

TABLA DE CONTENIDO

POLÍTICAS PCI DSS Versión 3.2.1.....	3
1. Introducción.....	3
2. Responsabilidades.....	3
3. Generalidades.....	3
4. Prohibiciones.....	4
5. Política de manejo de datáfonos y acceso.....	5
5.1. Propósito.....	5
5.2. Alcance.....	5
5.3. Cargos autorizados para manejo de datáfonos y acceso.....	6
5.4. Obligaciones para los responsables:.....	6
5.5. Revisión y Actualización.....	8
6. Política de manejo de tarjetas y acceso.....	8
6.1. Propósito.....	8
6.2. Alcance.....	8
6.3. Cargos autorizados para manejo de tarjetas y acceso.....	8
6.4. Deberes para el manejo de tarjetas y accesos.....	9
7. Política de manejo de incidentes.....	9
7.1. Propósito.....	9
7.2. Alcance.....	9
7.3. Manejo de incidentes.....	10
7.3.1. Incidentes con tarjetas.....	10
7.3.1.1. Abandono de tarjeta de pago en el comercio:.....	10
7.3.1.2. Doble transacción, fallida y/o por valor errado:.....	11
7.3.1.3. Reclamaciones por sospechas de fraude:.....	11
7.3.2. Incidentes con dispositivos (datáfonos):.....	12
7.3.2.1. Pérdida o robo del dispositivo:.....	12
7.3.2.2. Daño del dispositivo:.....	12
7.3.2.3. Alteración del dispositivo:.....	13
7.3.3. falla en la conexión:.....	13
7.3.3.1. Comunicación y Notificación.....	13
7.3.4. falla en la conexión WiFi – Servidor - Redes.....	13
7.3.4.1. Comunicación y Notificación.....	13
8. Política de contratación de proveedores.....	14
8.1. Propósito.....	14
8.2. Alcance y Aplicabilidad.....	14
8.2.1. Alcance:.....	14
8.2.2. Cumplimiento con PCI DSS:.....	14
8.3. Selección de Proveedores.....	14

8.3.1. Evaluación de Proveedores.....	14
8.3.2. Requisitos Contractuales:.....	15
8.4. Evaluación de Conformidad:.....	15
8.5. Cambios en la Relación con el Proveedor:.....	15
8.5.1. Notificación de Cambios:.....	15
8.5.2 Evaluación de Cambios:.....	15
8.6. Cumplimiento Continuo:.....	16
8.6.1. Monitoreo Continuo:.....	16
8.6.2. Actualizaciones de AOC:.....	16
8.6.3. Actualización del inventario de proveedores.....	16
8.7. Responsabilidades:.....	16
8.7.1. Responsabilidades del Proveedor:.....	16
8.7.2. Responsabilidades de la Organización:.....	16
8.8. Auditoría Interna:.....	16
9. Política de entrenamiento y Concienciación.....	16
9.1. Propósito.....	16
9.2. Alcance.....	17
9.3. Entrenamiento Inicial y continuidad.....	17
9.4. Campañas de Concienciación.....	17
10. Política de no almacenamiento de datos de autorización de pago.....	17
10.1. No Almacenamiento de Datos Sensibles:.....	17
10.2. Procesamiento Seguro:.....	17
10.3. Transparencia con los Clientes:.....	17
10.4. Eliminación Inmediata:.....	17
10.5. Acceso Restringido:.....	18
11. Revisión y Actualización.....	18
12. Glosario de términos.....	18
13. Bibliografía.....	19
14. Sanción:.....	19
15. Aprobación:.....	19
16. Control de cambios:.....	20

POLÍTICAS PCI DSS Versión 3.2.1

1. Introducción

COMBUSTIBLES DE COLOMBIA S.A. pone a disposición de los miembros de la Junta Directiva, Accionistas, Colaboradores y a quienes representa, proveedores, visitantes, clientes y prospectos, política de manejo de datáfonos, política de manejo de tarjetas de crédito, política de manejo de incidentes, política de proveedores.

5. Política de manejo de datáfonos y acceso

5.1. Propósito

El propósito de esta Política de manejo de datáfonos y acceso, es establecer las obligaciones y procedimientos para garantizar que el acceso a los dispositivos que manejan datos de tarjetas de pago esté restringido a personal autorizado y que se implementen controles de seguridad adecuados para proteger la confidencialidad e integridad de la información de tarjetas de pago.

