Seguridad
en ventas presenciales

bold

Contenido de la guía:

Para más información ingresa a: **ayuda.bold.co**

Seguridad en ventas presenciales

¿Por qué debes leer esta guía?

En esta guía encontrarás información sobre los distintos riesgos de fraude que pueden presentarse en las ventas presenciales, donde se hace uso de datáfonos. Este tipo de fraudes podrían afectar tu negocio, por lo que es importante que tengas en cuenta estas recomendaciones que te damos y así puedas evitarlos.

Ten en cuenta que tu negocio asumirá el riesgo de fraude en caso que se verifique la falta de cuidado, la posible falta de diligencia y/o el incumplimiento de alguna de las obligaciones de seguridad descritas en esta guía, en los Términos y Condiciones de Bold y en el Centro de Ayuda de Bold.

Bold podrá abstenerse de abonar recursos a tu cuenta registrada en las siguientes situaciones:

- Cuando la transacción no ha sido autorizada por el titular.
- Cuando la transacción es rechazada por error, fraude o son realizadas con tarjetas robadas, extraviadas o falsas.
- Cuando la firma del comprobante no corresponda con la firma del titular de la tarjeta.
- Cuando la tarjeta de crédito o débito utilizada en la transacción esté vencida, o no sea válida dentro del territorio colombiano.

Tu datáfono Bold es 100% seguro y confiable

El datáfono Bold cumple con los estándares más altos de seguridad. Contamos con todas las certificaciones que nos permiten proteger, almacenar y transmitir de forma segura los datos de tus clientes, durante y después de cada transacción.

Estas son las certificaciones de Bold y su datáfono:

- Visa PIN Security
- Visa PayWave
- EMVCo L1
- EMVCo L2
- Mastercard TQM
- Mastercard PayPass
- PCI PTS 4.x
- PCI DSS 3.2.1 nivel 1
- Mastercard NIV
- Mastercard M-TIP
- Mastercard AETED
- Amex ExpressPay

Recomendaciones para preservar la seguridad de tu datáfono

- No abras el datáfono.
- No introduzcas ningún elemento distinto a la tarjeta en las ranuras del datáfono.
- No uses ningún dispositivo para copiar información de tarjetas.
- No prestes el datáfono a personas que no sean de confianza ni a desconocidos. Debes mantener el control sobre el acceso y el uso de tu datáfono.
- No debes efectuar adaptaciones, reparaciones ni realizar cualquier tipo de manipulación en tu datáfono Bold, directamente o a través de terceros.
- Cuando tu datáfono requiera reparación, inspección, programación, reconfiguración, mantenimiento y/o revisión, ten en cuenta que solo las personas autorizadas por Bold, podrán tener acceso al dispositivo y así garantizar su óptimo funcionamiento en todo momento.
- No permitas que el tarjetahabiente manipule el datáfono cuando se esté procesando la transacción. Únicamente le entregarás el datáfono si la tarjeta solicita clave para procesar el pago.
- Asegurate de configurar de forma adecuada tu datáfono. Puedes revisar el manual de uso o ingresar a ayuda.bold.co.
- No utilices tu datáfono Bold fuera del territorio colombiano.

Fraude con *Skimming*

¿Qué es el *Skimming*?

El *Skimming* es uno de los métodos que utilizan los estafadores para robar información de las tarjetas de tus clientes y posteriormente realizar un fraude.

Todo negocio que utiliza datáfonos está en riesgo de ser víctima del *Skimming*.

Esta situación podría perjudicarte a ti como dueño del negocio, a tus empleados y a tus clientes, provocando pérdidas de ganancias, clientes y que se dañe la reputación y credibilidad de tu negocio.

Tipos de *Skimming*:

***Skimming* tradicional:** se desliza la banda de la tarjeta en un datáfono estándar y cuando el cliente está distraído, la tarjeta se desliza por un dispositivo ilegal para copiar la información de la misma.

Datáfonos ilegalmente modificados: son datáfonos que han sido modificados de manera ilegal, para capturar la información de una tarjeta a través de la banda magnética.

