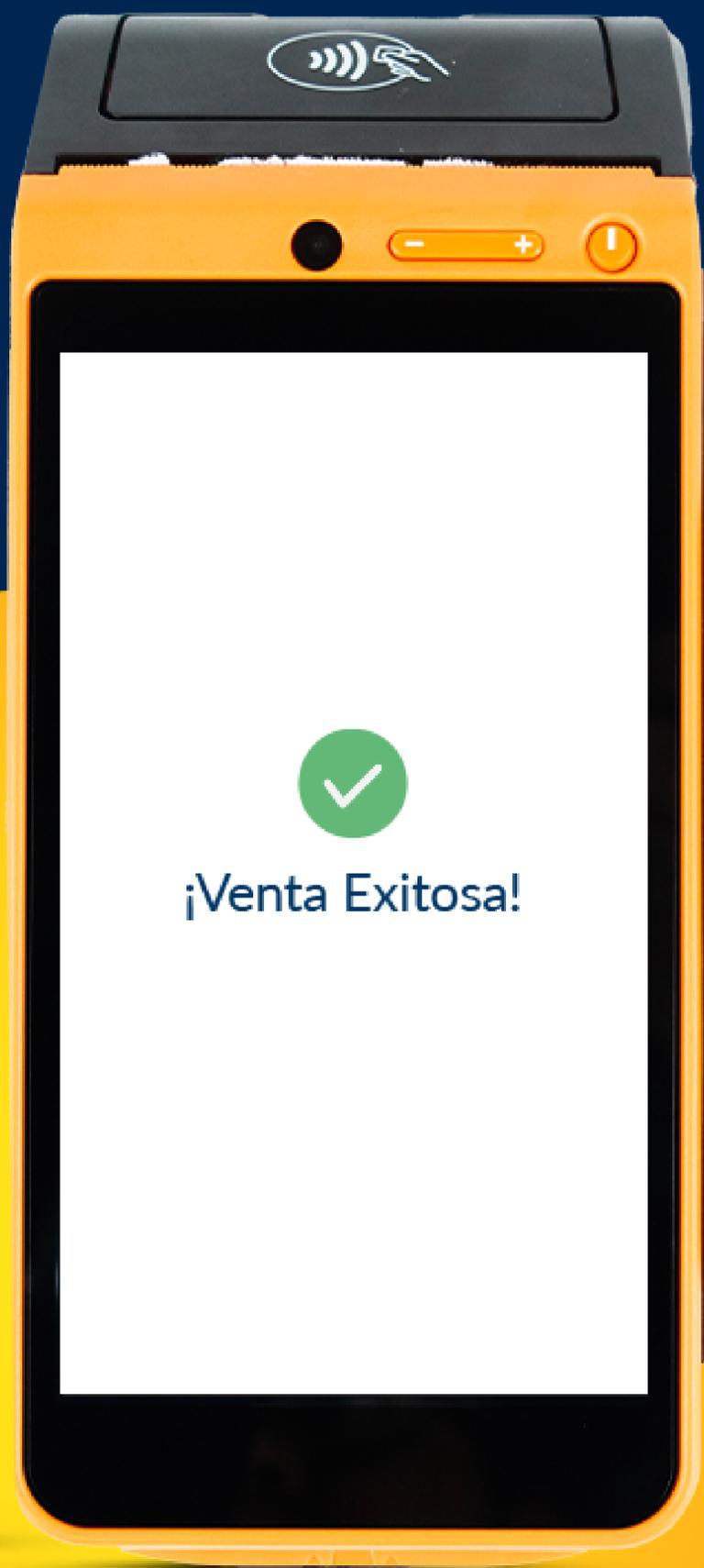


Manual de **Venta segura** 2025





Uso de tarjetas físicas.



Buenas prácticas



Solicita siempre la tarjeta y verifica la identidad del cliente.

