

SEMANA DE LA ADMINISTRACIÓN ABIERTA

DEEPFAKES Y FRAUDES BASADOS EN INTELIGENCIA ARTIFICIAL



MAYO 2026



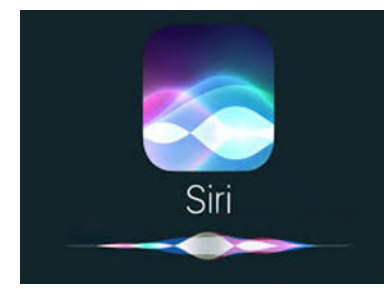
BANCO DE ESPAÑA
Eurosistema

1

Introducción a la IA

Inteligencia artificial generativa.

IA GENERATIVA: UNA BREVE INTRODUCCIÓN



LA IMPORTANCIA DE ELEGIR BIEN

Aplicaciones positivas

- Protección contra fraudes.
- Detección de patrones sospechosos.
- Análisis de comportamiento para la detección del fraude.

Desafíos éticos

- Privacidad.
- Acceso a grandes cantidades de datos.
- Gran sofisticación.
- ¿Cuándo confiar?

Aplicaciones negativas

- Phishing avanzado y automatizado.
- Deepfakes.
- Suplantaciones de identidad (por vídeo, por voz, etc.).

2

Fraudes basados en IA

Un cambio en la calidad de los engaños digitales.

Según el canal utilizado



Phishing
Correo
Electrónico



Smishing
SMS y Mensajería
Instantánea



Vishing
Llamada
telefónica



Angle Phishing
Redes
Sociales



QRishing
QR

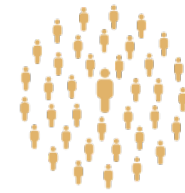


Pharming
Web

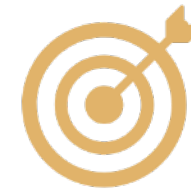


Evil Twin Phishing
Redes WIFI

Según el objetivo



Phishing masivo
Impersonal



Spear phishing
Dirigido a
una persona



Whaling
Dirigidos a ejecutivos
de alto nivel

S Soporte

Para [redacted].es

NETFLIX - Actualiza tu cuenta para volver a ver

N

Actualiza tu cuenta para volver a ver

Hola,

Tenemos problemas con tu información de facturación actual.Quieres volver a intentar procesar tu tarjeta La información de tu tarjeta se encuentra a continuación.

Reintentar pago

Introduzca un nuevo método de pago

Estamos aquí para ayudarte si lo necesitas. Visita el [Centro de ayuda](#) para obtener más información o [contáctanos](#).

El equipo de Netflix

N Preguntas? Llama al 0800-000-7969
Servicios de Netflix Alemania GmbH

Configuración de comunicación

La entrega se ha suspendido porque su pedido no tiene numero de casa. Se requiere firma. Gestione su entrega:

[https://www.netflix.com/...](#)



LIDL
LIDL
raz...r.shop

Mira lo que he compartido:
LIDL @Navegador Mi | <https://raz...r.shop/>

20:05

19/01/2026 10:29:18

Agencia Tributaria
Sede electrónica

ÁREA PERSONAL

Identificación

Escriba su contraseña de correo electrónico.

Entrar

¿Tienes dudas? visita la [ayuda de identificación electrónica](#)

Paquete n.º: 331667437

Tras un problema en el primer intento de entrega, su paquete será reenviado desde nuestro almacén. Es necesario un método de pago válido para abonar los gastos de reenvío, por un importe de 0,99 €.

PAID CARD VISA

Preautorización: 0,99€

Número de tarjeta

MM/AA

CVV

Los gastos solo se cobrarán una vez que se confirme la entrega exitosa de su paquete.

Confirmar mi método de pago

Este sitio es completamente seguro

miércoles, 16 de abril de 2025

Hola mama, mi telefono se ha roto, este es mi nuevo numero, enviame un mensaje por Whats App en cuanto puedas

11:08

¿QUÉ SON LOS “DEEPPFAKES”?

Vídeos, imágenes o audios
creados o modificados con
Inteligencia Artificial

USOS ÉTICOS:



- ✓ **Medicina y accesibilidad**
- ✓ **Entretenimiento y cine**
- ✓ **Educación y cultura**



¿QUÉ SON LOS “DEEPPFAKES”?