Fraude con *Skimming*

Robo de PIN: Cuando el cliente digita el PIN de su tarjeta, se graba el PIN a través de una cámara pequeña escondida en el datáfono o en elementos cerca al punto de pago como displays. El robo de PIN también puede efectuarse mediante las cámaras de seguridad del establecimiento.

Métodos que utilizan los criminales para hacer *Skimming* en tu negocio:

- Aparentan ser técnicos de datáfonos y te piden una revisión cuando no la has solicitado.
- Intercambian tu datáfono por uno modificado cuando tú o uno de tus empleados se distrae, o también cuando el punto de pago queda desatendido.
- Se llevan tu datáfono y luego te lo entregan modificado de manera ilegal.
- Colocan cámaras escondidas para capturar el PIN de tus clientes en diferentes puntos del comercio.
- Convencen a tus empleados para ser partícipes del *Skimming*.

Conoce las características de tu datáfono

Realiza una inspección diaria

Al inicio de cada turno, revisa el datáfono, sus alrededores y fíjate que:

1. Se vea igual que antes y no esté dañado o maltratado
2. Al conectar el datáfono con la App Bold los últimos 4 dígitos del serial que aparecen en el App correspondan a los 4 últimos del serial que están en la calcomanía del datáfono.
3. El comprobante de pago tenga el nombre de tu comercio **Ver pág. 19**
4. No hayan cámaras ocultas cerca al datáfono, en el techo y/o paredes.

¿Cómo prevenir y evitar el *Skimming* en tu negocio?

Cuida tu datáfono:

- Vigila tu datáfono y no lo pierdas de vista. Protege tu datáfono de la misma forma que cuidas el efectivo.
- Cada vez que debas estar lejos del datáfono, colócalo en un lugar fuera de la vista y alcance de otras personas.
- No permitas que un técnico no autorizado realice una inspección de tu datáfono Bold. En el caso de que tu datáfono presente alguna falla, contáctanos inmediatamente a **soporte@bold.co** para que podamos brindarte una solución.

Alerta y educa tus empleados:

- Alerta y educa a tus empleados acerca de las diferentes modalidades de *Skimming* a las que pueden estar expuestos.
- Enséñales sobre qué hacer en caso de un intento de fraude.
- Establece una señal confidencial específica para alertar un posible fraude.
- Limita el número de empleados que puedan usar el datáfono.
- Asegúrate que todos los empleados que van a utilizar el datáfono sean de confianza y lean esta guía de seguridad.
- Revisa que estén cumpliendo con las normas de seguridad.

Tarjetas de Crédito

mastercard.
Inicia en 5 o 2 y tiene 16 dígitos

VISA
Inicia en 4 y tiene 16 dígitos

Crédito Fácil CODENSA
Inicia en 5 u 8 y tiene 16 dígitos

AMERICAN EXPRESS
Inicia en 3 y tiene 15 dígitos

- Los pagos con tarjetas de crédito pueden ser procesados con el chip insertado en la tarjeta o por medio de la opción *contactless*, siempre y cuando la tarjeta cuente con el símbolo
- Para compras con tarjeta de crédito, es necesario que el cliente presente su documento de identidad y firme el comprobante de pago.
- Las franquicias más comunes que se utilizan para tarjetas de crédito son: MasterCard, Visa, Diners Club y Amex.
- Las tarjetas Visa cuentan con un holograma de una paloma en vuelo y las tarjetas MasterCard cuentan con un holograma que simboliza dos mundos.

Tarjetas Débito (Ahorros o Corriente)

- Las tarjetas débito comparten características físicas con las tarjetas de crédito como el chip, el holograma correspondiente a cada franquicia, entre otros.
- Las franquicias más comunes en las tarjetas de débito son:

maestro VISA Electron VISA Débito

- El nombre del titular de la tarjeta puede estar escrito en relieve o a mano. En algunos casos la tarjeta no tiene el nombre del titular.
- Si la tarjeta tiene la opción de *contactless*, será requerida la clave o PIN cuando la compra supere el monto establecido.
- La Superintendencia Financiera autorizó la eliminación de los siguientes datos del comprobante de venta para tarjetas débito:
  - Firma del cliente
  - Documento de identidad
  - Teléfono
  - Cualquier dato del tarjetahabiente.

