

## Mitiga el riesgo durante todo el ciclo de vida del cliente

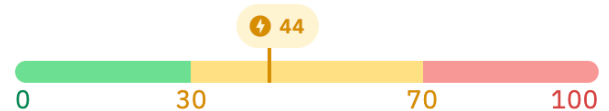
Para muchas empresas, la verificación de identidad requiere más que solo comprobar un documento de identidad. Las señales de riesgo avanzadas de Jumio proporcionan seguridad y confianza adicional de que tus clientes son quienes dicen ser sin generar un riesgo innecesario para tu empresa, durante el onboarding y cada vez que regresan a tu plataforma.

El hub de datos integral de Jumio proporciona acceso a más de 500 fuentes de datos para confirmar la información de carácter personal de tus clientes y evaluar su riesgo. Un score compuesto de riesgo hace que sea simple obtener una respuesta de sí/no y tomar decisiones automáticas en tus flujos de trabajo

A continuación, están algunos de los servicios de riesgo clave que proporciona Jumio.



### Risk Score



### Verificación de identidad global

Procesa el nombre, dirección, teléfono y correo electrónico del usuario a través de una red de bases de datos de identidad global para obtener la seguridad de que pertenecen a esta persona y para evaluar el riesgo general de la persona. Este servicio determina la validez de cada punto de datos, como verificar que el correo electrónico pertenezca a esta persona y determina el riesgo basándose en el comportamiento, como asignar un riesgo más alto si el teléfono está asociado con muchas direcciones IP. Después de evaluar todos estos factores, el servicio retorna con un score de riesgo único para la persona, la cual puedes usar luego en tus reglas para activar más procedimientos KYC rigurosos según sea necesario.

**Este servicio es especialmente útil como una verificación ligera durante el onboarding para determinar si se necesitan más verificaciones o para el monitoreo de riesgo continuo de tus clientes existentes.**



### Verificación de IP geográfica

Verifica el riesgo y la reputación de la dirección IP del usuario y determina la ubicación de su ISP.

**Este servicio es especialmente útil para detener el recorrido del usuario antes de que comience si el usuario está intentando ocultar su ubicación actual o si su dirección IP tiene una velocidad inusualmente alta que puede ser atribuida a un bot.**



### Verificación de dispositivo

Evalúa el riesgo del dispositivo del usuario a través de indicadores, como un extenso historial del dispositivo, anomalías en las huellas dactilares, patrones de uso y emuladores. Descubre si un estafador está utilizando emulación de GPS, rooteo del dispositivo o proxys para ocultar su ubicación de alto riesgo y engañar tu flujo de identificación en línea.

**Como este servicio evalúa el historial antes de que el usuario haya ingresado alguna información, es una excelente verificación sin fricción para ejecutar al comienzo del onboarding o transacción digital.**



## Verificación de correo electrónico

Evalúa el riesgo de una dirección de correo electrónico evaluando su velocidad, edad, detalles de dominio, país, historial de fraude y otros detalles.

**Este servicio retorna información detallada sobre la dirección de correo electrónico para que puedas tomar una decisión informada.**



## Verificaciones de bases de datos del gobierno

Verifica que los datos proporcionados por el usuario o extraídos de un documento de identidad coinciden con los datos registrados en la jurisdicción que emitió el documento legal.

**Este servicio verifica bases de datos de gobiernos de todo el mundo.**



## Verificación de número telefónico

Determina el riesgo y la reputación de un número telefónico. Este servicio observa los patrones de uso (incluyendo tráfico de voz), velocidad de uso y atributos de datos del teléfono, como el tipo de teléfono e información del portador. También comprueba el número en el Consorcio Global de Datos Telefónicos en busca de historial de fraude, evalúa el comportamiento de mensajería e identifica si se encuentra dentro de un rango de números telefónicos que son vistos repetidamente en uno o más servicios web, lo cual podría indicar que un perfil digital está siendo compartido.

**El servicio retorna con un score de riesgo y datos adicionales que pueden guiar tu flujo de trabajo, tal como requerir a usuarios con números de teléfono bloqueados que ingresen un número no bloqueado.**



## Verificación de BIN

Si solicitas una tarjeta de pago a los usuarios durante el onboarding, utiliza el número de identificación bancaria (BIN) de esa tarjeta para obtener información como el nombre del banco, el país y el tipo de tarjeta.

**Esto es útil para marcar tarjetas prepagas (a menudo utilizadas para fraude), tarjetas emitidas en un país diferente al de residencia del usuario (podrían indicar robo de identidad) y tarjetas corporativas (que no son aceptables para juegos de azar en línea).**



## Verificaciones de dirección

Valida y corrobora direcciones con fuentes de terceros e independientes. Determina si la dirección extraída de un documento de identidad emitido por el gobierno existe en el mundo real y comprueba si la persona que está siendo verificada vive en la dirección indicada en su documento de identidad. Jumio comprueba las direcciones en un número de fuentes de datos confiables (por ejemplo, USPS, Royal Mail) para dar un formato apropiado a la dirección, asegurarse de que exista en una dirección indicada y verificar que la persona vive ahí.

**Este servicio es útil para cumplir con las regulaciones regionales que requieren que valides la dirección y establezcas prueba de residencia usando fuentes públicas independientes.**

## ¿Qué señales de riesgo necesito?

Todas las empresas pueden beneficiarse de verificar la reputación del dispositivo antes de que el usuario ingrese su nombre, permitiéndote desviar a usuarios sospechosos a flujos de trabajo más rigurosos mientras simplificas la experiencia para tus buenos clientes. También puedes ejecutar la verificación de identidad global para filtrar identidades sospechosas antes de realizar verificaciones más rigurosas. Puedes verificar la dirección IP del usuario para prevenir que usuarios en ubicaciones prohibidas accedan a tu plataforma. De igual manera, si habilitas que los clientes se puedan transferir dinero entre ellos, puedes determinar si la transacción está teniendo lugar en una ubicación de alto riesgo que necesitaría verificaciones AML o KYC más rigurosas. Y para un escrutinio más exhaustivo, puedes realizar una verificación de dirección, teléfono y correo electrónico y verificaciones de bases de datos del gobierno durante el onboarding y ejecutar verificaciones de identidad global periódicamente en tus clientes existentes. Jumio hace que sea fácil escoger señales de riesgo que cumplan con las necesidades específicas de tu empresa y la tolerancia del riesgo.