Emisión digital instantánea: las mejores prácticas en la administración del fraude

Cómo proteger el futuro de los pagos

Tabla de contenidos

Emisión digital instantánea

Resumen

El futuro de las tarjetas de pago es una experiencia *end-to-end* totalmente digital. La emisión digital instantánea (IDI) permite que el tarjetahabiente cree una cuenta en tiempo real y reciba una credencial lista para usar mediante un canal digital. Es un primer paso fundamental para lograr una experiencia completamente digital, que posibilita la creación y entrega de credenciales de pago a demanda, que pueden utilizarse tanto en los puntos de venta presenciales como en las compras en *eCommerce*.

Cada vez más emisores eligen emitir las tarjetas con IDI; por ello, las instituciones financieras deben entender los riesgos que conllevan las propuestas cien por ciento digitales e informarse acerca de las mejores prácticas que aquí se proponen. Así, podrán mitigar tales riesgos y crear una experiencia segura y sólida, tanto para el cliente como para los emisores.

En este artículo, analizaremos en detalle la IDI, sus beneficios y los impulsores de su crecimiento. Compartiremos, además, cuáles son los mejores pasos que puedes dar para reducir el fraude vinculado.

Planteamiento del problema:

¡Aprobada! Recibirá su tarjeta dentro de los próximos 5 a 10 días hábiles.

Resumen de la emisión digital instantánea

Hacia dónde vamos

La demanda de IDI sigue creciendo a raíz de la migración hacia el comercio digital y una mejor experiencia para el consumidor, y es acelerada por la pandemia.

Hoy tan solo el **10%** de las instituciones financieras de EUA ofrecen IDI y *push provisioning*. Sin embargo, se calcula que este porcentaje superará el **50%** para 2024.[1]

Los beneficios de IDI

Mejor experiencia para el cliente

IDI elimina la inconveniencia de recibir la tarjeta por correo o de retirarla en una sucursal, y garantiza la entrega del 100% de las credenciales de tarjetas digitales

Mayores ingresos

Si la activación es más rápida y los índices de uso son más altos, el negocio crece

Mayor retención del cliente

Los resultados comerciales son mejores con IDI

[1] *In-Branch Instant Issuance – Cardholder Benefits and Competitive Advantage, Aite Novaricia,* noviembre de 2021

Casos de uso

Algunos casos de uso a nivel global son las estrategias para la adquisición de nuevos clientes a través del emisor o sus socios, las estrategias de optimización de los clientes actuales (como la gestión del ciclo de vida y los productos de venta cruzada o *up-selling*) y otros casos de uso que resultan de utilidad.

Distribución escalada

La solicitud y la emisión remotas optimizan el proceso y prescinden del requisito de acercarse a una sucursal o reunirse con un ejecutivo para retirar los documentos de evaluación de riesgo crediticio y KYC. Esto permite escalar la distribución y habilitar un canal disponible 24/7 mediante el cual se puede emitir una tarjeta, activarla instantáneamente y comenzar a utilizarla.

Habilitación

Por lo general, el procesador del emisor es quien habilita la funcionalidad IDI.

- Las capacidades del procesador del emisor, junto con las del emisor, determinan la facilidad o la complejidad de la adopción de IDI.
- Entre las posibles complicaciones que pueden surgir se incluyen las limitaciones de los sistemas bancarios tradicionales, la falta de capacidades para la creación de cuentas en tiempo real y otras restricciones tecnológicas. Cuando un banco consigue un nuevo cliente, la capacidad de verificación KYC es fundamental.
- Los primeros pasos para habilitar IDI en los portafolios de pago son la consulta con el procesador emisor, habilitación tecnológica, evaluación del riesgo de fraude y formas de reducirlo, diseño del ciclo de vida del cliente y elaboración de los casos empresariales. Gracias a los servicios, las alianzas y los productos de Visa, es posible zanjar las brechas identificadas en el análisis inicial.