Así mismo, se busca establecer un enfoque estructurado y coherente para identificar, responder, mitigar y documentar los incidentes de seguridad de la información relacionados con los datos de los datáfonos.

5.2. Alcance

Esta política se aplica a todos los dispositivos (datáfonos) que procesan, transmiten datos de tarjetas de pago. Todos los empleados, contratistas y terceros que interactúan con estos dispositivos deben cumplir con las disposiciones de esta política.

5.3. Cargos autorizados para manejo de datáfonos y acceso

- Vendedor isla - Islero
- Vendedor tienda - cajero
- Técnico Goodyear
- Administrador Goodyear
- Coordinador Operativo
- Administrador
- Asistente
- Servicio al cliente
- Lubricador

- Pilo entrenador

5.4. Obligaciones para los responsables:

- A. Se debe llevar un registro de los accesos a los dispositivos que manejan datos de tarjetas de pago. El registro debe contener información sobre el usuario, la fecha y hora del acceso, así como la actividad realizada.
- B. Se debe llevar un registro de todos los cambios realizados en la configuración de los dispositivos que manejan datos de tarjetas de pago, siguiendo el **Procedimiento de administración, custodia, manejo y accesos de dat...**
- C. Los datáfonos se protegen de captura de datos de tarjetas de pago, mediante la ubicación en áreas autorizadas y seguras cubiertas por el CCTV, con controles físicos (ubicados en cuartos seguros) para limitar el acceso no autorizado a estos dispositivos. El acceso a este sitio está bajo la responsabilidad del Administrador y/o Asistentes de la estación de servicio.
- D. Mantener actualizado el inventario control de los dispositivos (fecha, mes, centro de operación, movimiento, ubicación, franquicia, código único, terminal, marca, modelo, serial, cantidad, observación y destino) en el formato definido (**DATAFONOS COMBUSCOL**). Este debe ser revisado mínimo una vez al año.
- E. El personal nuevo, antes de manipular los dispositivos, recibe la respectiva capacitación y firma aceptación en formato de aceptación y recibido del procedimiento de administración, custodia, manejo y accesos de datáfonos. Esta capacitación se debe hacer al menos una vez al año.
- F. Inspeccionar los dispositivos diariamente al iniciar la jornada para buscar intentos de alteración o sustitución en el formato definido: Formato de datafonos **Formato chequeo datafonos** .
- G. Capacitar al personal para que detecten comportamientos sospechosos e informen la alteración o sustitución de dispositivos, al menos una vez al año.
- H. Para identificar que los funcionarios sean los autorizados para la manipulación de las tarjetas de pago y/o dispositivos de pago que puedan procesar datos del tarjetahabiente, estos deben portar el carnet de identificación en un lugar visible, además de ello, deben contar con su adecuado uniforme corporativo.
- I. Los datáfonos deben permanecer guardados o cargando en las zonas marcadas y asignadas por el administrador que cumplan con lo siguiente:
 - a. Ubicados en un cuarto con cámara dentro del CCTV.

- b. Ubicados en una superficie plana que les de estabilidad
 - c. Tener disponible tomacorriente dentro de la zona de videovigilancia para cargar allí los dispositivos.
- J. Antes de realizar la autorización para el acceso a los datáfonos, el administrador debe:
- a. Identificar plenamente a los funcionarios que van a tener acceso a los datafonos
 - b. Solicitar carnet de identificación
 - c. Confirmar los funcionarios y el servicio que se va a ejecutar, llamando a las líneas telefónicas autorizadas (Credibanco y Redeban).
 - d. Presenciar o delegar la inspección de los datafonos en el momento del servicio y evidenciar que los sellos no sean levantados.
 - e. Los funcionarios de Credibanco y Redeban realizan un acta de inspección dejando evidencia del trabajo realizado; este documento debe ser archivado por el administrador de la EDS en la carpeta del DRIVE correspondiente a la estación SOPORTES DE MANTENIMIENTO DE PROV DE RED.

5.5. Revisión y Actualización

Esta política será revisada y actualizada mínimo una vez al año, para asegurar su efectividad y cumplimiento continuo con los requisitos de la norma PCI DSS versión 3.2.1.

6. Política de manejo de tarjetas y acceso

6.1. Propósito

El propósito de esta Política de manejo de tarjetas y acceso, es establecer las directrices y procedimientos para garantizar que el acceso a las tarjetas de pago esté restringido a personal autorizado de COMBUSTIBLES DE COLOMBIA S.A. y que se implementen controles de seguridad adecuados para proteger la confidencialidad e integridad de la información de tarjetas de pago.

