



GUÍA BREVE · RIESGO · FRAUDE DE IDENTIDAD

¿Cliente nuevo, identidad falsa?

Señales comprobadas antes de comprometerse.

Quien se da de alta o solicita un contrato empieza afirmando quién es. Esta guía breve muestra cómo PaperOffice entrega la dirección de correo, la dirección IP, el dispositivo y el documento de identidad como señales que usted puede comprobar. Para tiendas, plataformas, arrendadores y comercios que venden a plazos.

LO ESENCIAL

Cada comprobación devuelve campos en los que su regla puede basarse: una recomendación para el correo, indicadores para VPN y Tor, un ID de dispositivo y campos del documento de identidad con su ubicación de origen. Su equipo toma la decisión.

01 · EL PROBLEMA

El nombre es correcto. La persona que hay detrás no lo es.

Un cliente nuevo firma online un contrato y el smartphone se paga a plazos. Nombre, dirección y correo electrónico parecen auténticos. Solo cuando dejan de llegar los pagos queda claro: los datos pertenecen a otra persona, o la persona no existe.

POR QUÉ OCURRE

Datos robados e inventados

Los defraudadores usan nombres y direcciones reales de filtraciones de datos o los mezclan con datos inventados. En el formulario, ambos parecen iguales.

Ocultarse en la red

Las direcciones desechables, las VPN, Tor y los servidores alquilados ocultan quién hace el pedido. La misma persona puede abrir muchas cuentas con poco esfuerzo.

Documentos de identidad con prisas

En el mostrador, la copia del documento de identidad se mira por encima y se transcribe. Una errata o un campo que falta pasan fácilmente desapercibidos.

CÓMO SE NOTA

- La dirección de correo procede de un servicio desechable, o su dominio no tiene servidor de correo.
- El alta llega por VPN, Tor o un centro de datos en lugar de una conexión habitual.
- El país de la dirección IP no coincide con la dirección indicada.
- El mismo dispositivo aparece en varios altas con nombres distintos.
- Los datos del formulario y los del documento de identidad no coinciden.

02 · LA SOLUCIÓN CON PAPEROFFICE

De la señal a la decisión.

PaperOffice entrega señales sobre correo, red, dispositivo y documento, mediante la API REST, el SDK y en la aplicación. Lo que sigue depende de su regla: dejar pasar, volver a preguntar, enviar a revisión o rechazar.

1

Evalúe la dirección de correo

POST /fakeemail/check comprueba los dominios desechables, los registros MX, SPF y DMARC y devuelve risk_score más la recomendación ACCEPT, REVIEW o REJECT.

MÓDULO: [DETECCIÓN DE CORREOS ELECTRÓNICOS FALSOS](#)

2

Compruebe la red y la ubicación

/ip2location/full devuelve país, región y proveedor, además de is_vpn, is_proxy, is_tor e is_datacenter. El campo type indica la lista en la que se encontró coincidencia.

MÓDULO: [DETECCIÓN DE VPN](#)

3

Reconozca el dispositivo

El SDK del navegador devuelve un visitor_id por dispositivo. En el siguiente inicio de sesión, /fingerprint/verify comprueba si es el mismo dispositivo, y risk.factors indica cualquier anomalía.

MÓDULO: [HUELLA DIGITAL DEL DISPOSITIVO](#)

4

Lea el documento de identidad

Un IDP Agent lee nombre, fecha de nacimiento, dirección, número de documento y fecha de caducidad de una foto o un escaneo, con cada valor y su ubicación en el original.

MÓDULO: [IDP AGENT](#)

5

Decida

Su aplicación combina los campos en una regla, por ejemplo: una dirección desechable o Tor significa revisión por una persona. Su equipo toma la decisión.

03 · EN LA APLICACIÓN

Claves, SDK, agente: cómo configurarlo.

Las comprobaciones de señales se ejecutan mediante la API REST y el SDK; el documento de identidad, mediante un IDP Agent en la aplicación. Los nombres coinciden con la aplicación.