Emisión digital vs. emisión digital instantánea

	Tradicional	**Instantánea**
Física	Emisión tradicional Se crea y entrega una tarjeta de pagos física que estará lista para usar luego de activarla (de 5 a 10 días hábiles) *Ej.: tarjeta plástica entregada por correo*	Emisión instantánea Se crean y entregan instantáneamente tarjetas de pago físicas que estarán listas para usar en tiempo real *Ej.: tarjeta plástica impresa en la sucursal*
Digital	Emisión digital tradicional Se crean y entregan credenciales de pago a las que se accede mediante una interfaz de usuario digital y que están listas para usar luego de la activación de la tarjeta física (de 5 a 10 días hábiles) *Ej.: tarjeta existente cargada manualmente a la billetera móvil*	Emisión digital instantánea Se crean y entregan instantáneamente credenciales de pago a las que se puede acceder mediante una interfaz de usuario digital y están listas para usar en tiempo real *Ej.: aprobación, creación, emisión y carga en la billetera móvil, todo en tiempo real*

Beneficios e impulsores del crecimiento de la emisión digital instantánea

Qué es lo que está impulsando la adopción de IDI

El tiempo es dinero

Con IDI se puede reducir el tiempo entre la emisión de la tarjeta y la entrega al cliente: de 5-10 días hábiles a 5-10 *minutos*.

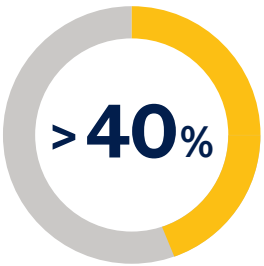
1.Con IDI se puede alcanzar y mantener la condición *top-of-wallet*

Hasta un **25%** de la condición *top-of-wallet* se pierde cada año*

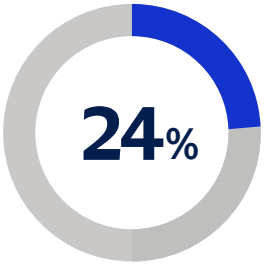
Dado que el gasto *top-of-wallet* de los tarjetahabientes es hasta **4 veces** el promedio del portafolio, esta rotación tiene efectos sustanciales.

Una vez que se abandona la posición *top-of-wallet*, los riesgos de inactividad de compra aumentan. En el 40% de los casos, esto conduce directamente a una deserción activa[1].

2. IDI atrae y motiva a los clientes nativos digitales



de los clientes de bancos minoristas que cambiaron de banco quería un proveedor más innovador[2]



de los clientes bancarios, en todo el mundo, dijo que es menos probable que se acerque a una sucursal luego del cambio de conducta por la pandemia de COVID-19[3]

3. IDI incrementa el uso

+5 transacciones con débito por mes con tarjetas emitidas instantáneamente*

5% **de aumento** en el volumen total de transacciones[4]

4. IDI reduce los costos de la atención al cliente

- Menos gastos en asistencia al cliente y un mejor servicio de autogestión digital, que permite que los clientes resuelvan más problemas por su cuenta
- Menores costos en contraste con la emisión de tarjetas físicas en la sucursal, con terminales y gestión de disponibilidad de tarjetas, que incluye recibir y destruir las tarjetas devueltas

*Análisis de Visa

[1] *The importance of tracking customer engagement through the COVID-19 pandemic, VCA,* octubre de 2020

[2] *Global Data, Digital OnlyBanks: Threat or Motivator?,* diciembre de 2018

[3] *Retail Banking in the New Reality, Survey, Boston Consulting Group,* mayo de 2020

[4] *Instant Issuance is Revolutionizing Financial Institutions' Customer Experience, Harland Clarke,* 2018

Flujo universal de la emisión digital instantánea

Entender el riesgo y mantenerse informado

La emisión instantánea de cuentas digitales incluye la combinación de distintas etapas donde el consumidor y su emisor intercambian información sensible.
Además de proteger los datos, se debe brindar información correcta, autenticada y segura, ya que el emisor la utiliza para tomar decisiones relacionadas con el consumidor, como la extensión de la línea de crédito, y eventualmente para compartir las credenciales de la tarjeta de pago de forma digital.

