilizan el mínimo número de datos. 2. El detalle del patrón sería insuficiente para una reversión.
Barrera de la relación riesgo / recompensa	1. El riesgo de robar los datos biométricos es muy alto. 2. La recompensa es baja ya que el patrón obtenido es inútil.

ribas

Facilidad de la suplantación a través de una foto de redes sociales

El proceso de suplantación de identidad basado en la obtención de los datos biométricos a través de una foto o un vídeo publicado en las redes sociales y utilizando IA para la suplantación es mucho más fácil.

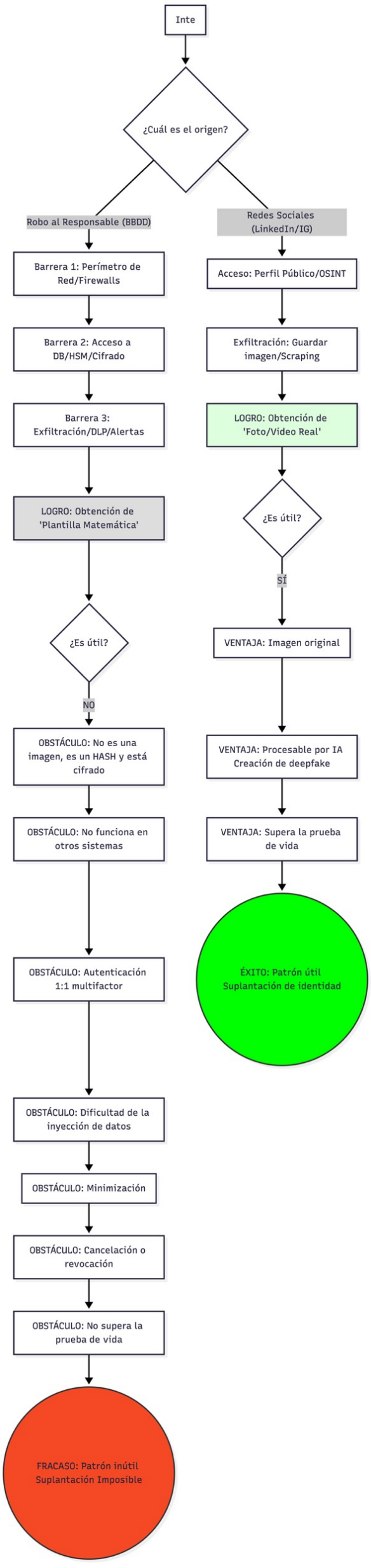
Barreras de acceso	1. No hay barreras de acceso. 2. Cualquier usuario puede acceder a una foto o un vídeo.
Barreras de salida	1. No hay barreras de salida. 2. Cualquier usuario puede descargar una foto o un vídeo.
Barrera de la irreversibilidad	1. Esta barrera no existe. 2. No hay hash.
Barrera de la incompatibilidad	1. Esta barrera no existe. 2. Los datos son totalmente compatibles.
Barrera de la prueba de vida	1. La muestra biométrica obtenida es suficiente. 2. La IA actuar puede simular pruebas de vida.
Barrera del cifrado	1. Esta barrera no existe. 2. Los datos no están cifrados.
Barrera de la inyección de datos	1. No es necesario inyectar datos. 2. Se trata de un ataque de presentación.
Barrera de la autenticación multifactor	1. El dato biométrico va asociado a otro factor. 2. No puede haber autenticación 1:1 sin el otro factor.
Barrera de la caducidad	1. Esta barrera no existe. 2. Los datos no pueden ser cancelados ni revocados.
Barrera de la minimización	1. Esta barrera no existe. 2. Los patrones utilizan el máximo número de datos.
Barrera de la relación riesgo / recompensa	1. El riesgo de la obtención de los datos es muy bajo. 2. La recompensa es alta ya que el patrón obtenido es útil.