1

Una clave API para su backend

En **API y Desarrollador > Claves API**, use **Crear nueva clave** para crear una **Clave API**. Su backend la usa para comprobar correo y IP. Puede copiar la clave allí en cualquier momento.

2

Una clave para el SDK del navegador

En **API y Desarrollador > Claves API**, use **Crear nueva clave**, elija el tipo **Clave Publicable** e introduzca los dominios de su sitio web. Su web carga entonces el SDK de huellas digitales con ella.

3

Cree un IDP Agent para los documentos de identidad

Seleccione una foto de muestra y después **Acciones > Agentes y flujos de trabajo > IDP** y **Crear nuevo agente**. Elija una plantilla para documentos de identidad o describa los campos con sus propias palabras.

4

Compare los valores con el origen

En la pestaña **Campos de datos**, cada valor aparece junto al fragmento del documento de identidad. La vista **IDP Review** muestra todos los documentos con campos abiertos.

5

Gestione las tareas de revisión

Si falta un campo obligatorio, se crea una tarea en la cola de revisión elegida. En **Workflow AI > Tareas Human In The Loop**, una persona ve el documento de identidad y los campos y completa la revisión.

CONSEJO PRÁCTICO

Valore varias señales en conjunto Una VPN por sí sola suele tener motivos inofensivos. Adquiere significado junto con una dirección desechable o con un dispositivo que ya está vinculado a otras cuentas de su sistema. Defina cuándo revisa una persona.

04 · UN EJEMPLO

Un comercio de telefonía. Contratos a plazos.



Un comercio de telefonía móvil con seis tiendas y una tienda online vende smartphones con contratos y planes a plazos. En la tienda, el equipo copia el documento de identidad y transcribe los datos; online basta con un formulario. Una y otra vez, los pagos se interrumpen y no se puede contactar con los clientes.

ANTES

- En la tienda, el documento de identidad se copia y se transcribe campo a campo en el formulario del contrato.
- Online se acepta cualquier dirección de correo, también las desechables.
- Las solicitudes a través de VPN o centros de datos parecen como todas las demás.
- Nadie se da cuenta de que un mismo dispositivo ya ha presentado varias solicitudes.

CON PAPEROFFICE

- El formulario online comprueba la dirección de correo y, con REVIEW, la solicitud pasa a revisión.
- La comprobación de IP indica VPN, Tor y centro de datos, y la solicitud compara el país con la dirección.
- Cada solicitud guarda el visitor_id, de modo que los dispositivos usados varias veces destacan.
- En la tienda, un IDP Agent lee el documento de identidad de una foto, y el equipo contrasta los valores con el original.

Ejemplo ilustrativo; la empresa y el proceso son ficticios. Consulte con su delegado de protección de datos qué datos de identidad y de dispositivos recoge y durante cuánto tiempo los conserva.

05 · LISTA DE CONTROL

Diez puntos para el alta de sus clientes.

Repáselos con ventas, TI y protección de datos. Cada punto se puede comprobar en su propia empresa.

- ☐ Cada alta comprueba la dirección de correo antes de activar la cuenta.
- ☐ Su backend envía la dirección IP del cliente a la API en el parámetro ip.
- ☐ El país de la dirección IP se compara con la dirección indicada.
- ☐ Si una cuenta conocida inicia sesión desde un dispositivo desconocido, su aplicación pide un segundo factor.
- ☐ Para las solicitudes de supresión, la vía mediante POST /privacy/forget está documentada.
- ☐ Para REVIEW y REJECT está definido qué ocurre: volver a preguntar, enviar a revisión o rechazar.
- ☐ VPN, Tor y centro de datos se valoran por separado, con una regla para cada caso.
- ☐ El visitor_id se guarda con cada cuenta y cada solicitud.
- ☐ Un IDP Agent lee los documentos de identidad, y los campos obligatorios están definidos.
- ☐ La finalidad, la base legal y el plazo de conservación de los datos de dispositivo están acordados con protección de datos.

