emBlue

EMBLUE PARA BANCOS · CÓMO FUNCIONA

OPERACIONES Y SEGURIDAD

Cada resumen, cada vencimiento y cada código, entregado y registrado.

Las comunicaciones operativas sostienen la confianza en el banco todos los meses. Esta guía muestra cómo emBlue las entrega con trazabilidad y seguridad: qué resultados buscar, cómo funciona, qué conectar y por dónde empezar.

Menos contactos evitables **Pagos a tiempo** **Resúmenes con constancia**

Autenticación segura

01 La pregunta y los resultados
02 Cómo funciona
03 Recorridos operativos
04 Un mes en el ciclo de la tarjeta de Lucía
05 Qué sistemas conectar
06 Seguridad y cumplimiento
07 Por dónde empezar y cómo medir

01 · LA PREGUNTA Y LOS RESULTADOS

¿Cómo te aseguras de que cada comunicación operativa llegue a tiempo y quede registrada?

Un resumen que no llega, un vencimiento que se olvida o un código que demora se convierten en un llamado, una mora o una operación que no se completa. Operar bien estas comunicaciones también prepara el terreno para marketing.

Menos contactos evitables

Información clara y a tiempo sobre resúmenes, pagos, movimientos e incidentes.

CÓMO SE MIDE

Contactos por motivo (resumen, pago, saldo, incidente) cada 1.000 clientes activos.

Más pagos a tiempo

Avisos de vencimiento oportunos y recordatorios que se detienen cuando el pago se registra.

CÓMO SE MIDE

Pagos a término sobre resúmenes con vencimiento. Mora temprana.

Resúmenes con constancia

Cada resumen de tarjeta y de cuenta con registro de envío y de entrega.

CÓMO SE MIDE

Resúmenes con entrega confirmada. Pedidos de reenvío.

Autenticación segura

Códigos de verificación que llegan dentro de su tiempo de validez, con canal alternativo.

CÓMO SE MIDE

Códigos entregados en tiempo. Reintentos por código no recibido.

Cada paso se mide por separado

Evento recibido → enviado	El tiempo desde que el sistema del banco informa el hecho hasta que sale el mensaje, contra el SLA acordado.
Entrega confirmada	Un envío exitoso no prueba que el cliente recibió la información. La entrega se registra mensaje por mensaje.
Exceso de comunicación	Bajas de suscripción y reclamos por cantidad de mensajes, para que más avisos no signifique más insistencia.

Metas que se acuerdan, no que se prometen: se fijan después de medir la línea base de cada banco.

Lo que dice el mercado

US$ 470 M

en pérdidas reportadas en 2024 en EE. UU. por las estafas por mensaje de texto más comunes, que a menudo parecen venir de un banco. Más de cinco veces lo de 2020.

17 veces

más fraude en pagos con tarjeta cuando el receptor estaba fuera del EEE, donde la autenticación reforzada (SCA) no es obligatoria y a menudo no se usa.

53% / 58%

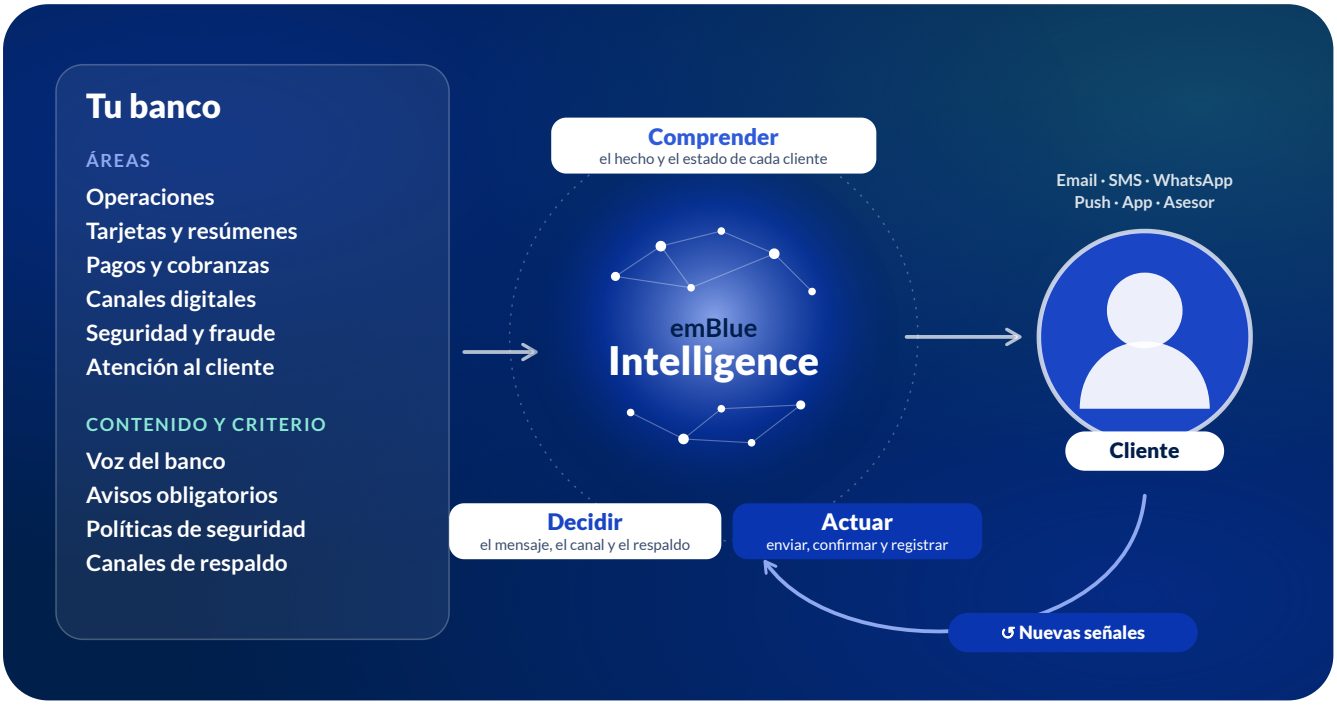
de los clientes bancarios se preocupa por su privacidad y teme riesgos de hackeo, respectivamente.