Comparativa de barreras

En esta tabla se puede comprobar un contraste demoledor. Para el robo al responsable, el atacante debe ser un ingeniero experto enfrentándose a una fortaleza digital. Para la recolección en redes sociales, solo necesita ser un usuario medio con acceso a herramientas de IA comunes. Esto explica por qué las denuncias por suplantación desde redes sociales son masivas, mientras que desde bases de datos robadas son cero.

Barrera	Robo de datos biométricos	Obtención en redes sociales
Barrera de acceso	MUY ALTA	MUY BAJA
Barrera de salida	MUY ALTA	MUY BAJA
Barrera de la irreversibilidad	MUY ALTA	NO EXISTE
Barrera de la incompatibilidad	MUY ALTA	NO EXISTE
Barrera de la prueba de vida	MUY ALTA	BAJA
Barrera del cifrado	MUY ALTA	NO EXISTE
Barrera de la inyección de datos	MUY ALTA	NO ES NECESARIA
Barrera de la autenticación multifactor	ALTA	ALTA
Barrera de la caducidad	MUY ALTA	NO EXISTE
Barrera de la minimización	MUY ALTA	NO EXISTE
Barrera de la relación riesgo / recompensa	Riesgo muy alto Recompensa inexistente	Riesgo muy bajo Recompensa alta

ribas



Comparativa de procesos

En este diagrama de flujo pueden verse los obstáculos que un experto va a encontrar en el camino a la suplantación de identidad a partir del robo de datos biométricos al responsable del tratamiento.

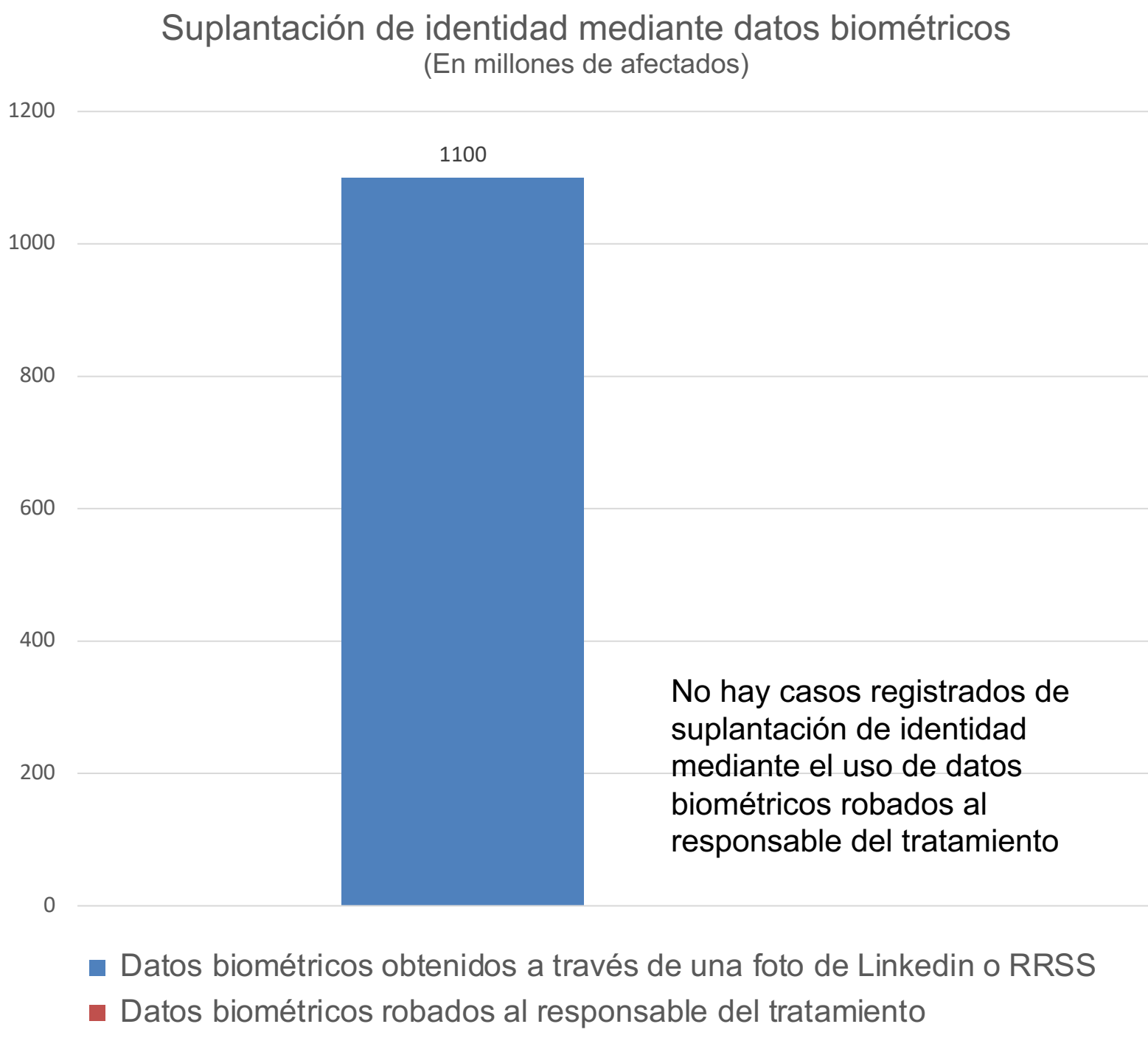
También puede verse el camino llano hacia el mismo objetivo a partir de la obtención de datos biométricos mediante una fotografía o un vídeo publicado por la víctima en LinkedIn o en una red social como Facebook o Instagram, utilizando herramientas gratuitas y sin necesidad de ser un experto.