Así mismo, se busca establecer un enfoque estructurado y coherente para identificar, responder, mitigar y documentar los incidentes de seguridad de la información relacionados con datos de tarjetas de pago.

6.2. Alcance

Esta política se aplica a todas las tarjetas que se procesan y los funcionarios autorizados a su manejo.

6.3. Cargos autorizados para manejo de tarjetas y acceso

- Vendedor isla - Islero
- Vendedor tienda - cajero
- Técnico Goodyear
- Administrador Goodyear
- Coordinador
- Administrador
- Asistente
- Servicio al cliente
- Lubricador
- Pilo entrenador

6.4. Deberes para el manejo de tarjetas y accesos

- A. En una transacción con medio de pago tarjeta, siempre se debe realizar en presencia del tarjetahabiente, presentando documento de identidad y la tarjeta.
- B. Solicitar y verificar el documento de identidad y la tarjeta de pago en caso de ser tarjeta de crédito antes de la transacción.
- C. Revisar que el nombre del titular de la tarjeta de crédito coincida con el nombre del documento de identidad.
- D. Validar, al momento de la transacción los 4 últimos números de la tarjeta, fecha de vencimiento, tipo de tarjeta, franquicia o marca.
- E. Verificar que la firma en el comprobante coincida con la firma registrada en el panel al respaldo de la tarjeta.
- F. Verificar que el número de cédula en el comprobante coincida con el del documento de identidad.
- G. Mantener al personal de su establecimiento capacitado.
- H. El Administrador de la estación realiza monitoreo de transacciones de manera aleatoria para detectar posibles fraudes o actividades sospechosas.

- I. Los usuarios del alcance deben cumplir a cabalidad el
- Procedimiento de Manejo de tarjetas de crédito y_o débito.pdf

7. Política de manejo de incidentes

7.1. Propósito

El propósito de esta política de manejo de incidentes, es establecer las directrices y procedimientos para garantizar que todos los incidentes sean tratados de manera oportuna y efectiva para minimizar el riesgo y el impacto en la confidencialidad, integridad y disponibilidad de la información de tarjetas de pago.

Así mismo, se busca establecer un enfoque estructurado y coherente para identificar, responder, mitigar y documentar los incidentes de seguridad de la información relacionados con datos de tarjetas de pago.

7.2. Alcance

Esta política se aplica a todas las tarjetas y datáfonos que se procesan así como a todos los funcionarios autorizados para su manejo.

Los funcionarios del alcance deben cumplir con el

- Procedimiento de manejo de incidentes, recuperación y continuidad del nego...

7.3. Manejo de incidentes

7.3.1. Incidentes con tarjetas

Los incidentes presentados en el turno con las transacciones, dispositivos (datáfonos) o alguna inconformidad de clientes, se debe informar de manera oportuna al jefe inmediato.

7.3.1.1. Abandono de tarjeta de pago en el comercio:

Puede ocurrir cuando se hace una transacción dentro del establecimiento y por error humano del cliente y/o alguno de los responsables la tarjeta de pago se queda en la estación y el cliente ya no se encuentra allí.

- Los únicos funcionarios de Combuscol autorizados para hacer la custodia de la tarjeta olvidada, son el ADMINISTRADOR, ASISTENTE Y COORDINADOR OPERATIVO.
- Si la tarjeta de crédito y/o débito es encontrada por un funcionario distinto a los anteriormente mencionados, este tendrá que informar de inmediato a los funcionarios autorizados.
- Si en el momento están ausentes estos funcionarios autorizados, el funcionario tendrá que depositar la tarjeta en un sobre de

consignación, con copia del tiquete de compra (si aplica), hora y fecha en que se la encontró.