USOS FRAUDULENTOS:



- Suplantación de identidades, ciberacoso
- Manipulación de opiniones y desinformación
- Estafas de ingeniería social

8M

deepfakes en 2025

+3000%

fraudes en 2023

\$500k

pérdida media por incidente

24,5%

tasa de detección humana

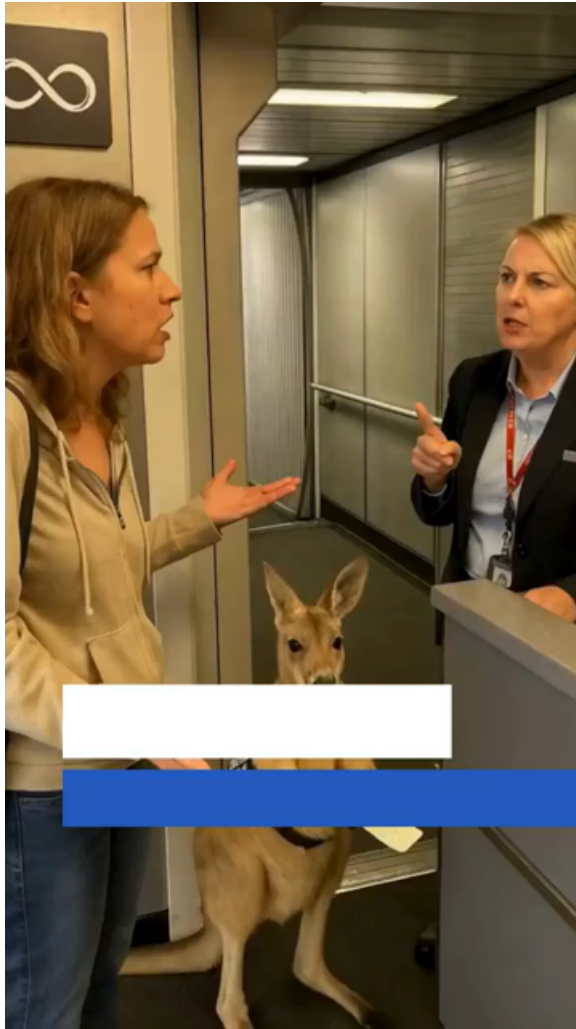


3

Esto ya no es ciencia ficción

Un acercamiento a las técnicas utilizadas.





VerificaRTVE



PROBLEMA DE CIBERSEGURIDAD

Estafa con 'deepfakes': 24 millones de euros y una reunión virtual con solo una persona real

- Una videoconferencia entre un empleado y varios ejecutivos de una multinacional británica resultó ser una estafa que ha supuesto pérdidas millonarias para la empresa

CIBERSEGURIDAD >

Los usos criminales de los 'deepfakes' se disparan: estafas, pornografía y suplantación de identidad

Los expertos y las compañías de ciberseguridad advierten de que esta tecnología ahora es capaz de engañar a algunos métodos de autenticación biométrica o crear perfiles de trabajadores falsos que postulan a puestos reales

Los padres de un menor sancionados por la difusión de imágenes falsas de chicas desnudas generadas con IA en Almendralejo

La multa, de 2.000 euros, se impone por la implicación de su hijo en la creación y difusión de imágenes manipuladas con inteligencia artificial que afectaron a varias adolescentes de la localidad pacense

Crece denuncias de suplantación y no tienes que ser CEO o influencer para ser víctima

Se eleva uso de inteligencia artificial, y ahora hay históricas sentencias por este delito en TikTok y Facebook

Recuerda:

1. No uses la imagen de otras personas con la IA sin su consentimiento.
2. No hagas nada que no te gustaría que te pasase.
3. Piensa en las consecuencias: repercusiones legales y daños psicológicos.

El Gobierno aprueba una nueva Ley del derecho al honor más garantista y adaptada al entorno digital