Esto explica por qué las denuncias por suplantación desde redes sociales son masivas, mientras que desde bases de datos robadas son cero.

ribas

Casos de suplantación de identidad

En este gráfico puede verse que las estadísticas relativas a la suplantación de identidad mediante el uso de datos biométricos de la persona suplantada demuestran que el uso de datos robados es prácticamente inexistente.



ribas

Casos de suplantación de identidad a partir de datos biométricos robados o expuestos

La leyenda urbana en la que se sustentan los argumentos de las autoridades de control está basada en la creencia de que, si los datos biométricos que gestiona el responsable del tratamiento son robados o expuestos en una brecha de seguridad, el interesado podrá ser víctima de una suplantación de identidad. Según las estadísticas mundiales sobre la materia, esta creencia está infundada, ya que, de un total de más de 300 millones de personas afectadas por incidentes de seguridad relacionados con datos biométricos, ninguno de ellos ha presentado una queja o una denuncia.

Las autoridades de control consideran la ausencia de quejas y denuncias como un indicador importante en la decisión de archivar la investigación de una brecha de seguridad, incluso en el caso de que los datos hayan sido publicados.

Más de 1.000 millones de afectados
vs.
Cero denuncias

ribas

Casos de suplantación de identidad a partir de datos biométricos obtenidos a través de fotos de redes sociales

Los datos relativos a este tipo de suplantaciones son relevantes:

1. Crecimiento del 3.000% de los ataques con deepfakes.
2. El 71% de los usuarios no sabe identificar un deepfake biométrico.
3. 1,4 millones de denuncias en EEUU según la FTC en el periodo 2024 -2025

La disponibilidad de imágenes en fuentes abiertas y la facilidad de obtener datos biométricos a través de ellas genera actualmente un riesgo de suplantación mucho probable, fácil y perjudicial que el robo de bases de datos almacenadas en los sistemas del responsable del tratamiento.