Antes de procesar el pago, revisa que el nombre y/o firma de la tarjeta coincida con una cédula o documento válido. Esto previene fraudes y brinda seguridad a ambas partes.



Utiliza el POS en presencia del cliente.

Nunca retires la tarjeta ni el datáfono del campo visual del cliente. Realiza la transacción frente a él, explicando cada paso si es necesario.



Muestra el monto antes de procesar la transacción.

Verifica y enseña al cliente el valor ingresado en el POS antes de que coloque su tarjeta. La transparencia evita errores y genera confianza.



Entrega siempre el comprobante de pago.

Ofrece el voucher físico o digital al cliente, incluso si no lo solicita. Además de ser una buena práctica, es respaldo para ambas partes en caso de reclamos.





Uso de tarjetas físicas.



Malas prácticas

- ✘ No anotes, tomes fotos ni almacenes datos de la tarjeta.**

Es ilegal y peligroso registrar el número, CVV o fecha de vencimiento. Protege la privacidad del cliente y evita riesgos de fraude.

- ✘ Evita pasar la tarjeta fuera de la vista del cliente.**

No te lleves el POS a otro lugar. Esto puede generar desconfianza y sospechas de clonación o cobros indebidos.

- ✘ No cobres montos diferentes sin informar al cliente.**

Cualquier cambio en el precio acordado debe ser comunicado antes del cobro. Evita sorpresas que puedan dañar tu reputación.

- ✘ No dividas el pago en varias transacciones sin autorización.**

Fraccionar montos en múltiples cobros, sin una razón clara y sin consentimiento, puede generar alertas bancarias o devoluciones de dinero.





Ventas con dispositivos NFC

(wearables y celulares)



Buenas prácticas



El dispositivo siempre debe permanecer en poder del cliente.

El cliente debe ser quien acerque su celular, reloj o anillo al datáfono. Bajo ninguna circunstancia se debe solicitar que entregue el dispositivo al cajero.



Brinda una experiencia segura e informada.

Acompaña el proceso con confianza y claridad. Si el cliente tiene dudas, explícale que los pagos NFC están encriptados y son altamente seguros.



Confirma que el POS haya detectado correctamente el pago.

El lector debe emitir un sonido, vibración o mensaje como "Procesando" o "Aprobado". No entregues el producto hasta tener esta confirmación en pantalla.



No solicites PIN, cédula o firma si el sistema no lo exige.

Si el pago sin contacto ha sido autorizado por el sistema, no es necesario solicitar pasos adicionales al cliente. Confía en el protocolo del banco o emisor.





Ventas con dispositivos NFC

(wearables y celulares)



Malas prácticas

- ✘ Rechazar pagos con billeteras digitales por desconocimiento.**

No está permitido negar pagos con medios válidos como Apple Pay, Google Wallet o anillos NFC, únicamente por no conocerlos. Infórmate y capacita a tu equipo.
- ✘ Pedir al cliente que entregue su dispositivo para efectuar el pago.**

Nunca tomes en tus manos el celular, reloj o wearable del cliente. Esto compromete su privacidad y va en contra de las normas de seguridad.
- ✘ Solicitar comprobantes ajenos al POS para validar pagos NFC.**

No es profesional ni seguro exigir capturas de pantalla, notificaciones bancarias o comprobantes manuales. Valida siempre desde el sistema o terminal oficial.
- ✘ Desinformar al cliente sobre la seguridad de los pagos sin contacto.**

Evita comentarios como “eso no es seguro” o “mejor en efectivo”. Estos métodos cuentan con estándares internacionales de protección y respaldo bancario.