Fraude con tarjeta adulterada

La tarjeta adulterada es un plástico auténtico emitido por una entidad financiera, a la cual un tercero le ha modificado la información en el relieve o en la banda magnética. Para identificar estas alteraciones deberás tener en cuenta que:

Frontal

Las letras o números **no** están alineados, ni homogéneos, ni comparten la misma distancia.

El relieve tiene marcas o rayones a su alrededor y tiene vestigios de otros datos en el reverso.

Posterior

Observa la tarjeta por detrás, muchas veces es más fácil detectar las alteraciones que le han hecho, tanto en los números como en las letras.

Así debe verse una tarjeta real Visa

Chip
Está integrado a la tarjeta, **no** es autoadhesivo y **no** se desprende.

Nombre del titular
Deben ser claras y uniformes (pueden venir con o sin relieve).

Contactless

Número de tarjeta
Deben ser claros y uniformes en tamaño y espacio.

Mes y año de vencimiento
mm/aa en ese orden.
Si la tarjeta esta vencida, **no** es válida.

Logo de la franquicia

Panel para firma
Tiene textura al tacto y debe estar firmado. Puede contener los últimos 4 dígitos del número de la tarjeta. Si aparece la palabra VOID-NULA la tarjeta **no** es válida.

Banda magnética
En general es negra. Puede ser de otros colores y puede tener hologramas.

Número de Verificación (CVC o CVV)
Se utiliza solo para ventas no presenciales.

Información comercial del banco

Holograma de la franquicia
Paloma en vuelo.

Así debe verse una tarjeta real Mastercard

Número de tarjeta
Puede empezar con 2 o 5

Contactless

Logo de la franquicia

Panel para firma
Puede contener un estampado y no tener número de la tarjeta.

Banda magnética
Puede ser negra o del mismo color de la tarjeta.

Número de Verificación (CVC o CVV)
Se utiliza solo para ventas no presenciales.

Holograma de la franquicia
Dos mundos entrelazados.
Este holograma también puede ir en la parte frontal de la tarjeta.

Así debe verse una tarjeta real Codensa

Nombre del titular
Suele ser en alto relieve.

Estructura del nombre
1. Primer nombre
2. Inicial del segundo nombre
3. Primer apellido
4. Inicial del segundo apellido

Número de la tarjeta

Mes y año de vencimiento
mm/aa en ese orden.
Si la tarjeta esta vencida, **no** es válida.

Panel para firma

Logo de Colpatria

Banda magnética
Suele ser de color negro.

Número de Verificación (CVC o CVV)
Se utiliza solo para ventas no presenciales.

Estos digítos deben ser iguales a los 4 últimos números de la tarjeta.

Así debe verse una tarjeta real Amex

Código de verificación al frente
Se utiliza solo para ventas no presenciales.

Holograma de la franquicia

Panel para firma
Puede contener el número de la tarjeta y el código de verificación.

Banda magnética
Suele tener hologramas.

Información comercial del banco

Fraude con tarjeta auténtica

Sucede cuando el portador efectúa una compra con una tarjeta de crédito robada o extraviada, que no está bloqueada. Usualmente el portador se puede identificar con un documento de identidad que ha sido hurtado o con una cédula falsa. Para evitar este tipo de fraudes te recomendamos:

- Verificar que el nombre de la tarjeta coincida con el nombre del documento de identidad.
- Comparar las características físicas de la persona que presenta la tarjeta, con la foto del documento de identidad. Si tienes sospechas, pregúntale los datos de la cédula como RH, fecha de expedición, lugar de nacimiento, etc.
- Confirmar que la firma del comprobante sea la misma del documento.
- Si la información no coincide, no recibas pagos con esa tarjeta.

Nombre **Firma** **Características físicas**

Así es una Cédula de Ciudadanía real en Colombia

Imagen obtenida de registraduria.gov.co

Imagen obtenida de registraduria.gov.co

Durante una transacción:

Verifica las características físicas del portador en comparación con la foto del documento que presenta.