Como existen muchos aspectos en relación con el riesgo, estrategias de mitigación y posibles soluciones que se deben tener en cuenta para garantizar la precisión y autenticidad de los datos, el propósito de este documento es ayudar a que los emisores logren lo siguiente:

a) Comprender los posibles riesgos de fraude vinculados a IDI
b) Informarse acerca de las principales estrategias para mitigar tales riesgos de fraude

Etapas en el flujo universal de la emisión digital instantánea

Para entender mejor los roles dentro del ecosistema y los *benchmarks* del sector, se puede desglosar IDI en estas cuatro etapas:

- **Generación**
- ***Onboarding***
- **Activación**
- **Uso**

	Generación		*Onboarding*		Activación		Uso	
	Captura	**Procesamiento**	**Cuenta**	**Emisión**	**Activación**	**Entrega**	**Transacción**	**Gestión**
Adquisición	Captura de datos de la solicitud y verificación de identidad completamente digitales	Verificaciones de riesgo y fraude (eKYC, AML, OFAC) y decisiones de otorgamiento de crédito	Aprobación y creación de una cuenta de depósitos a la vista o con línea de crédito	Creación, emisión y financiamiento de credenciales en tiempo real	Activación separada para la tarjeta física y el PAN digital	Credenciales digitales con *push provisioning* para los casos de uso tokenizados (billeteras y COF)	Lista para transacciones CNP presenciales o digitales	Permite controlar la tarjeta y otorga herramientas de gestión
Remisión	Solicitudes por pérdida o robo completamente digitales	Verificación de fraude y elegibilidad para la reemisión instantánea	Bloqueo de tarjeta y actualización de la condición (fraude/no fraude)	Creación y emisión de PAN en tiempo real	Activación separada para la tarjeta física y el PAN digital	Actualización del ciclo de vida del PAN para los casos de uso con y sin token	Lista para transacciones CNP presenciales o digitales	Muestra actualizaciones de los comercios COF y administra las suscripciones
Benchmark	**3 minutos** para procesar una solicitud por pérdida/robo		**2 factores de forma** con emisión del PAN digital primero y tarjeta física opcional		**1 solo clic para la activación y entrega** por canales digitales		**Disponible en todas partes** en más de 100 millones de localidades con comercios a partir del 30 de septiembre de 2021,[1] las principales billeteras digitales, *eCommerce*, *card-on-file*, y cajeros automáticos sin contacto.	

De 5-10 días hábiles a 5-10 minutos!

Visa ayuda a que los clientes alcancen su objetivo **"3 –2 –1 –En todas partes"** con emisión digital instantánea

Términos clave:
AML: anti lavado de dinero
OFAC: oficina de control de activos extranjeros
DDA: cuenta de depósitos a la vista
COF: *Card-On-File*
CNP: tarjeta no presenta
PAN: número de cuenta primario

[1] *Visa Fact Sheet*

Mejores prácticas en la administración del fraude con emisión digital instantánea

Cuatro pasos para reducir el fraude

Paso 1: Generación

Uno de los riesgos en este paso es que en las solicitudes se consigne información incorrecta/falsa. Para reducir el riesgo, se pueden aplicar las siguientes mejores prácticas a fin de verificar la identidad del solicitante y validar la precisión de la información.

Utilizar las bases de datos centralizadas de cada país

Los emisores pueden utilizar la información del usuario que figura en la base de datos centralizada de su país. Esto ayudará a que los emisores tengan menos pérdidas de crédito y por fraude, además de proteger a los consumidores contra robos de identidad u otros tipos de fraude. Los emisores pueden definir que el campo para completar con una foto del rostro en la solicitud de emisión digital instantánea de una tarjeta sea obligatorio. Luego podrán usar esa foto y procesarla en la base de datos centralizada nacional para verificar la información que aportó el solicitante. Para posibilitar estas verificaciones y dar una respuesta a la solicitud, un segundo factor de autenticación confirmará la petición del cliente. Durante un lapso razonable, se debe proceder con precaución y excluir a los clientes que hayan cambiado recientemente su número telefónico o su ID de correo electrónico.

Los emisores también pueden realizar un análisis adicional del comportamiento basado en los movimientos del *mouse* en la pantalla, en la velocidad de tecleo o al completar campos, en las veces que se vuelve a la pantalla anterior o que se cambia de pestañas durante el proceso, y más.