13.1.2026

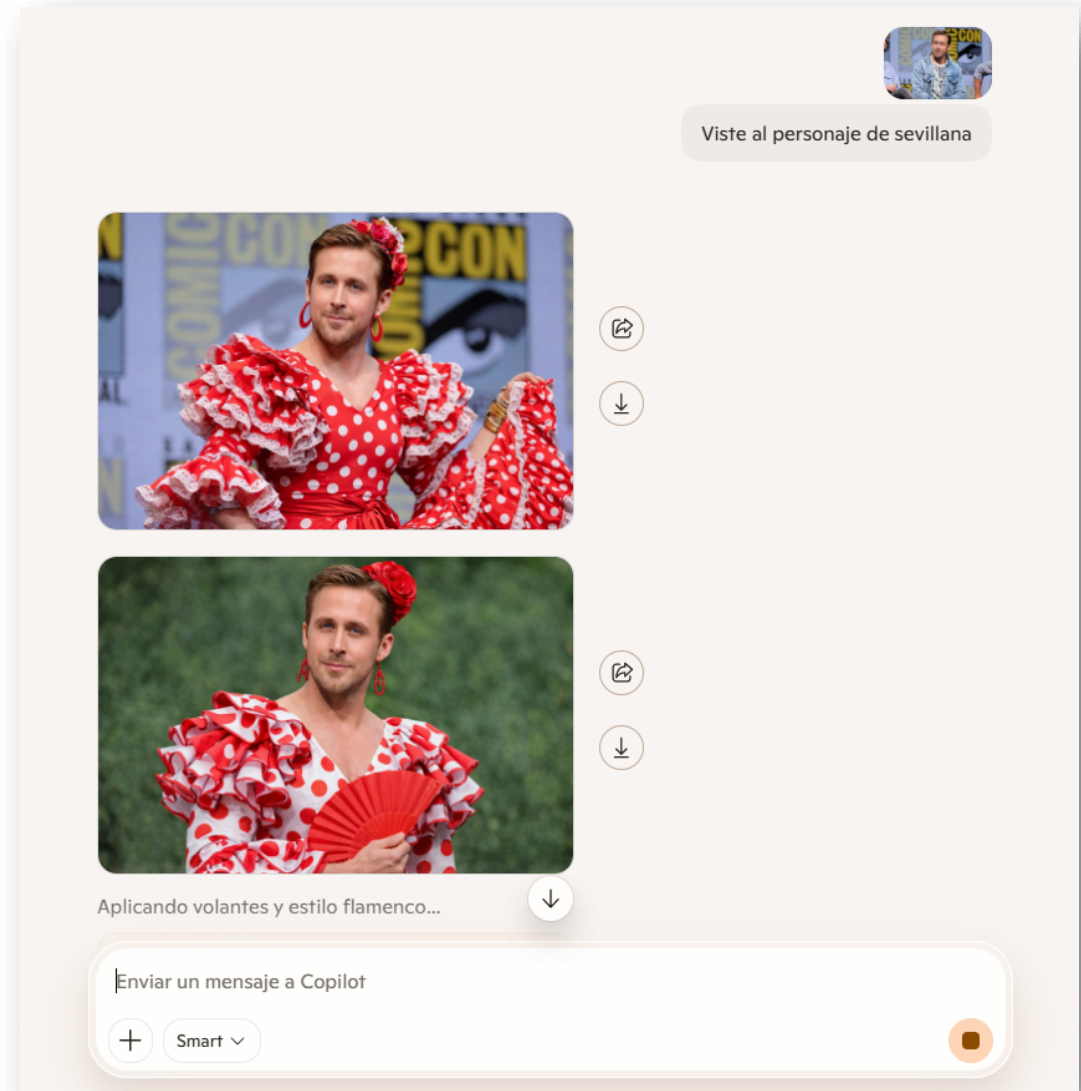
El Gobierno aprueba tipificar como delito los deepfakes de contenido sexual y el grooming



La Unión Europea acuerda la propuesta de España de prohibir los 'deepfakes' sexuales

[Transformación Digital y Función Pública - 7.5.2026](#)

Crear o difundir imágenes íntimas generadas por IA sin consentimiento no es una broma tecnológica. **Es un delito.**



FaceFusion 3.0.1

join our community

PROCESSORS

- face_swapper
- age_modifier
- expression_restorer
- face_debugger
- face_editor
- face_enhancer
- frame_colorizer
- frame_enhancer
- lip_syncer

FACE SWAPPER MODEL

inswapper_128_fp16

FACE SWAPPER PIXEL BOOST

128x128

EXECUTION PROVIDERS

- cpu
- cuda
- tensorrt

EXECUTION THREAD COUNT 32

WEBCAM

Iriun Webcam v2.8.9

OPPO CPH2639 [USB]

Video format 640 x 360

視訊的另一頭的聲音、影像都可以即時換臉、換聲
所以要小心這類的詐騙喔!



4

DEEPVOICE

Caso práctico y sus repercusiones.

BENEFICIOS DE LA CLONACIÓN DE VOZ

- **Accesibilidad**
- **Industria del entretenimiento (cine, videojuegos...)**
- **Asistentes virtuales**
- **Audiolibros**
- **Doblaje y traducción**
- **Detección del fraude**



Una **Inteligencia Artificial** que **permite hablar** a quien no tiene voz, que dinamiza la industria del **entretenimiento** y que sirve para detectar **fraudes**.