Tarjeta integralmente falsa

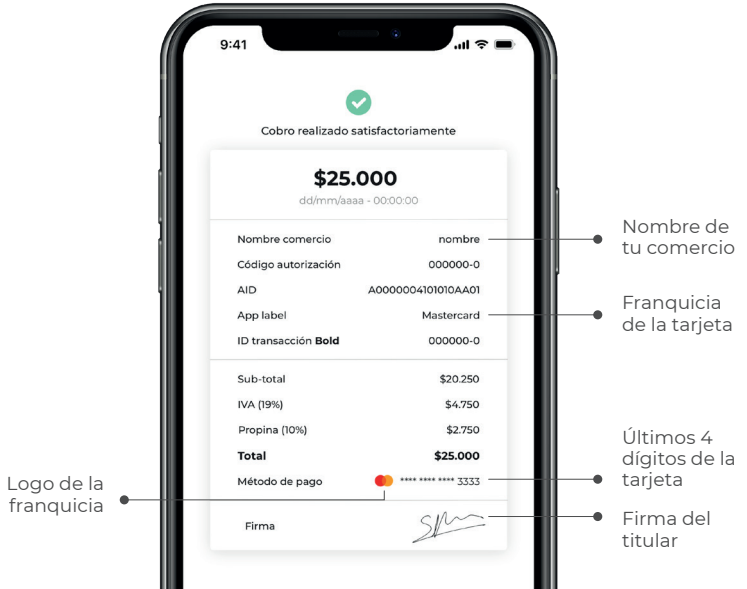
Esta tarjeta cuenta con características similares a los plásticos emitidos por las entidades financieras. Está impresa, grabada y codificada con información, simulando una tarjeta auténtica. Ten en cuenta esto para identificarlas:

- Confronta toda la información que arroje el comprobante.
- Sospecha de tarjetas que tienen colores demasiado vivos o muy desgastados.
- Algunas tarjetas falsas son de muy buena calidad, por lo tanto debes estar atento a los detalles.

Tipos de fraudes con tarjetas

Conoce las partes de tu comprobante de pago Bold

Verifica que coincida la información que arroja el comprobante con los datos de la tarjeta y que la firma coincida con la firma del documento de identidad que presenta el portador.



Cómo identificar un pagador sospechoso

- Es nervioso/ inseguro
- Es irascible
- Olvidó/perdió su documento de identidad
- No es habitual en tu establecimiento
- Es extremadamente amigable
- Compra de afán y llega antes de cerrar
- Te pide dividir el pago en montos bajos para no tener que insertar la clave o PIN

Cuándo reportar un fraude

¿Cuándo debes reportar un fraude?

- Cuando desees nuestra ayuda para confirmar un fraude
- Cuando recibas una propuesta para participar de un fraude
- Cuando detectes acciones sospechosas
- Cuando estés completamente seguro de un fraude.

¿Qué debes hacer ante un fraude con tarjeta?

Ante la sospecha, no recibas el pago. Si después del pago te surge la duda de fraude, escríbenos de manera oportuna (máximo 30 días) a nuestro chat en **www.bold.co** o envíanos un correo electrónico a **soporte@bold.co.** Realiza el monitoreo permanente a tus transacciones y reporta aquellas que puedan ser consideradas sospechosas o inusuales. Las entidades correspondientes podrán realizar las investigaciones y tomar las medidas preventivas o legales que considere pertinentes.

¿Qué debes hacer ante un posible caso de *Skimming*?

Realiza una inspección del datáfono. Apagálo y guárdalo en un lugar seguro. Debes notificarnos inmediatamente para que en Bold podamos bloquear tu cuenta de manera preventiva, mientras realizamos la investigación. Escríbenos a **soporte@bold.co** o a nuestro chat en línea.

Qué hacer en caso de robo o pérdida

En el caso de pérdida o robo de tu datáfono Bold, por favor envíanos un correo a **soporte@bold.co** respondiendo las siguientes preguntas:

- ¿Cuál es el modelo y el número serial del datáfono? **Ver pág. 7**
- Si el datáfono fue robado, ¿en qué lugar sucedieron los hechos?
- Haz un breve resumen de lo que sucedió el día que se robaron o se extravió el datáfono.
- ¿Cuándo te diste cuenta de que el datáfono estaba desaparecido?
- ¿Con qué regularidad utilizabas el datáfono?