Determine appropriate level of validation strictness on name and address verification (AVS)

Los emisores deben determinar el grado de exigencia de la validación de los datos durante la verificación del nombre y el domicilio (AVS) que se requiere para proveer el servicio, o bien deben ayudar a los tarjetahabientes a minimizar la variación en los datos que ingresan. Como los tarjetahabientes pueden completar su domicilio y su nombre de muchas maneras distintas (por la puntuación, abreviaturas), los emisores deben tener una metodología para generar consistencia en los datos ingresados (por ejemplo, utilizar los datos de domicilio oficiales del servicio postal) o regular el grado de exigencia de la validación.

Rastrear los sistemas/dispositivos personales

Los emisores deben monitorear constantemente la ubicación geográfica desde la que el usuario solicita la IDI de una tarjeta, mediante el rastreo de la dirección IP del dispositivo. Esto sirve para identificar la posible actividad fraudulenta de un estafador que busca abrir una cuenta en un banco fuera de su ubicación geográfica o en el caso de que se estén abriendo distintas cuentas desde un mismo dispositivo/sistema.

Separar los rangos de números de tarjeta según el tipo de emisión

Los emisores pueden asignar diferentes rangos de BIN a los 16 dígitos de la tarjeta según el tipo de emisión; es decir, diferentes rangos de BIN para la emisión digital y para la IDI. Esto ayudaría a los emisores a establecer distintos grupos de reglas antifraude para los distintos tipos de solicitudes de emisión, lo cual mejoría la seguridad.

Paso 2: *Onboarding*

En este paso, se crea la cuenta del tarjetahabiente y se generan, emiten y reemiten las credenciales. Cuando el tarjetahabiente activa las credenciales, puede quedar expuesto a los ataques de enumeración, es decir, a la iteración automática de secuencias numéricas para identificar las combinaciones de PAN y CVV2. Sugerimos las siguientes mejores prácticas para reducir este riesgo:

Uso de PAN no secuencial y CVV2 dinámico

Los emisores pueden usar PAN no secuenciales durante la generación de estos números para los tarjetahabientes. Con esto, se puede reducir el riesgo de sufrir ataques de enumeración.

En el caso de las transacciones con tarjeta no presente, los emisores deberían darles a los tarjetahabientes un CVV2 dinámico (dCVV2). Así, se genera un CVV2 nuevo cada vez que se inicia una transacción de *eCommerce,* con lo cual se puede reducir el riesgo de sufrir ataques de enumeración.

Implementar controles de gastos

Uno de los riesgos en esta etapa de IDI de tarjetas es la aprobación y disponibilidad instantánea de toda la línea de crédito o del saldo disponible, según el caso. Esto significa que, ante una actividad fraudulenta, los fondos pueden ser usados de forma indebida.

- Una de las mejores prácticas para evitar actividades fraudulentas es establecer límites al monto inicial de compra. El emisor puede extender el límite de compra luego de confirmar la autenticidad del tarjetahabiente. Por ejemplo, en un proceso de emisión *digital-first,* una vez que el tarjetahabiente realizó exitosamente la autenticación en una *app* móvil, o luego de recibir y activar la tarjeta física.
- Otra forma de control puede ser fijar límites de gasto separados en cada factor de forma, como la credencial IDI o la tarjeta física.
- Para limitar el riesgo de transacciones no autorizadas, puede ser útil limitar los tipos de transacción y excluir códigos de categoría de comercio (MCC) de alto riesgo, de modo que la credencial emitida digitalmente permita determinadas transacciones con tarjeta no presente. Si las transacciones con tarjeta no presente pasan por una verificación adicional y se busca un segundo nivel de autenticación, el emisor tiene mayor protección.
- Establecer controles específicos sobre los tipos de compras con tarjeta y los patrones de gasto puede disminuir la actividad fraudulenta. Por ejemplo: se puede asignar una credencial IDI a un conjunto de reglas de detección de fraude distinto del de la tarjeta física (por ej., mediante la herramienta *Risk Services Manager*). Esto puede incluir evaluaciones de riesgo basadas en el tiempo durante las autorizaciones. Si no se realizan estas evaluaciones, las reglas de detección de fraude asignadas se pueden cambiar cuando se activa la tarjeta física.

Se recomienda habilitar los reportes y realizar evaluaciones de riesgo constantes en todas las credenciales emitidas digitalmente.

Paso 3: Activación

En esta etapa, se llevan a cabo la activación y el aprovisionamiento inmediato de las credenciales digitales para acceder a la *app* bancaria.