- Ningún funcionario de Combuscol podrá almacenar, copiar, transcribir y/o utilizar, de ninguna forma, la banda magnética, el chip de la tarjeta y/o los datos completos de la misma, con fines económicos, comerciales y/o algún otro fin lucrativo. Sin embargo, serán el ADMINISTRADOR y/o COORDINADOR, los únicos funcionarios que podrán utilizar la información de la tarjeta (número y nombre impreso en la misma) para hacer la verificación de la propiedad de la misma, si hay reclamo por parte del propietario de la tarjeta.
- Seguir el procedimiento de responsabilidad de escalamiento ante incidentes para con ello dar cumplimiento al **■ Procedimiento de manejo de incidentes, recuperación y contin...**
- Después de realizar el procedimiento, si la tarjeta no ha sido reclamada por el cliente, después de 15 días hábiles, pasado este tiempo la tarjeta será destruida según el **■ Procedimiento de manejo de incidentes, recuperación y contin...**
- Modo para destrucción de la tarjeta: La tarjeta debe ser destruida con tijeras, de tal forma que la siguiente información quede destruida: número de tarjeta, fecha de vencimiento, chip, código de seguridad y banda magnética. Una vez hecho esto, se deja acta de la destrucción, donde se relaciona el tipo de tarjeta, entidad bancaria, los últimos 4 dígitos del número de la tarjeta y tarjeta habiente.

7.3.1.2. Doble transacción, fallida y/o por valor errado:

Esta situación se presenta cuando al terminar la transacción la copia del voucher no se imprime, ya sea por falla en la comunicación con la entidad bancaria, por falla del dispositivo datáfono o error en la digitación por parte del funcionario responsable de la transacción.

- Diligenciar el formato PQR con los datos del cliente, nombre, cédula y detalle de lo ocurrido.
- Enviar al área de contabilidad y servicio al cliente el formato de PQR, para iniciar los procesos de validación y verificación, en la plataforma bancaria e identificar si la transacción fue efectiva o declinada, en este caso nunca se debe enviar la información completa del PAN del cliente, solamente los último 4 dígitos del número y entidad bancaria de la tarjeta de la novedad.

- Seguir el
■ Procedimiento de manejo de incidentes, recuperación y contin...
para dar solución a este incidente.

7.3.1.3. Reclamaciones por sospechas de fraude:

Este incidente ocurre cuando por parte del tarjetahabiente hace una reclamación por sospecha de fraude ante la entidad INCOCREDITO, y está a su vez inicia una investigación con el establecimiento implicado, con el fin de tener las pruebas de las transacciones en sospecha y dar respuesta al cliente.

- Guarda los comprobantes de pago y los registros de transacciones como respaldo en caso que sea necesario presentar una reclamación o disputa por parte de Incocredito.
- En ningún caso solicitar al cliente la información completa del PAN, solamente los últimos 4 dígitos del número de la tarjeta y el nombre de la entidad bancaria de la tarjeta que presentó la novedad.
- Seguir el
■ Procedimiento de manejo de incidentes, recuperación y contin...
para dar solución a este incidente.

7.3.2. Incidentes con dispositivos (datáfonos):

7.3.2.1. Pérdida o robo del dispositivo:

Hace relación a las situaciones en las que se extravía un dispositivo datáfono, ya sea porque por error algún cliente se lo lleva, o por un acto delictivo en donde el responsable de su tenencia fue víctima.

- En caso de pérdida o robo de un datáfono, se debe comunicar de inmediato al proveedor (Redeban o Credibanco) para informarles sobre la situación y solicitar su asistencia en la resolución del problema y bloqueo del mismo.
- Se debe notificar a las autoridades locales para que puedan tomar medidas y recuperar el dispositivo realizando los respectivos bloqueos del equipo (Denuncio)

7.3.2.2. Daño del dispositivo:

Ocurre cuando por mala manipulación o por error del sistema del dispositivo datáfono, genera fallas que afectan el normal funcionamiento de las transacciones que allí se ejecutan.

- Informar al administrador inicialmente.
- El administrador utilizará los siguientes canales de comunicación:

REDEBAN

- Línea nacional 018000931022
- Bogota (601) 3078205 -332 32 00- 560 04 70- 332 25 00
Cali 660 85 25 Medellín 355 60 05 Barranquilla 369 61 61
- A través ChatBot Carla 3125087080
- servicio.cliente@rbm.com.co
- A través de la App RedeAPP

CREDIBANCO

- Línea nacional 6013278690 – 018000975806
- Línea Whatsapp asistente virtual PABLO
<https://www.credibanco.com/>
- <https://www.credibanco.com/pqrs-centro-de-ayuda/>

7.3.2.3. Alteración del dispositivo:

Hace relación a las situaciones en las que algún datafono presenta alteraciones tales como daño en pantalla, teclado, equipo golpeado, anomalías en la programación del equipo:

- En caso de identificar alguna alteración de un datáfono, se debe comunicar de inmediato al jefe inmediato inicialmente.
- El administrador debe reportar al proveedor (Redeban o Credibanco) para informarles sobre la situación y solicitar su asistencia en la resolución del problema.