Bold procederá a bloquear de manera preventiva el datáfono perdido o robado para tu seguridad.

Recomendaciones para tu negocio y tus empleados

- Capacita al personal de tu establecimiento sobre transacciones seguras con tarjetas.
- Lleva un registro actualizado de las personas que intervienen en el proceso de transacciones con tarjetas.
- Los estafadores buscan ganarse la confianza de los empleados de tu establecimiento, para así convencerlos de participar en un fraude.
- Recuerda que ni tú ni tus empleados, podrán ver el PIN que ingresen tus clientes al datáfono.
- Recuerda que eres responsable por los actos u omisiones de tus empleados, dependientes, administradores y proveedores, en el desarrollo de las actividades de aceptación de tarjetas en tu negocio y en la manipulación del datáfono.
- Establece procesos internos para la prevención y control del riesgo de fraude, relacionados con tus instalaciones físicas, sistemas internos, manejo de personal y servicios que contrates con terceros.
- Los reglamentos de afiliación de franquicias prohíben: fraccionamiento, avances en efectivo, autofinanciamiento, engaño comercial, recargo de comisión; entregar o cambiar al tarjetahabiente dinero en efectivo y cheques, aceptar una tarjeta para cobrar o refinanciar una deuda preexistente, y aceptar un pago para depositar fondos a la cuenta del Comercio.

Recomendaciones para tu negocio y tus empleados

- Exhibe de forma adecuada en tu comercio, local y/u oficina, el material distintivo y promocional de Bold (calcomanías, habladores, cinta, etc.) En caso de uso indebido, Bold podrá exigir la corrección que esté afectando negativamente a la marca.
- No compartas, no intercambies, no divulgues, ni permitas que terceros revisen o manipulen información de los comprobantes de pago ni de las transacciones con tarjetas, a menos que las autoridades pertinentes lo requieran.
- Recuerda que debes conocer y aplicar la ley 1273 de 2009 sobre “la protección de la información y de los datos”.

Garantía

Introducción

La presente garantía tiene un término de seis (6) meses, a partir de la entrega o recolección del datáfono por parte de Bold y puede hacerse efectiva con este documento, en caso de presentarse un defecto de fabricación, siempre y cuando el Comercio haya seguido las recomendaciones de uso que se exponen a lo largo de este documento.

Responsabilidades del Cliente

El datáfono es dado por Bold con el único propósito de que el Comercio acepte pagos con tarjeta de crédito, débito y demás instrumentos de pago electrónico habilitados por Bold. Está prohibido hacer modificaciones al software o hardware del datáfono, excepto cuando sea acordado con Bold o esté permitido por mandato legal.

Responsabilidades de Bold

Durante el periodo de garantía, Bold garantiza que tanto el datáfono como el cable USB incluidos en la caja, están libre de defectos de fabricación que afecten su funcionamiento. La garantía no cubre otros cables, enchufes y en general cualquier otro accesorio. Si el datáfono presenta defectos de fabricación durante el periodo de la garantía, bajo un uso normal y adecuado del mismo, Bold reemplazará o reparará el datáfono o las partes defectuosas del datáfono por piezas, o productos nuevos o reacondicionados que sean equivalentes a los inicialmente entregados; los cuales estarán cubiertos por la garantía durante su periodo de vigencia.

Excluyentes de Responsabilidad

Los presentes términos y condiciones de este documento constituyen el contrato de garantía entre el Comercio y Bold, sobre el datáfono, el cual prevalece ante cualquier acuerdo no escrito y sustituye cualquier acuerdo previo que exista entre las partes. Todo cambio en las condiciones de esta garantía es válido, siempre que conste por escrito y sea aceptado por el Representante legal de Bold.