Una decisión importante que se debe tomar es si se usará el mismo PAN en la credencial emitida digitalmente y en la consiguiente tarjeta física, o bien un PAN distinto para cada una. Estas son las ventajas y desventajas:

1. Dos PAN distintos

Ventajas	Desventajas
• Con múltiples PAN, se cuenta con un canal aislado para las transacciones con un número de 16 dígitos que es distinto al de la tarjeta física, que llega desactivada. • Más que evitar ataques de enumeración, sirve para prevenir el secuestro de la tarjeta y el fraude que eso implica. No disminuye la posibilidad de sufrir ataques de enumeración.	• Utilizar múltiples PAN puede generarle confusión al consumidor al momento de saber cuál número usar. • Si el consumidor usa múltiples PAN o si solicita la reemisión, puede tener inconvenientes para actualizar los datos del PAN guardado o con los proveedores de servicios.

2. Un único PAN

Ventajas	Desventajas
• Usar un único PAN para las transacciones evita que el consumidor se confunda.	• La tarjeta física llega activada para usar en diversos tipos de canales. A modo de mitigación, puedes leer la tabla "Activación por canales: mejores prácticas recomendadas" en la página 12 de este artículo.

Una vez que se activa la cuenta del tarjetahabiente en la *app* bancaria, se puede establecer la tarjeta como la preferida en otras *apps* y canales de pago mediante un proceso de *push provisioning* de la nueva cuenta.

Push Provisioning

Habilita el gasto instantáneamente con *push provisioning* de las credenciales digitales en las billeteras móviles, comercios COF y *Click to Pay*.

Al agregar una credencial a una billetera digital, la tarjeta se tokeniza. La tokenización reemplaza el número de la tarjeta por un número aleatorio, llamado *token*. Los *tokens* aseguran que la información de la tarjeta no sea vulnerada durante la transacción y ofrecen un método de pago más seguro que los métodos tradicionales.

Diseñar una solución de *push provisioning* en la *app* puede ser complejo y costoso. Los clientes deberían hacer grandes inversiones para crear estas capacidades, y el tiempo de lanzamiento al mercado sería apresurado. Además, hay otros aspectos, como el mantenimiento de los *endpoints* de la billetera, las actualizaciones del proveedor de billetera, los requisitos normativos y el cumplimiento, entre otros, que pueden complicar el mantenimiento de la solución propia. Sin embargo, los clientes pueden implementar las soluciones de aprovisionamiento que ofrecen sus socios, para acelerar el tiempo de lanzamiento al mercado y minimizar la inversión inicial y posterior.

Paso 4: Uso

Esta es la etapa final, que incluye la transacción del tarjetahabiente y la administración de la cuenta. En esta fase, el tarjetahabiente debería poder recuperar los detalles de la tarjeta desde la *app* bancaria en su móvil para realizar transacciones presenciales sin contacto, además de transacciones de *eCommerce*.

Estas son algunas formas de mejorar la seguridad al exponer los detalles de la tarjeta:

1. Notificar al tarjetahabiente que tiene una nueva credencial
2. Autenticar al tarjetahabiente antes de permitir la activación de la tarjeta. Aquí se pueden incluir preguntas y respuestas de seguridad, verificación adicional con códigos de un solo uso y otras formas de validación para confirmar que el supuesto receptor de la tarjeta es el tarjetahabiente correcto
3. Configurar un temporizador en pantalla que indica un breve período luego del cual el usuario es forzado a volver a la página previa o al inicio si se mantuvo inactivo durante ese lapso
4. Inhabilitar las capturas de pantalla cuando se le muestran estos datos al usuario
5. Ocultar o censurar la pantalla si el usuario mueve la *app* móvil a un segundo plano
6. Inhabilitar la opción de cortar y pegar los datos para usar en otra *app* o impedir que se copien datos al portapapeles

Garantizar una estrategia de activación por canales

Visa recomienda implementar una estrategia de activación por canales a fin de mitigar el riesgo de fraude en las transacciones. El siguiente cuadro sirve a modo de guía:

	Banda magnética	Chip de contacto	Chip sin contacto		*eCommerce*		Cajero automático		Servicios de transferencias de fondo
Campos de datos	PEM 90 Tipo de transacción 01 = extracción de dinero Tipo de transacción 30 = consulta de fondos disponibles	PEM 05	PEM 07		PEM 01; ECI 5, 6, 7; AVS		MCC 6010/6011; Tipo de transacción 01, 30		
			PAN	Token	PAN	Token	PAN	Token	
Creación de cuenta nueva	Deshabilitada	Deshabilitada	Deshabilitada	Deshabilitada	Deshabilitada	Deshabilitada	Deshabilitada	Deshabilitada	Deshabilitada
Push Provisioning de pagos / *App* bancaria	Deshabilitado	Deshabilitado	Deshabilitado	Habilitado	Deshabilitado	Habilitado	Deshabilitado	Habilitado	Habilitado
PAN / CVV2 exhibido en la *app*	Deshabilitado	Deshabilitado	Deshabilitado	Deshabilitado	Habilitado	N/A	Por definir	Deshabilitado	Habilitado
Token / CVV2 exhibido en la *app*	Deshabilitado	Deshabilitado	Deshabilitado	Deshabilitado	Deshabilitado	Habilitado	Deshabilitado	Por definir	Habilitado
Asignación de PIN para cajeros	Deshabilitada	Deshabilitada	Deshabilitada	Deshabilitada	Deshabilitada	Deshabilitada	Habilitada	Habilitada	Deshabilitada
Entrega de la tarjeta física	Habilitada	Habilitada	Habilitada	N/A	Habilitada	N/A	Habilitada	N/A	Habilitada

Marca de verificación	
N/A	No corresponde – No es posible la combinación de canal y campo de datos
Por definir	Por definirse según las necesidades del cliente

Permite el uso de la tokenización para que las transacciones sean seguras y

La tokenización reemplaza los datos sensibles de la cuenta, como el número de cuenta de 16 dígitos, por un identificador digital único llamado token. El token permite procesar pagos sin exponer los detalles de la cuenta, lo cual evita que puedan ser vulnerados. La tokenización tiene otros beneficios, como la habilitación de billeteras digitales y mejores índices de autorización en las transacciones *online*.

Términos claves:

PEM - Modo de entrada de POS (POS - Punto de venta)
PEM 01 = Ingreso manual de clave
PEM 07 = Sin contacto
PEM 05 = *Card on File*
PEM 90 = Banda magnética
ECI - Indicador de comercio electrónico
Tipo de transacción 01 = Extracciones de dinero
Tipo de transacción 30 = Consulta de fondos disponibles
AVS - Servicio de verificación de domicilio
MCC - Código de categoría del comercio
MCC 6010 = Desembolso manual de efectivo, instituciones financieras
MCC 6011 = Desembolso automático de efectivo, instituciones financieras
PAN - Número de cuenta primario
CCV2 - Código de verificación de la tarjeta 2

Cómo puede ayudarte Visa

Visa cuenta con las herramientas y los servicios necesarios para ayudar a que los emisores implementen, en cada etapa del ciclo de vida de la emisión digital instantánea, las siguientes mejores prácticas:

Visa cuenta con las herramientas y los servicios necesarios para ayudar a que las instituciones financieras implementen las mejores prácticas en cada etapa de la emisión digital instantánea. En la etapa de la generación, las instituciones financieras pueden implementar Visa ICS, un producto de gestión de riesgos que se utiliza para mejorar el análisis crediticio y la prevención de fraudes.

Luego, para el *onboarding,* Visa ofrece distintas API y herramientas, como *Visa Account Updater Suite;* y para la activación de las tarjetas emitidas, Visa ofrece soluciones como *Visa Token Service (VTS), Visa Card Enrollment Hub (VCEH), Visa In-App Provisioning (VIAP)*, API y SDK, como refuerzo de las capacidades internas de las instituciones financieras para la prevención del fraude.