7.3.3. falla en la conexión:

Ocurre cuando la señal es inestable y el dispositivo no procesa las transacciones, en este caso el administrador, con apoyo de tecnología, deben cambiar la red.

Los vendedores deben realizar el proceso de prueba de comunicación (HECHO TEST) confirmando si la transacción fue exitosa o no.

Si el problema persiste, se escala la novedad con el operador de servicios de la red en los canales de comunicación autorizados.

7.3.3.1. Comunicación y Notificación

- a. Se notificará a las partes interesadas internas relevantes sobre el incidente de acuerdo con los procedimientos de notificación establecidos.

b. Se notificará a las entidades bancarias pertinentes, proveedores de servicios de pago y autoridades reguladoras, según lo requiera la normativa aplicable y la gravedad del incidente.

7.3.4. falla en la conexión WiFi – Servidor - Redes

En el caso que las transacciones propias de Combustibles de Colombia S.A, no funcionen, se determinará que la falla corresponde a Tecnología, por tanto, el Administrador, Asistente y/o Coordinador, informará a los siguientes funcionarios:

7.3.4.1. Comunicación y Notificación

a. Se notificará a las partes interesadas internas relevantes sobre el incidente de acuerdo al plan de respuesta a incidentes.

8. Política de contratación de proveedores

8.1. Propósito

Establecer requisitos y expectativas para la contratación y gestión de proveedores que manejan información de tarjetas de pago en cumplimiento con los estándares de la PCI DSS.

8.2. Alcance y Aplicabilidad

8.2.1. Alcance:

Esta política se aplica a todos los proveedores que procesan, almacenan o transmiten información de tarjetas de pago en nombre de nuestra organización.

8.2.2. Cumplimiento con PCI DSS:

Todos los proveedores deben cumplir con los requisitos de la Norma PCI DSS y proporcionar evidencia de su conformidad mediante un AOC.

8.3. Selección de Proveedores

8.3.1. Evaluación de Proveedores

8.3.1.1. Cumplimiento de vinculación de proveedores:

Se cuenta con el manual 02. Manual de procedimientos de gestión del riesgo LAFT-FPADM V.5, el cual cita el Procedimiento de vinculación de proveedores y contratistas V3.en la página 16 y 17, punto 6.1.4 "política de conocimiento y vinculación de contrapartes"

Procedimiento corporativo de COMBUSTIBLES DE COLOMBIA S.A., para el ingreso de cualquier proveedor persona jurídica o natural.

8.3.1.2. Certificación AOC del proveedor:

Para garantizar que la AOC se encuentre actualizada, se solicitará, esta verificación estará a cargo del Jefe de Tecnología, y se realizará anualmente en el mes de agosto con esta información se actualizará el inventario de proveedores.

8.3.1.3. Contrato

El contrato está clasificado como contrato de tipo, por tanto, no requiere de firma por las partes, sino que es general para los establecimientos de comercio que realizan pagos a través de datáfonos.

8.3.1.4. Alianzas comerciales

En caso de existir alianzas estratégicas con las productoras de transacciones el Director Administrativo y Financiero, verificará el contrato y garantizará que esté acorde con lo pactado.

8.3.1.5. Otrosí.

En caso de existir Otrosí con las productoras de transacciones el Director Administrativo y Financiero deberá cumplir con los mismos lineamientos que se mencionan para las Alianzas Comerciales.

8.3.2. Requisitos Contractuales:

El contrato tipo son los que actualmente se trabaja con las procesadoras de paga, es replicable a todos los clientes porque el tipo de servicio no requiere distinciones entre un cliente u otro, por tanto, se debe verificar su publicación y colocar la evidencia de esta revisión en la **unidad compartida PCI archivos y soportes**. Igualmente en este sitio debe estar el **AOC** con fecha vigente de cada uno de los proveedores de pago. Será responsabilidad del Director Administrativo y Financiero.

8.4. Evaluación de Conformidad:

8.4.1. Revisión de AOC:

Los proveedores deben proporcionar un AOC válido y actualizado como parte del proceso de evaluación de conformidad, que será solicitado y revisado anualmente.