Caso Arup - Ataque mediante deepfake de IA

Año	2024
Víctima	Filial en Hong Kong de Arup, empresa global de ingeniería con sede en Londres
Tipo de ataque	Suplantación de directivos mediante ataque de presentación con deepfake
Mecánica del ataque	1. Videollamada con deepfake en tiempo real que suplantaba al CFO. 2. En la videollamada participaban otros deepfake de directivos. 3. El empleado creyó estar viendo al director financiero y autorizó los pagos.
Datos biométricos	Sí, obtenidos a partir de las fotos y vídeos del director financiero y otros.
Uso de sistema de IA	Sí, para crear un deepfake en tiempo real a partir de los datos biométricos.
Resultado	15 transferencias que sumaron 25,6 millones de dólares
Origen de los datos	Fotos y vídeos de los directivos publicados en LinkedIn y en YouTube.
Dificultad del ataque	Muy baja: Herramientas de bajo coste + investigación en LinkedIn.

Otros casos de obtención de datos biométricos a través de fotos de redes sociales

En esta tabla se resumen casos similares de obtención de datos biométricos a través de fotos publicadas en redes sociales.

Caso	Metodología	Resultados
Clearview AI	Scraping masivo de imágenes en redes sociales.	Obtención de más de 30.000 millones de imágenes de redes sociales (LinkedIn, Facebook, Instagram) para entrenar algoritmos de reconocimiento facial.
KnowBe4	El atacante utilizó fotos de alta calidad de una persona real encontradas en redes profesionales para construir su avatar digital clonado.	Una empresa de ciberseguridad contrató al avatar clonado por el atacante que usó una el deepfake en tiempo real durante la entrevista.
Caso Ana	Los atacantes utilizaron fotos frontales de sus perfiles públicos para superar las verificaciones biométricas sencillas de las operadoras (que solo pedían una foto estática o un parpadeo).	Suplantación de la identidad para contratar 11 líneas telefónicas con las que se realizaron múltiples estafas.

Estadísticas sobre suplantación de identidad

En esta tabla se hace una breve referencia a los datos estadísticos disponibles para el periodo 2024 - 2025. En ninguno de ellos se han utilizado patrones biométricos robados al responsable del tratamiento.

Metodología	Datos y denuncias
Deepfakes biométricos	Según Identity Fraud Report de 2025, los intentos de suplantación mediante deepfakes biométricos creados a partir de fotos y vídeos publicados en redes sociales ocurren a un ritmo de uno cada cinco minutos a nivel global.
Fotos de redes sociales DNI escaneados en falsas ofertas de empleo	Según INCIBE, en 2024 se registraron 7.712 denuncias específicas de suplantación de identidad solo en el sector del juego online (Protocolo PACS). La mayoría de estas víctimas denunciaron que sus fotos de redes sociales o DNI escaneados en falsas ofertas de empleo fueron usados para crear cuentas.
	El INCIBE reportó que un 14% de los internautas españoles sufrió algún tipo de suplantación de identidad digital en el último año, siendo la duplicación de perfil con fines fraudulentos, usando fotos de Instagram/LinkedIn la modalidad más denunciada.
	El reporte de Veriff 2025 indica que 1 de cada 20 intentos de verificación de identidad en el sector financiero ya es fraudulento, y el 40% de esos fraudes son ataques de presentación, mediante fotos o vídeos obtenidos de redes sociales.
	1.4 millones de denuncias en EE.UU según la FTC relacionados con la suplantación de identidad con datos biométricos obtenidos a través de las fotos y los vídeo publicados en las redes sociales.

Tasa de éxito

En la siguiente tabla puede verse una comparativa de la tasa de éxito de cada modalidad de ataque de obtención de datos y suplantación de identidad:

Metodología	Tasa de éxito estimada	Razón del éxito o el fracaso
Robo de datos biométricos al responsable del tratamiento.	Baja o inexistente	Las plantillas robadas suelen estar en formatos propietarios o hashes que no pueden reinyectarse fácilmente en otros sistemas.
Obtención de datos biométricos a través de fotos obtenidas en redes sociales.	Muy alta	Las fotos y videos descargados permiten crear deepfakes. En 2025, 1 de cada 20 rechazos en la verificación de identidad bancaria fue un deepfake realizado con IA.
Obtención de datos biométricos a través de videoconferencias.	Muy alta	La obtención de datos biométricos a través de videoconferencias permite crear avatares muy precisos.