USO FRAUDULENTO DE LA CLONACIÓN DE VOZ

- **Fraudes y estafas**
- **Manipulación de la información**
- **Vulneración de la seguridad**
- **Pruebas falsas**
- **Falsos consentimientos**
- **Consecuencias psicológicas**



DIY: HAZLO TÚ MISMO



LAS TRES FASES DE LA CLONACIÓN DE VOZ

1. **Recolección de datos:** grabación de la voz original.
2. **Entrenamiento del modelo:** pronunciación, estilo.
3. **Creación de voz:** nuevas frases.

El deep learning utiliza redes neuronales para aprender y reconocer patrones en grandes conjuntos de datos.

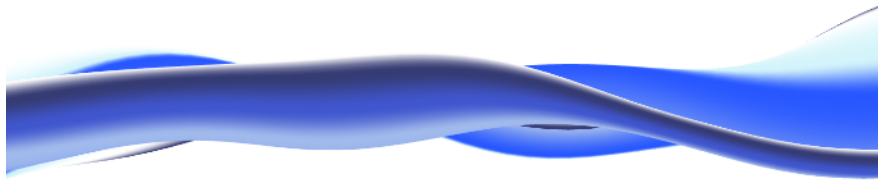


MÉTODOS DISPONIBLES

Create the most realistic speech with our AI audio platform

Pioneering research in Text to Speech, AI Voice Generator, and more

GET STARTED FREE TRY A SAMPLE



The All-in-One AI Voice Platform

Resemble AI delivers a cutting-edge AI Voice Generator and robust Deepfake Audio Detection, engineered for enterprises prioritizing advanced security and safety.

Create AI Voices Explore Deepfake Detection

Products Use Cases Resources Pricing AI Voice Agents **NEW** API Log in Try for Free

AI VOICE GENERATOR: MOST REALISTIC TEXT TO SPEECH AI

Generate AI voices, Indistinguishable from Humans

Ultra realistic Text to Speech(TTS) voice. Leading AI Voice Generator. Free Unlimited downloads. Most Fluent & Conversational AI voices

Product Solutions Resources Open Source Enterprise Pricing

Corentini / Real-Time-Voice-Cloning Public

Code Issues 192 Pull requests 17 Actions Wild Security Insights

1 member 1 Branch 0 Tags

Commit	Message	Time
encoder	Major maintenance update (#961)	2 years ago
samples	Added no_max_support argument and added a check for ...	4 years ago
synthesizer	Major maintenance update (#961)	2 years ago
text2speech	Major maintenance update (#961)	3 years ago
utils	New link for synthesizer download (#1030)	2 years ago
vocoder	Major maintenance update (#961)	2 years ago

CereProc by capcity Productos & Servicios Tienda Casos De Éxito Conócenos Nuestro Equipo Empleo Blog Contacto

Welcome to CereProc text-to-speech

CereProc create expressive voices with real character

VOICE DEMO

Explore the most natural and diverse text-to-speech voices on the market!

Bienvenido a la demo CereVoice, introduzca su texto aquí y pulse 'Play'.

spanish Aina (Slovakia, Mexico)

PLAY BUY

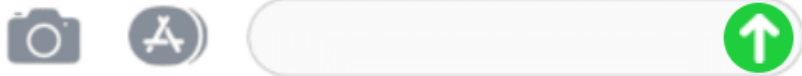
Find your voice

Readme View license Activity \$2.4k stars 938 watching 8.8k forks

Departamento IT 09:16
Buenos días. Su cuenta aparece en el sistema como el origen de un ciberincidente. Su conexión puede verse afectada, le mandamos las instrucciones por audio para seguirlas paso a paso.

Hola, soy el responsable de la unidad. Necesito que envíes una documentación lo antes posible, te mando la información en un audio.

Chat Screenshot by pranx.com



ElevenLabs

- ElevenCreative
- Home
- Voices
- Studio
- Flows
- Templates
- Files
- Pinned
- Text to Speech
- Sound Effects
- Image & Video
- Voice Isolator
- Voice Changer
- Music
- Speech to Text
- More tools

Voices

Explore My Voices

+ Create Voice

Search library voices... Filters

Language Accent Conversational Narration Characters Social Media Educational Advertisement

Default voices have been moved to My Voices and will be deprecated by the end of the year.