8.5. Cambios en la Relación con el Proveedor:

8.5.1. Notificación de Cambios:

Los proveedores deben notificar de inmediato cualquier cambio en su entorno operativo que pueda afectar su conformidad con la PCI DSS.

8.5.2 Evaluación de Cambios:

La organización evaluará cualquier cambio en la relación con el proveedor para garantizar que no se comprometa la seguridad de la información de tarjetas de pago.

8.6. Cumplimiento Continuo:

8.6.1. Monitoreo Continuo:

La organización implementará un programa de monitoreo continuo para evaluar el cumplimiento continuo del proveedor con la PCI DSS.

8.6.2. Actualizaciones de AOC:

Los proveedores deberán proporcionar actualizaciones periódicas del AOC para reflejar cualquier cambio en su entorno operativo.

8.6.3. Actualización del inventario de proveedores.

La organización revisará y actualizará anualmente el inventario de proveedores que se encuentra en la unidad compartida PCI - archivos y soportes.

8.7. Responsabilidades:

8.7.1. Responsabilidades del Proveedor:

Los proveedores son responsables de mantener y demostrar el cumplimiento continuo con la PCI DSS.

8.7.2. Responsabilidades de la Organización:

La organización es responsable de la supervisión y gestión efectiva de los proveedores para garantizar la seguridad de la información de tarjetas de pago.

9. Política de entrenamiento y Concienciación

Se proporcionará formación al menos una vez al año a todos los empleados y contratistas para aumentar la concienciación sobre las políticas de manejo en tarjetas y dispositivos, fomentando la comprensión de los procedimientos, y siguiendo el

■ [Procedimiento para entrenar al personal.pdf](#)

9.1. Propósito

El objetivo de esta política es establecer un marco para el entrenamiento continuo y la concienciación sobre las políticas PCI DSS entre los funcionarios abarcados dentro del alcance.

9.2. Alcance

Esta política se aplica a todos los empleados autorizados para el manejo de tarjetas de pago y datáfonos.

9.3. Entrenamiento Inicial y continuidad

Todos los nuevos empleados recibirán orientación sobre los requisitos y obligaciones de la certificación PCI DSS durante su proceso de inducción, acorde al [Procedimiento para entrenar al personal.pdf](#)

De igual manera se cumple con el cronograma de capacitaciones anual establecido en [Cronograma de capacitación PCI 2024](#) para el personal autorizado dentro del alcance.

9.4. Campañas de Concienciación

Se llevarán a cabo campañas de concienciación regulares para destacar la importancia de la seguridad de la información de tarjetas de pago, datafonos y fomentar una cultura de seguridad.

10. Política de no almacenamiento de datos de autorización de pago

Esta política establece nuestro compromiso de no almacenar datos de autorización de pago y describe las medidas que tomamos para garantizar la confidencialidad y protección de dicha información.

10.1. No Almacenamiento de Datos Sensibles:

En ningún momento almacenaremos información sensible de autorización de pago, incluyendo, pero no limitándose a, números de tarjetas de crédito, fechas de vencimiento, códigos de seguridad u otra información asociada a las transacciones financieras.

10.2. Procesamiento Seguro:

Cualquier información relacionada con la autorización de pago será procesada de manera segura y cumpliendo con los estándares de seguridad de la industria.

10.3. Transparencia con los Clientes:

Informaremos a nuestros clientes de manera clara y transparente sobre nuestras prácticas de gestión de datos, incluyendo la no retención de información de autorización de pago.

10.4. Eliminación Inmediata:

Los funcionarios de la empresa deben eliminar inmediatamente cualquier información que pueda ser recibida con datos de transacciones de pago, de cualquiera de los medios de comunicación en el que se reciba.

10.5. Acceso Restringido:

El acceso a la información de autorización de pago estará restringido a personal autorizado dentro del alcance y capacitado para manejar dicha información.

11. Revisión y Actualización

Esta política será revisada y actualizada al menos una vez al año, para asegurar su relevancia y efectividad en respuesta a cambios en el entorno de seguridad de la información.

Esta Política se considera un documento vivo y su cumplimiento es obligatorio para todos los empleados y partes involucradas en el manejo de datos de tarjetas de pago. La Dirección comercial y operativo es responsable de asegurar la adhesión a esta política y de proporcionar los recursos necesarios para su implementación efectiva.

Estas políticas serán publicadas en la intranet de la compañía intranet.combuscol.co, donde se encuentran actualizadas para su consulta, de igual forma, cualquier cambio en la política será informado a través de correo electrónico para que los funcionarios puedan conocer las nuevas directrices.