Fuentes: FTC, Data Spotlight “Top text scams of 2024”, 14 de abril de 2025 (pérdidas reportadas por consumidores en EE. UU.). EBA y BCE, informe conjunto sobre fraude en pagos, 15 de diciembre de 2025 (Espacio Económico Europeo). Accenture, Global Banking Consumer Study 2025 (encuesta global). Cifras traducidas del inglés. Muestran el contexto de riesgo y confianza, no el efecto de implementar una plataforma, y no son datos del mercado latinoamericano.

02 · CÓMO FUNCIONA

Cada aviso parte de un hecho del banco y llega por el canal que corresponde.

Tus sistemas informan qué pasó, el perfil dice a quién y por dónde, y tus políticas definen cómo. emBlue comprende, decide y actúa con los datos, las reglas, los journeys y la IA que configura tu equipo.



GENÉTICA
Avisos obligatorios, políticas de seguridad, canal de respaldo para cada tipo de mensaje, horarios y voz del banco.

MEMORIA
Productos y tarjetas, titular o adicional, canales verificados y consentimiento por canal, push habilitado, historial de entregas.

CONTEXTO
Un resumen emitido, un vencimiento próximo, un pago registrado, un pedido de código, un consumo o un incidente de servicio.

CONTEXTO El sistema de autenticación pide un código.
MEMORIA Celular verificado. WhatsApp habilitado.
GENÉTICA Sin entrega a tiempo, el canal alternativo.

→ **Enviar el código por SMS, con respaldo**

CONTEXTO Se emite el resumen de la tarjeta.
MEMORIA Adherida al resumen digital por email.
GENÉTICA Registrar envío y entrega de cada resumen.

→ **Enviar el resumen y guardar la constancia**

Tráfico transaccional

Resúmenes, vencimientos, códigos y alertas viajan separados de las campañas y se envían siempre que corresponda, según las políticas del banco.

Comunicaciones de marketing

Las promociones del banco usan solo los canales con consentimiento y se pausan con una mora, un reclamo o una alerta de seguridad abierta.

03 · RECORRIDOS OPERATIVOS

Seis recorridos, cada uno con su canal, su respaldo y su métrica.

Se comunican los hechos relevantes, no cada movimiento. Cada recorrido usa un canal que el cliente habilitó, tiene una alternativa si la entrega falla y una métrica que muestra si funcionó.