Ataque de inyección vs. ataque de presentación

No se han localizado evidencias de que un ataque de inyección de plantilla biométrica robada haya prosperado y haya escalado a un fraude masivo, mientras que los ataques de presentación de deepfake a partir de datos obtenidos en redes sociales causaron pérdidas millonarias documentadas en 2024 y 2025.

En esta tabla se pueden ver las diferencias entre ambos tipos de ataque.

Ataque de Inyección A partir del robo de datos biométricos al responsable del tratamiento	El atacante intenta introducir el código binario robado directamente en el flujo de datos del sistema. Es mucho más difícil que el ataque de presentación porque requiere una manipulación experta de la aplicación de destino, no solo tener el dato biométrico. Además, hay que superar un gran número de barreras técnicas, como hemos visto.	No se han reportado casos
Ataque de Presentación A partir de la obtención de los datos biométricos a través de fotos obtenidas en redes sociales	El atacante utiliza una foto de LinkedIn o de otras redes sociales, la anima con IA y la pone frente a la cámara del móvil. Es el método más común en los fraudes actuales.	Ha sido la técnica más utilizada y más letal en 2024 y 2025. Existen miles de casos documentados, además de los grandes casos corporativos comentados.

Obtención de datos biométricos en entrevistas laborales falsas

La trampa biométrica basada en una entrevista laboral falsa es un método muy eficaz, que ha generado muchas denuncias en 2025. En este caso el atacante captura de forma directa los datos biométricos de la víctima.

La mecánica es la siguiente:

1. El atacante crea una falsa oferta de empleo en LinkedIn.
2. Durante la entrevista por videoconferencia, el atacante pide al usuario que realice movimientos faciales o escanee su DNI para validar su perfil.
3. Con esos datos vivos capturados directamente de la víctima y no robados de un servidor, el atacante abre cuentas bancarias o pide préstamos.

Los casos de suplantación reportados a causa de esta técnica son menos numerosos que los relacionados con la obtención de datos biométricos a través de fotos y vídeos publicados en redes sociales, como puede verse en esta tabla.

Origen de los datos biométricos	Casos de suplantación reportados
Robo de los datos biométricos al responsable del tratamiento.	0
Obtención de datos biométricos a través de fotos y vídeos publicados en redes sociales.	Miles - Crecimiento del 3.000%
Entrevistas laborales falsas.	Más de 35

Irreversibilidad

En la resolución de la AEPD en el caso de AENA se menciona el riesgo de reversión no autorizada de los datos biométricos que permita la reidentificación del interesado aparece como un atributo que AENA considera acreditado y propio de la inmensa mayoría de los sistemas biométricos del mercado.

La capacidad de los sistemas biométricos de evitar la reversión de los datos biométricos y la reidentificación del interesado no es una materia controvertida en la resolución.

Los responsables del tratamiento no guardan imágenes de la huella dactilar o de la cara, sino representaciones matemáticas. Reconstruir una cara física a partir de un código binario robado es actualmente una imposibilidad técnica para la mayoría de los sistemas comerciales.

Cifrado

En conexión con la prevención del riesgo de reversión y reidentificación en la resolución de la AEPD en el caso de AENA en la EIPD también se considera acreditado la existencia del cifrado.