Bold no se hace responsable de los daños derivados del incumplimiento de las instrucciones que se establezcan en en el documento de Términos y Condiciones, en el manual de uso y en cualquier otro documento proporcionado por Bold sobre manipulación, almacenamiento, instalación, uso y mantenimiento del datáfono; ni de aquellos ocasionados al modificar o intentar reparar el datáfono sin el consentimiento escrito de Bold.

Bold no se hace responsable de ningún daño o defecto en el datáfono causado por el mal uso del mismo o en razón de accidentes, daños intencionados, exceso de humedad, penetración de líquidos, subidas de tensión al momento de conectarse, u otras condiciones ambientales anormales para un entorno de trabajo normal.

En caso de que el datáfono entregado no sea el que el Comercio solicitó o el Comercio identifique que el datáfono viene defectuoso, el Comercio deberá escribir al correo **soporte@bold.co** notificando dicha novedad y seguir el procedimiento de reclamo de garantía indicado a continuación.

Los datáfonos están diseñados y certificados para ser conectados con dispositivos cuyo sistema operativo sea iOS o Android. Tanto los desarrolladores de estos sistemas operativos como las compañías fabricantes de estos dispositivos de comunicación, no se hacen responsables del funcionamiento del datáfono. Se debe tener presente que la utilización del datáfono en estos dispositivos de comunicación, puede afectar el rendimiento del mismo.

Procedimiento de reclamo de la garantía

Para hacer válida la garantía, el Comercio deberá cumplir las siguientes condiciones:

- Contactar al equipo de ayuda de Bold al correo **soporte@bold.co**. Es importante contar con la mayor cantidad de información posible sobre la falla que está presentando el dispositivo, en el momento de contactar al equipo de Bold.
- Proporcionar al equipo de Bold la presente garantía y su factura de compra con el fin de hacer el registro del caso. Con dicho número de registro, el Comercio deberá enviar el dispositivo defectuoso a la dirección de Bold indicada en la página web de la compañía **www.bold.co.**
- En dado caso que la garantía se pueda hacer efectiva, el datáfono será reparado o reemplazado en un periodo de máximo 30 días, desde la fecha en que fue recibido el dispositivo.

Devoluciones

La decisión de reparar el datáfono defectuoso o de reemplazarlo en los términos definidos en el presente documento, será determinada por Bold. En el evento en que el datáfono devuelto por el Comercio funcione correctamente, o se evidencie que los daños provengan del mal uso o de los eventos por los que Bold está exento de responsabilidad; éste será devuelto al Comercio, el cual también deberá correr con los gastos de envío.

En el evento de que el datáfono haya sido reparado o reemplazado por Bold, tendrá la cobertura de la garantía original por el término que falte, antes de que expire.

En el caso de que el datáfono reparado o sometido a mantenimiento presente defectos imputables al técnico de Bold, o responsable de la reparación y/o mantenimiento dentro de los siguientes 30 días calendario contados a partir de la entrega del datáfono al Comercio, éste tendrá derecho a que sea reparado o reemplazado sin costo alguno.

Cuidados del datáfono Bold

- No abras el interior del datáfono.
- No golpees ni dejes caer el datáfono.
- No rocíes agua ni ningún líquido sobre el datáfono ni el teclado.
- Evita que las ranuras y entradas del datáfono se humedezcan.
- Limpia suavemente el datáfono con paño delicado y húmedo. El teclado es sensible al tacto, por lo que si lo limpias con mucha fuerza podrías dañar los sensores y las teclas.
- Evita que el datáfono tenga contacto con líquidos corrosivos (ácido, gasolina, entre otros).
- Mantén el datáfono en un lugar fresco y seco (entre 5 a 45°C, preferiblemente a 22°C), alejado de la contaminación, el sol y el polvo.
- Utiliza siempre el datáfono a un nivel óptimo de carga, para proteger la batería.
- Si no vas a usar el datáfono durante un largo periodo de tiempo, es necesario que cargues la batería a un 70% cada seis meses, y así evites que se dañe.

Accede a nuestro Centro de Ayuda a través de:
ayuda.bold.co
soporte@bold.co

Bold.co S.A.S.
www.bold.co
NIT 901.281.572-4
Bogotá, Colombia