RECORRIDO	OBJETIVO	CANAL PRINCIPAL	MÉTRICA
1 · Resúmenes con envío certificado	Que cada resumen de tarjeta y de cuenta llegue, con constancia de envío y de entrega.	**Email** Sin entrega confirmada: aviso por SMS o en la app para descargarlo	Resúmenes con entrega confirmada. Pedidos de reenvío.
2 · Vencimientos y pagos	Informar fecha y monto antes del vencimiento y confirmar el pago.	**WhatsApp** Sin opt-in o sin entrega: SMS. Con el pago registrado, los recordatorios se detienen	Pagos a término. Contactos para confirmar un pago.
3 · Estados de cuenta al día	Informar movimientos, límites y cambios en la cuenta en el momento.	**Push** Sin push habilitado: email	Contactos por consultas de saldo, límite o movimientos.
4 · Códigos de verificación (2FA)	Autenticar accesos y operaciones con un código OTP.	**SMS** Sin entrega dentro del tiempo acordado: WhatsApp o email, según la política del banco	Códigos entregados en tiempo. Reintentos por código no recibido.
5 · Alertas de seguridad	Avisar consumos, transferencias, un dispositivo nuevo o un cambio de datos.	**Push** Alertas críticas sin entrega confirmada: SMS	Alertas entregadas. Tiempo del evento a la entrega.
6 · Avisos de servicio e incidentes	Anticipar mantenimientos e informar un incidente y su resolución.	**App y email** Clientes afectados sin entrega confirmada: SMS	Contactos al centro de atención durante el incidente.

Reglas que se configuran

- Las comunicaciones obligatorias y de seguridad se mantienen siempre.
- Con mora, un reclamo o una alerta de seguridad abierta, no se envían ofertas.
- Titular y adicional reciben lo que les corresponde, sin duplicar avisos.
- Frecuencia y horario de contacto, salvo códigos y alertas de seguridad.

Alcance

emBlue recibe los eventos de los sistemas del banco y activa las comunicaciones que su equipo definió, con el canal y el respaldo acordados.

El sistema de autenticación del banco genera y valida cada código. Los criterios de riesgo y de fraude siguen siendo del banco.

04 · CASO ILUSTRATIVO

Un mes en el ciclo de la tarjeta de Lucía. Primero lo operativo, después la promoción.

Lucía es clienta de Banco Pradera, un banco ficticio. Cada paso deja una señal que el banco usa en el siguiente. Plazos, canales y promociones dependen de cada banco.

Día 1	**Cierra el resumen** El resumen de su tarjeta Pradera llega por email. El envío y la entrega quedan registrados como constancia.	SEÑAL Resumen entregado. Constancia guardada.
Día 15	**Se acerca el vencimiento** Tres días antes, un WhatsApp le recuerda la fecha y el monto a pagar.	SEÑAL Recordatorio entregado.
Día 16	**Paga desde la app** Cobranzas registra el pago, llega la confirmación y el recordatorio del día del vencimiento se cancela.	SEÑAL Pago registrado. Recordatorios detenidos.
Día 20	**Estrena celular** Entra a la app desde un dispositivo nuevo y recibe por SMS un código de verificación. El banco valida el código.	SEÑAL Código entregado en tiempo.
Día 22	**Hace una compra grande** Un push le confirma el consumo al instante. Si no lo reconociera, la app le muestra cómo avisar al banco.	SEÑAL Alerta entregada. Sin reportes.
Día 28	**Recién ahora, una promoción** Sin mora ni alertas abiertas, y con consentimiento de marketing, recibe una promoción del banco en un rubro donde ya compra.	SEÑAL Interés en la promoción.

Qué cambia para operaciones

Cada mensaje se activa por un hecho que registra un sistema del banco y queda en la historia de Lucía con su estado de entrega. Atención ve qué se envió y cuándo, y marketing solo llega cuando lo operativo está en orden.

Las fuentes de cada recorrido operativo y con qué frecuencia actualizarlas.

SISTEMA DEL BANCO	QUÉ APORTA	CAPA	RECORRIDOS QUE HABILITA	ACTUALIZACIÓN REQUERIDA
Core bancario	Cliente, cuentas, titulares y adicionales, datos de contacto verificados, movimientos	MEMORIA CONTEXTO	Estados de cuenta, alertas, todos los demás	En minutos Movimientos y límites. Cartera completa: diaria.
Procesador de tarjetas Emisor o procesador	Cierre, vencimiento, monto, consumos y autorizaciones	CONTEXTO	Vencimientos, alertas de consumo	Inmediata Consumos. Cierres y vencimientos: diaria.
Resúmenes y documentos Generación documental	Resumen generado, archivo o enlace, cliente destinatario	CONTEXTO	Resúmenes con envío certificado	En minutos Por lote de cierre, dentro del plazo acordado.
Pagos y cobranzas	Pago registrado, débito rechazado, mora temprana	CONTEXTO	Vencimientos y pagos	Inmediata Un pago registrado detiene los recordatorios.
Autenticación e IAM	Pedido de código, operación a autenticar, dispositivo nuevo, cambio de datos	CONTEXTO	Códigos de verificación, alertas de seguridad	Inmediata El código vence en minutos. El banco lo genera y lo valida.
App móvil y push	Permisos de push, dispositivos activos, ingresos a la app	MEMORIA CONTEXTO	Alertas, estados de cuenta, incidentes	En minutos Permisos de push: inmediata.
CRM y atención	Reclamos abiertos, motivo de contacto, segmento, interacciones	CONTEXTO MEMORIA	Pausa de ofertas, promociones del banco	En minutos Reclamos abiertos. Segmentos: diaria.
Preferencias y consentimientos	Consentimiento por canal, marketing y transaccional por separado, resumen digital	MEMORIA	Todos	Inmediata La política para respetarlos es Genética.
Incidentes y estado del servicio	Mantenimiento programado, incidente abierto, clientes afectados, resolución	CONTEXTO	Avisos de servicio e incidentes	Inmediata Mantenimientos: con anticipación.