06 · PREGUNTAS FRECUENTES

Lo que quieren saber los equipos antes de empezar.

¿PaperOffice comprueba los documentos de identidad de forma biométrica?

PaperOffice funciona sin comparación facial. Un IDP Agent lee los campos del documento de identidad con su ubicación de origen, y las demás comprobaciones aportan señales sobre correo, red y dispositivo. Su equipo decide si una identidad queda confirmada.

¿Qué pasa con las personas que usan una VPN por buenos motivos?

Una VPN es una señal que su regla pondera. La respuesta separa VPN, proxy, Tor y centro de datos, y nombra la lista correspondiente en el campo type. Las direcciones de listas de bloqueo también aparecen en is_vpn.

¿Cómo llegan las comprobaciones a nuestro portal?

Mediante la API REST desde su backend, mediante el SDK de huellas digitales con una **Clave Publicable** vinculada a sus dominios, y mediante MCP. Los documentos de identidad se suben a un Workspace donde se ejecuta un IDP Agent.

¿De dónde procede la puntuación de riesgo?

De la comprobación del correo: risk_score de 0 a 100, risk_level de MINIMAL a CRITICAL y la recomendación ACCEPT, REVIEW o REJECT. La comprobación del dispositivo aporta sus propios factores de riesgo, por ejemplo una VPN o una velocidad de desplazamiento imposible.

¿Puedo detectar el mismo dispositivo tras varias cuentas?

Sí, si guarda el visitor_id con cada cuenta. Entonces el mismo ID aparece en varias cuentas. /fingerprint/similar encuentra dispositivos con rasgos parecidos; /fingerprint/linked, dispositivos de la misma red.

¿Cómo gestiono las solicitudes de supresión?

POST /privacy/forget elimina el perfil del dispositivo, los vínculos, el historial y las alertas de un identificador en su organización. Una marca de bloqueo impide que el mismo identificador vuelva a registrarse.

07 · CÓMO EMPEZAR

Compruebe su próximo alta con señales reales.

Cree una cuenta en app.paperoffice.ai, genere una clave API en [API y Desarrollador > Claves API](#) y compruebe su primera dirección con `POST /fakeemail/check`. La facturación es de pago por uso; los detalles están en la página de precios.

Añada la comprobación del correo

Su formulario de alta envía la dirección a través de su backend a `/fakeemail/check` y actúa según el campo de recomendación.

Añada IP y dispositivo

`/ip2location/full` para red y ubicación, el SDK de huellas digitales para el `visitor_id`. Guarde ambos con la solicitud.

Haga leer los documentos de identidad

Cree un IDP Agent con una plantilla de documento de identidad y déjelo ejecutarse automáticamente tras el procesamiento en el Workspace de solicitudes.

FICHAS TÉCNICAS SOBRE ESTE TEMA

Detección de correos electrónicos falsos

paperoffice.ai/downloads/paperoffice-ai-datasheet-fake-email-detector.pdf

Detección de VPN

paperoffice.ai/downloads/paperoffice-ai-datasheet-anonymity-detector.pdf

API de ubicación por IP

paperoffice.ai/downloads/paperoffice-ai-datasheet-ip-location.pdf

Huella digital del dispositivo

paperoffice.ai/downloads/paperoffice-ai-datasheet-device-fingerprint.pdf

IDP Agent

paperoffice.ai/downloads/paperoffice-ai-datasheet-idp-intelligent-document-processing-es.pdf

MÁS SOBRE ESTE TEMA

Fraude de identidad

paperoffice.ai/es/solutions/riesgo/ai-fraude-identidad-deteccion-prevencion



MÁS SOBRE ESTE TEMA

paperoffice.ai/es/solutions/riesgo/ai-fraude-identidad-deteccion-prevencion

PRECIOS

paperoffice.ai/es/precios

CONTACTO

paperoffice.ai/es/contacto