Pago con billeteras Electrónicas

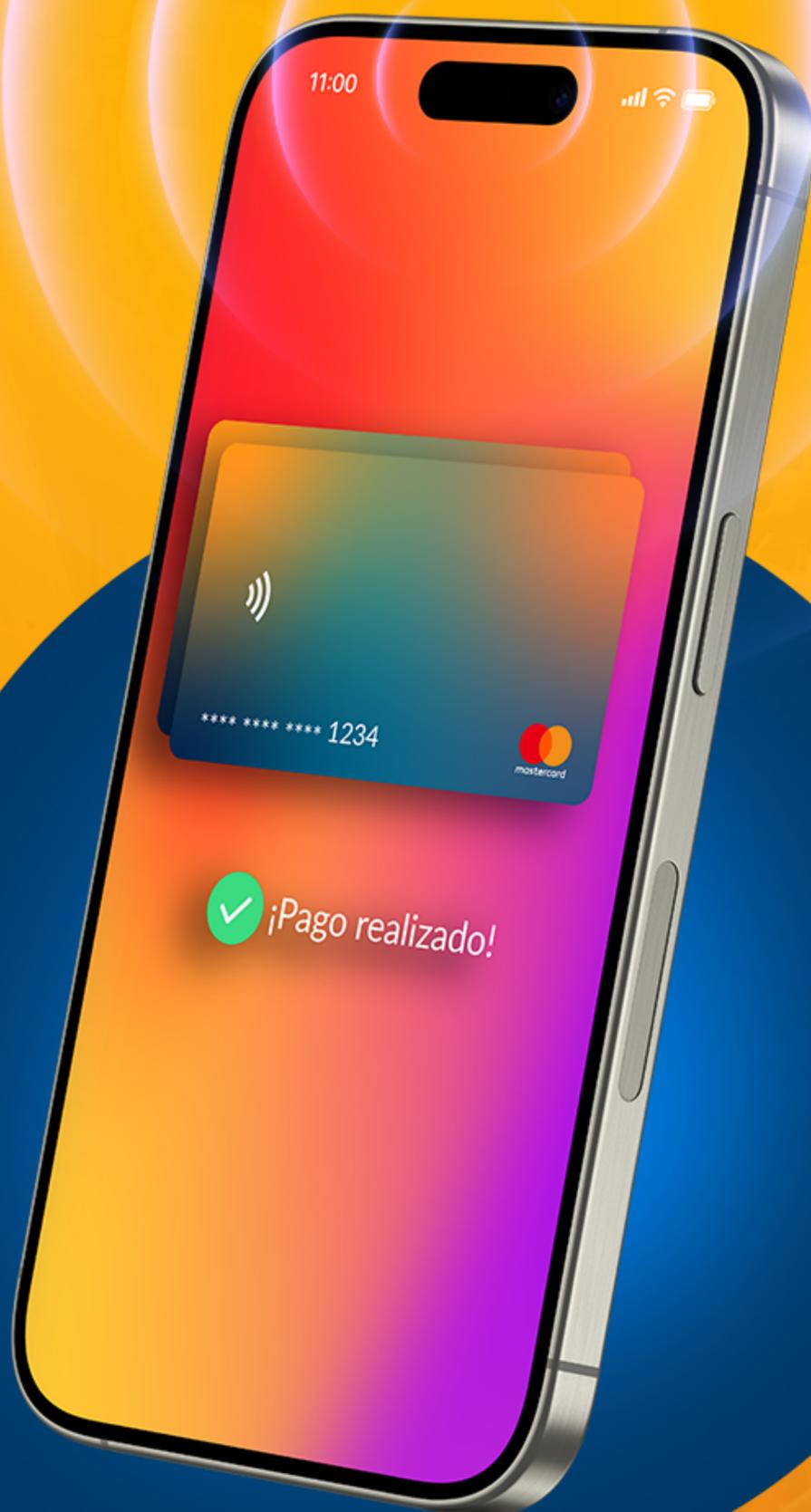


Buenas prácticas

- ✓ **Confirma el monto antes de generar el código QR o enlace de pago.**
Antes de mostrar el código QR o enviar el link, asegúrate de que el valor ingresado sea correcto. Esto evita errores y garantiza una transacción transparente.
- ✓ **Verifica en el sistema o app que el pago haya sido procesado.**
No entregues el producto o servicio hasta que el sistema confirme el pago. Captura o guarda la pantalla de confirmación como respaldo.
- ✓ **Solicita al cliente que valide el pago en su dispositivo.**
Permite que el cliente realice el proceso en su celular, sin presionarlo ni manipular su dispositivo. Respeta siempre su privacidad y tiempo de validación.