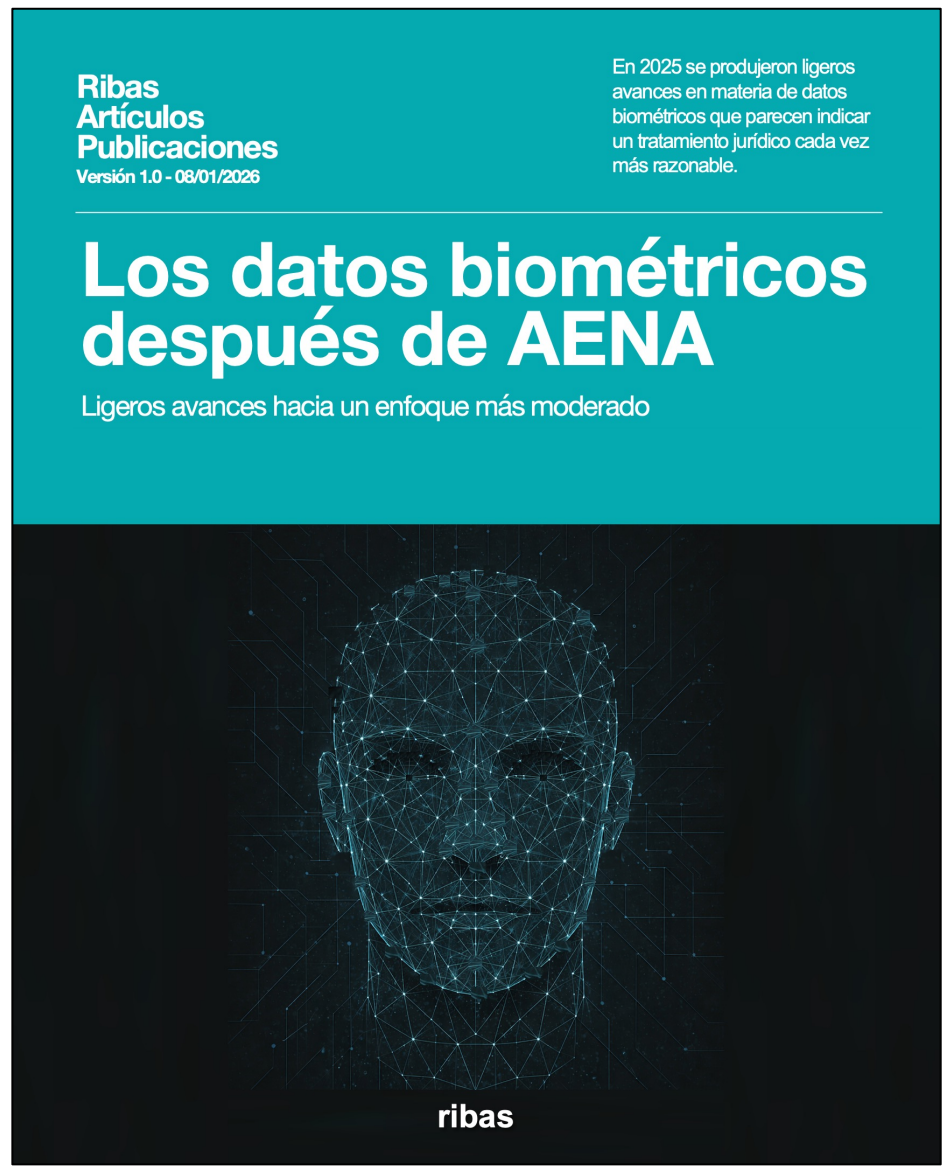
La existencia y la idoneidad del cifrado no es una materia controvertida en la resolución.

Incompatibilidad

Cada fabricante utiliza un algoritmo propietario y una configuración de hash diferente para cada cliente, por o que un patrón biométrico robado de la base de datos de una empresa no sirve para entrar en el sistema de otra empresa.

ribas

Informe completo



Accede al informe completo en este enlace:

https://lnkd.in/eE2MaMJX

ribas

Datos de contacto

Nombre del despacho	Ribas
Domicilio	Diagonal 640 1C - 08017 Barcelona
Persona de contacto	Xavier Ribas
Correo electrónico	xavier.ribas@ribastic.com
Teléfono fijo	934940748
Teléfono móvil	639108413
LinkedIn	https://www.linkedin.com/in/javierribas/
Web	http://ribas.legal
Blog	http://xribas.com

ribas