Inmediata: segundos después del evento. En minutos: dentro del SLA acordado. Diaria: actualización por lotes. La frecuencia final se acuerda con el banco. Los datos llegan a emBlue mediante integraciones, conectores de Data Lab y API. El banco conserva sus sistemas y sus criterios de riesgo y fraude.

06 · SEGURIDAD Y CUMPLIMIENTO

La infraestructura de mensajería que un banco puede auditar.

Las comunicaciones operativas llevan información sensible y sostienen la confianza en el banco. Por eso cada envío se controla, se registra y se puede revisar.

CERTIFICACIÓN

ISO 27001

Gestión de la seguridad de la información.

INFORME DE CONTROLES

SOC 2

Controles de seguridad auditados.

El alcance y la vigencia de cada certificación se revisan en la evaluación de proveedores del banco.

Controles que se configuran en cada recorrido

Entrega y errores por mensaje. Cada envío registra su estado: enviado, entregado o con error, y el motivo.

Deduplicación. Cada evento se identifica de forma única y no genera dos mensajes.

Registro. Cada comunicación queda en la historia del cliente, disponible para atención y auditoría.

Canal alternativo. Un error de entrega activa el canal de respaldo definido para ese tipo de mensaje.

Tráfico transaccional separado. Resúmenes, códigos y alertas no compiten con las campañas.

Volumen a escala. Infraestructura de mensajería para envíos masivos, como el cierre de resúmenes.

Lo que conserva el banco

- Sus criterios de riesgo y de fraude.
- La generación y validación de los códigos.
- Qué se comunica, por qué canal y con qué respaldo.
- Sus sistemas y sus fuentes de datos.

Mensajes que el cliente reconoce

Una voz y unos canales consistentes ayudan a que el cliente distinga un aviso real de un intento de fraude. Lo que el banco nunca pide por mensaje forma parte de su Genética.

emBlue no valida identidades ni decide si una operación es segura: envía las comunicaciones que el banco define.

Con la información que recibe de sus sistemas y dentro de las políticas que configura su equipo.

07 · POR DÓNDE EMPEZAR Y CÓMO MEDIR

Un recorrido, los datos que ya tienes y una métrica desde el primer día.

No hay una secuencia única. Elige el problema operativo que más pesa hoy y suma las promociones del banco cuando lo operativo esté en orden.

SI TU OBJETIVO ES...	EMPIEZA POR	DATOS NECESARIOS	MÉTRICA PRINCIPAL
Probar la entrega de resúmenes	Resúmenes con envío certificado	Resúmenes y documentos, procesador de tarjetas, consentimientos	Resúmenes con entrega confirmada.
Bajar la mora temprana	Vencimientos y pagos	Procesador de tarjetas, pagos y cobranzas	Pagos a término.
Asegurar la autenticación	Códigos de verificación (2FA)	Autenticación e IAM, contactos verificados del core	Códigos entregados en tiempo.
Informar en el momento	Alertas y estados de cuenta	Core bancario, procesador, app móvil y push	Contactos por saldo o movimientos.
Ordenar los incidentes	Avisos de servicio	Incidentes y estado del servicio, CRM y atención	Contactos durante el incidente.
Sumar las promociones propias	El siguiente paso, con lo operativo en orden	CRM, consentimientos de marketing, estado de mora	Conversión. Bajas de suscripción.

Trazabilidad de cada comunicación

Evento recibido → **Mensaje enviado** → **Entrega confirmada** → **Respuesta o acción**

Línea base primero

Mide antes de empezar: contactos por motivo, pagos a término, reenvíos de resúmenes y reintentos de códigos.

Comparar lo comparable

Compara por producto, ciclo de cierre y canal. Las comunicaciones obligatorias y de seguridad nunca se retienen para medir.

Cuando lo operativo llega a tiempo y con constancia, cada aviso suma confianza.

Habla con un especialista