12. Glosario de términos

PCI DSS: (Payment Card Industry Data Security Standard) es el Estándar de Seguridad de Datos para la Industria de Tarjeta de Pago creado como un instructivo de obligatorio cumplimiento para las organizaciones que procesan, almacenan y/o transmiten datos de tarjetahabientes (o titulares de tarjeta), a asegurar dichos datos, con el fin de evitar los fraudes que involucran tarjetas de pago débito y crédito.

Tarjeta débito: es un instrumento financiero relacionado con una cuenta bancaria, que permite operar con la entidad a través de cajeros automáticos (consultar saldos, realizar depósitos o extracciones de efectivo, pagar servicios, y enviar transferencias entre otras operaciones).

Tarjeta crédito: Es un medio de pago que te permite hacer compras y cancelar el valor posteriormente. Es “de crédito” porque la suma de dinero que usas cuando haces una compra, corresponde a un préstamo que te otorga la entidad financiera.

PAN : PAN o número de tarjeta es el acrónimo de "Personal Account Number" y no es otra cosa que el número que aparece en el anverso de las tarjetas de pago, ya sean de crédito, débito, virtuales o prepago.

Datáfono: Un datáfono es un dispositivo que, instalado en un establecimiento comercial o tienda, permite cobrar a sus clientes (por red telefónica, o IP vía GSM, GPRS, Wi-Fi, etc.) mediante tarjeta de crédito o débito. Normalmente el datáfono de un comercio es proporcionado por el banco con el que trabaja.

Tarjetahabiente: Es el nombre que recibe el usuario de una tarjeta de crédito y débito.

Incidente de Seguridad: Cualquier evento que pueda comprometer la confidencialidad, integridad o disponibilidad de los datos de tarjetas de pago, incluidos, entre otros, el acceso no autorizado, la pérdida o robo de dispositivos que contienen datos de tarjetas de pago.

Equipo de Respuesta a Incidentes (IRT): Grupo designado para coordinar la respuesta y mitigación de los incidentes de seguridad de la información relacionados con datos de tarjetas de pago.

CCTV: Circuito cerrado de televisión. Es una tecnología de videovigilancia diseñada para supervisar las actividades y lugares claves de los establecimientos de la empresa.

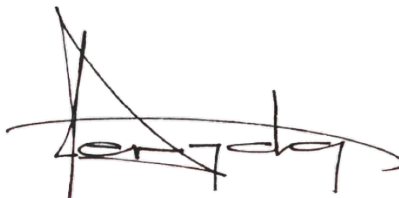
13. Bibliografía

- [https://docs-prv.pcisecuritystandards.org/SAQ%20\(Assessment\)/SAQ/PCI-DSS-v3-2-1-SAQ-B-r2.pdf](https://docs-prv.pcisecuritystandards.org/SAQ%20(Assessment)/SAQ/PCI-DSS-v3-2-1-SAQ-B-r2.pdf)
- <https://www.incocredito.com.co/>

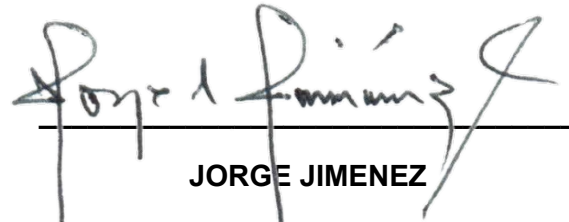
14. Sanción:

Por incumplimiento de las políticas, funciones y procedimientos del cargo conforme a la circular normativa, manual de funciones y procedimientos, código de conducta y reglamento interno de trabajo dependiente del impacto económico, operación y de imagen y de acuerdo a la gravedad del incumplimiento; el jefe inmediato aplicará los correctivos y medidas correspondientes de acuerdo al reglamento interno de trabajo.

15. Aprobación:



Cesar Ayala Pizano
DIRECTOR OPERATIVO



JORGE JIMENEZ

DIRECTOR FINANCIERO Y ADMINISTRATIVO

16. Control de cambios:

CONTROL DE CAMBIOS		
Versión	Fecha	Justificación de la versión
2	04/01/2024	Actualización
3	05/01/2024	Actualización incidente WiFi-Servidor-Redes
4	15/02/2024	Actualización bibliografía, inclusión de políticas
5	20/2/2024	Actualización a la política de contratación de proveedores