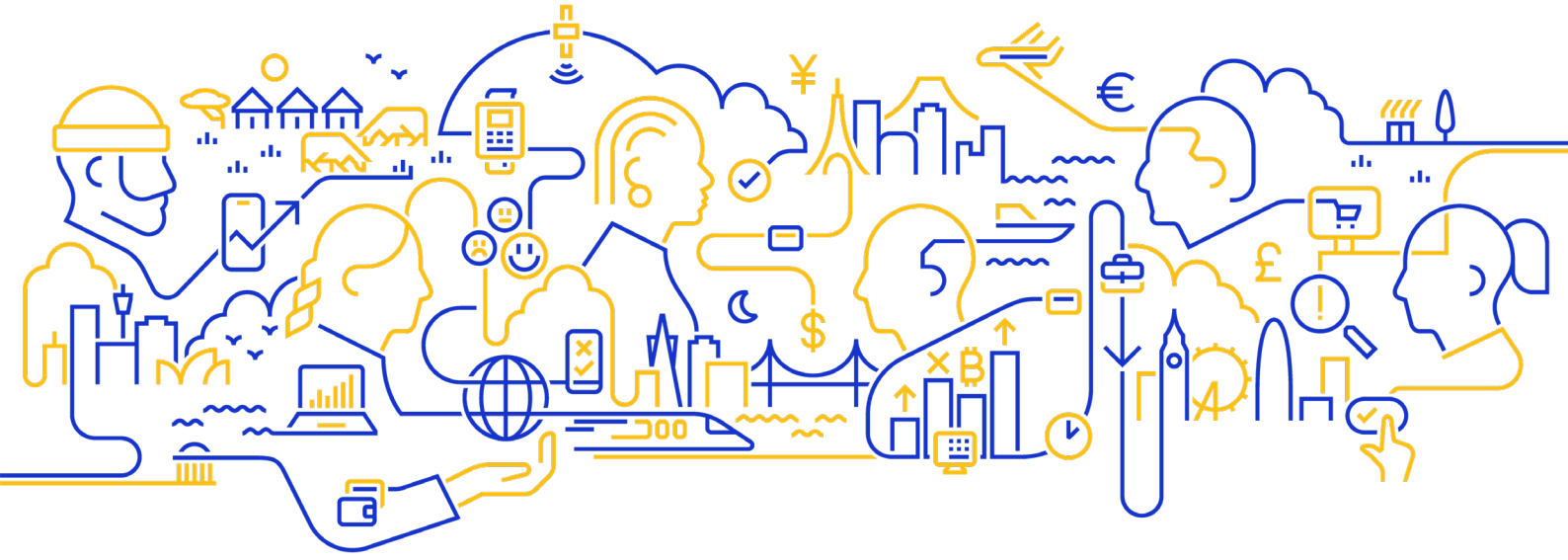
Por último, cuando las instituciones financieras están listas para la etapa del uso, pueden aprovechar múltiples herramientas, como *Visa Risk Manager (VRM), Visa Transaction Controls (VTC) y Risk Services Manager (RSM)*, además de *Visa Consumer Authentication Service (VCAS) y Visa Advanced Authorization (VAA)* para mejorar los mecanismos de puntuación y las capacidades de detección, prevención y mitigación del fraude en transacciones.

Si quieres más información sobre estos productos de Visa, comunícate con tu representante Visa.

Sobre *Visa Consulting & Analytics*

Visa cuenta con el posicionamiento ideal para trabajar con los clientes y formular un caso empresarial de IDI, dimensionar las oportunidades, desarrollar estrategias, diseñar el ciclo de vida del usuario y evaluar las capacidades de prevención del fraude, además de recomendar cómo resolver las brechas.

- Nuestros consultores cuentan con décadas de experiencia en la industria de pagos y son expertos en estrategia, producto, gestión de portafolio, riesgos, recursos digitales y más.
- Nuestros científicos de datos son expertos en estadísticas, analítica avanzada y *machine learning* con acceso exclusivo a datos obtenidos a través de VisaNet, una de las redes de pago más grandes del mundo.
- Entender las condiciones económicas que afectan al consumo permite a nuestros economistas brindar información única y oportuna sobre las tendencias de consumo global. La combinación de nuestra amplia experiencia en consultoría de pagos, nuestra inteligencia en estrategias económicas y la amplia variedad de datos con la que contamos nos permite identificar conocimientos prácticos y recomendaciones que ayudan a tomar mejores decisiones comerciales.



Para más información, contacta a tu ejecutivo de cuenta Visa, escribe a *Visa Consulting & Analytics* a **VCA@Visa.com** o visita **Visa.com/VCA**

Sigue a VCA en **LinkedIn**