- ✓ **Entrega comprobante de venta (digital o físico).**

Aunque el pago fue digital, siempre brinda un comprobante con los datos de la transacción. Esto aporta profesionalismo y seguridad para ambas partes





Pago con billeteras Electrónicas



Malas prácticas

✘ No pidas que el cliente te entregue su celular.

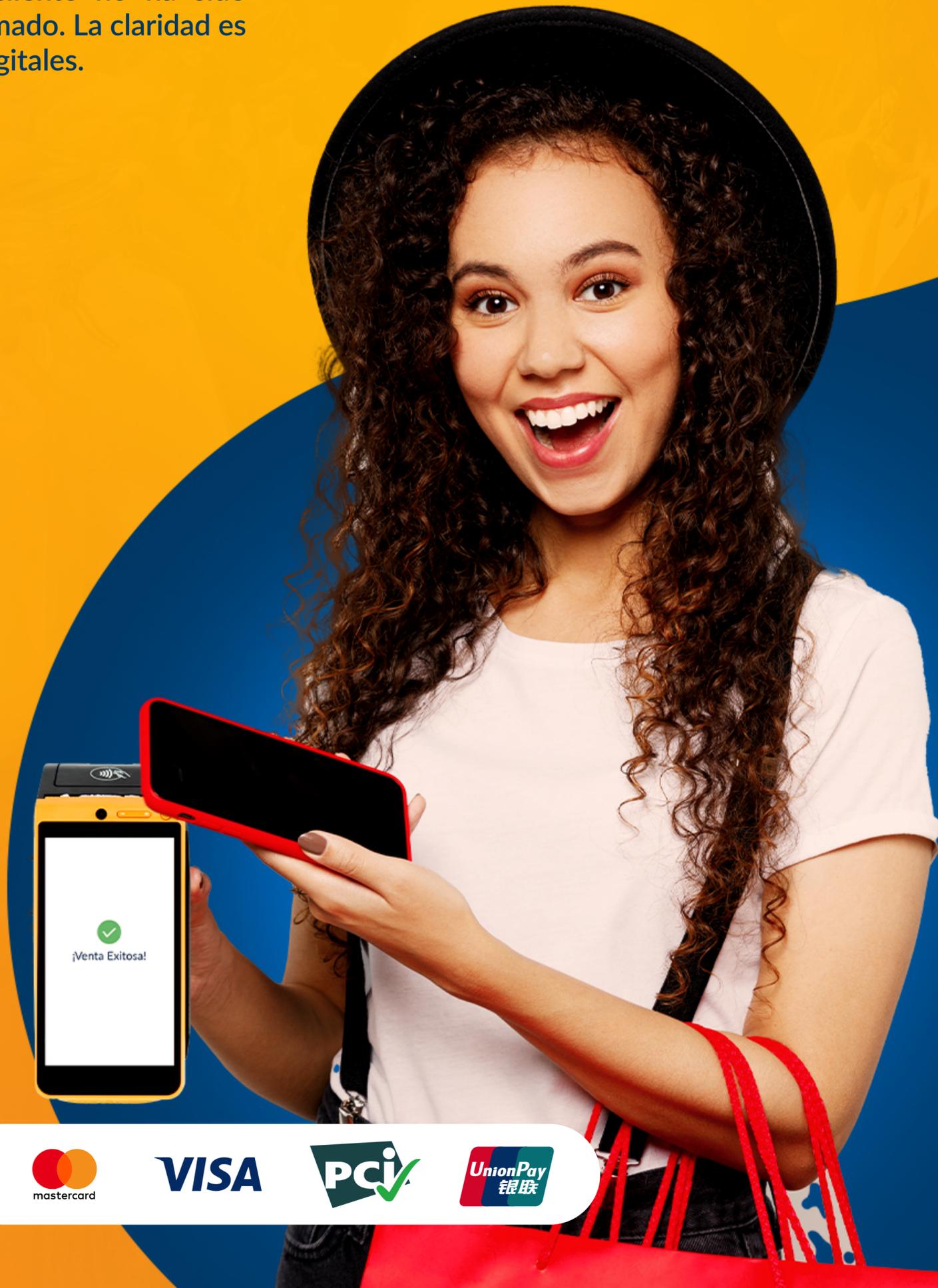
Manipular el teléfono del cliente para procesar un pago digital puede vulnerar su seguridad y confianza. Nunca lo solicites.