Trending voices

- Miguel - Deep, Rich and Cinematic**
Entertainment
Spanish +15
- Arconte - Evocative, Deep and Elegant**
Narration
Spanish
- Cristina Campos - Natural Conversa...**
Conversational
Spanish
- Sandra - Dynamic, Engaging and En...**
Social Media
Spanish +11
- David Martin - Confident and Balanc...**
Narration
Spanish +19
- Raquel - Young, Bright and Cheerful**
Conversational
Spanish

Handpicked for your use case

- V3** Best voices for Eleven v3
- Popular Tiktok voices**
- Studio-Quality Conversational Voices**
- Engaging Characters for Video Games**

Invite team members
Bring your team in to collaborate and share your creations.

Developers

5

CONCLUSIONES

IA: Una frontera ética.

USA LA IA DE FORMA SEGURA

Cuida tu privacidad y evita el uso de información personal:

- Limita quién puede ver tus vídeos, fotos o audios en redes sociales.
- Evita facilitar esta información en aplicaciones de IA generativa.

Analiza los contenidos que consumes:

- Verifica su veracidad a través de aplicaciones y fuentes externas.
- Busca errores en los contenidos, como parpadeos, manos y gestos extraños.
- Verifica la identidad de las personas a través de otras vías si te interpelan personalmente.

Desconfía de contenidos extraños o alarmantes:

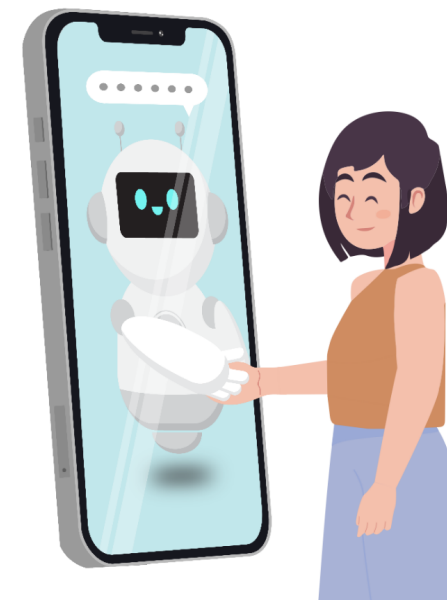
- Vídeos, imágenes y audios sensacionalistas.
- Mensajes demasiado buenos para ser verdad o que apelen a las emociones.

Mantente alerta ante la ingeniería social:

- Desconfía por defecto de peticiones inusuales o de desconocidos.
- Reporta cualquier anomalía o sospecha de suplantación de identidad.

Reporta el contenido fraudulento generado con IA:

- Cuando usen tu imagen o la de una persona conocida de tu entorno.
- Usa los métodos de reporte a través de los mecanismos de las redes sociales.
- Busca ayuda en organismos como INCIBE o la AEPD.
- Denuncia los delitos a las Fuerzas y Cuerpos de Seguridad del Estado.



¿CÓMO PODEMOS RECONOCER UN FRAUDE CON IA?



- ¿Suena igual que siempre?
- ¿Hay demasiadas pausas?
- ¿Notas cambios de tono?
- ¿Hay fallos en la imagen?
- ¿Cuántos dedos tienen las manos?
- ¿Tiene expresiones faciales extrañas?
- ¿Es correcta la sincronización?
- ¿Aparecen fallos en el fondo?

RECUERDA: también minimizamos riesgos evitando mensajes inusuales y **comprobando siempre la información.**

PASOS A SEGUIR PARA DETECTAR VÍDEOS CON IA



1. Localiza el origen de la publicación.
2. Amplía la información con fuentes externas.
3. Analiza el vídeo y el audio con detenimiento.
4. Comprueba los metadatos.
5. Utiliza los detectores de contenidos generados con IA.

Herramientas útiles para identificar contenido falso generado por IA ↻

Para complementar los consejos facilitados anteriormente, es esencial emplear técnicas prácticas que permitan una verificación más profunda y técnica del contenido. A continuación, se describen algunas herramientas que pueden servir de ayuda:

1. **Detectores de IA para texto:** Existen varias herramientas diseñadas para analizar textos y detectar si han sido generados artificialmente. Mostramos algunos ejemplos:
 1. **plagiarismdetector:** analiza patrones lingüísticos y estructuras gramaticales para indicar un tanto por ciento de posibilidades de que sea generado artificialmente.
 2. **GPTZero:** tiene la capacidad de detectar contenido generado por modelos como ChatGPT y GPT-4. Muestra los porcentajes de probabilidad de autoría humana o IA, y resalta las secciones sospechosas.
 3. **Copyleaks:** proporciona un análisis detallado a nivel de oración para detectar contenido generado por IA con una alta precisión.
2. **Herramientas de detección de multimedia:** Para detectar *deepfakes* y otros tipos de contenido multimedia generado por IA, estas herramientas pueden ser muy útiles:
 1. **VerifAI,** una web respaldada por la empresa Telefónica que detecta en pocos segundos si un contenido ha sido generado o alterado con IA.
 2. **Resemble Detect** detecta audios generados con IA.
 3. **Deepware:** permite analizar vídeos y detectar deepfakes mediante un análisis exhaustivo que identifica alteraciones y anomalías.
 4. **Illuminarty:** proporciona análisis avanzado para detectar deepfakes en imágenes, utilizando inteligencia artificial para identificar discrepancias y manipulaciones.
 5. **AI or Not:** permite a los usuarios cargar imágenes y audios para verificar si han sido manipulados o generados por inteligencia artificial.
 6. **VerificAudio:** ayuda a verificar, enviando a un equipo especializado, voces sintéticas.

REPORTA EL CONTENIDO EN REDES SOCIALES

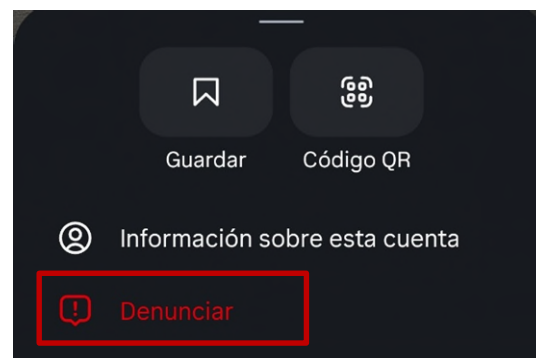
facebook

(En los tres puntos)

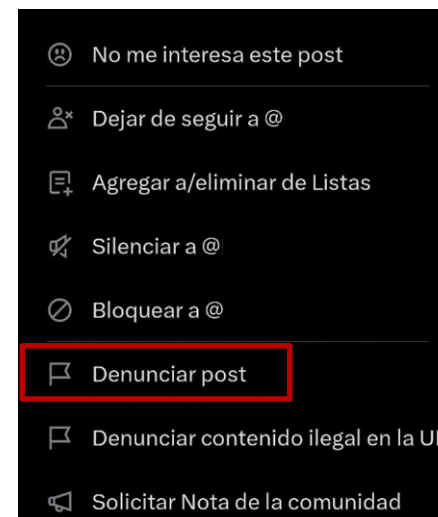


Instagram

(En los tres puntos)



(En los tres puntos)



TikTok

(Dejando pulsado)



CONTACTA CON EL INCIBE (INSTITUTO NACIONAL DE CIBERSEGURIDAD)

Servicio gratuito y confidencial, disponible de 08:00 am a 11:00 pm los 365 días del año.



TU AYUDA EN CIBERSEGURIDAD



Teléfono 017



WhatsApp 900 116 117



Telegram @INCIBE017



Formulario web



Atención presencial



CONTACTA CON LA AEPD (AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS)



Formularios de solicitudes para el ejercicio de los derechos

- [Formulario de solicitud para el ejercicio del derecho de acceso](#)
- [Formulario de solicitud para el ejercicio del derecho de rectificación](#)
- [Formulario de solicitud para el ejercicio del derecho de oposición](#)
- [Formulario de solicitud para el ejercicio del derecho de supresión](#)
- [Formulario de solicitud para el ejercicio del derecho a la limitación del tratamiento](#)
- [Formulario de solicitud para el ejercicio del derecho a la portabilidad de los datos](#)

DENUNCIA EL CASO A LAS FUERZAS Y CUERPOS DE SEGURIDAD DEL ESTADO

Policía Nacional



Brigada de Investigación Tecnológica de la Unidad de Investigación Tecnológica (UIT) de la Policía

Guardia Civil



Grupo de Delitos Telemáticos (GDT) de la Guardia Civil

Ertzaintza



Sección Central de Delitos en Tecnologías de la Información (SCDTI) de la Ertzaintza

Mossos d'Esquadra



Unidad Central de Delitos Informáticos de los Mossos d'Esquadra

Policía Foral



Grupo de Apoyo Tecnológico de la Policía Foral de Navarra

Muchas gracias por su atención