✘ No confíes únicamente en capturas de pantalla enviadas por el cliente.

Las capturas pueden ser falsas o manipuladas. Siempre valida el pago directamente en tu sistema o app vinculada a la wallet.

✘ No realices cobros sin consentimiento previo del cliente.

Evita activar cobros automáticos o repetidos si el cliente no ha sido claramente informado. La claridad es clave en pagos digitales.



Medianet S.A. informa a todos los comercios afiliados que, por medio del presente instructivo, da cumplimiento a lo dispuesto en la quinta disposición general de la Resolución Nro. JPRM-2024-018-M. Esta disposición establece lineamientos clave para garantizar la seguridad en los procesos de cobro electrónico y proteger tanto al comercio como al consumidor.

En este sentido, se recuerda que el **dispositivo POS debe estar ubicado de manera que el cliente pueda observar claramente la inserción**, deslizamiento o acercamiento de su tarjeta durante toda la operación. Esta visibilidad es fundamental para generar confianza en cada transacción y evitar cualquier malentendido.

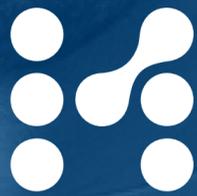
Adicionalmente, el personal encargado del cobro **no deberá manipular la tarjeta o la billetera electrónica del cliente fuera de su campo visual en ningún momento del proceso de pago**. Esta medida busca evitar cualquier posible vulnerabilidad en la gestión de medios de pago electrónicos, reforzando la transparencia en el punto de venta.

Medianet S.A. agradece su atención y compromiso con la implementación de prácticas responsables que refuercen una experiencia de compra segura y confiable para todos los usuarios.

A continuación, compartimos un extracto de la normativa:

QUINTA.- Los partícipes del Sistema Auxiliar de Pagos instruirán permanentemente a los comercios afiliados a su red de pagos que las transacciones presenciales con tarjetas de crédito, débito, prepago o billetera electrónica deberán realizarse a la vista del cliente. El punto de venta (P.O.S.) deberá estar ubicado de manera que el cliente pueda observar claramente la inserción, deslizamiento o acercamiento de su tarjeta. El personal encargado del cobro no deberá manipular la tarjeta o billetera electrónica fuera del campo visual del cliente en ningún momento durante el proceso de pago. Los partícipes del Sistema Auxiliar de Pagos que operen con medios de pago electrónicos y/o billeteras electrónicas mantendrán programas de comunicación permanentes para instruir a sus clientes sobre buenas prácticas de seguridad antes, durante y después del uso de sus medios de pago.





Medianet

Manual de
Venta segura
2025

Para mayor información visita nuestra web

www.medianet.com.ec

Av. Circunvalación entre todos los Santos y
Única. Cdl. Urdesa mz 8 solar 2

PBX:04 3814660

info@medianet.com.ec

Escanea el QR y conoce
más de Medianet

