**Medellín, 27 de enero de 2026**

RAD-VSP-E-26-0008

Señora:

**Adriana Maria Zuluaga Gomez**

COBELEN

Ciudad Medellín

**Asunto:** Certificado Cumplimiento Circular 036 de la Superintendencia de Economía Solidaria.

Adriana Maria Zuluaga Gomez:

Para nosotros es grato poder estar de la mano de las entidades aliadas como lo es COBELEN, en el proceso y crecimiento de la organización, a través de la prestación de servicios eficientes y competitivos con las exigencias actuales del mercado.

Respecto a la solicitud de la certificación para el cumplimiento de la circular 036 emitida por la Superintendencia de Economía Solidaria, damos constancia que Visionamos como Sistema de Pago Cooperativo, actualmente cuenta con las siguientes certificaciones:

- **ISO/IEC 27001:2022**
- **PCI – DSS V 4.0.1**

En lo que corresponde al estándar **ISO/IEC 27001:2022**, Visionamos cuenta con un Sistema de Gestión de Seguridad de la Información “SGSI”, contemplado dentro de dicho sistema todo un Gobierno de seguridad soportado en Políticas, Planes, procedimientos, roles y perfiles, procesos y lo más importante los respectivos controles tecnológicos que exige el Anexo A.

Adicional al SGSI, Visionamos cumple con los requisitos que exige la certificación internacional **PCI – DSS V 4.0.1**, para la industria de tarjetas de pago.

Visionamos cuenta con un plan de continuidad para asegurar la prestación de los servicios críticos del negocio a las entidades participantes, el cual contiene procedimientos, sistemas y recursos necesarios para operar en contingencia y retornar a la operación normal, en caso de indisponibilidad o falla total de las instalaciones del centro de cómputo principal, ubicado en la ciudad de Medellín. Durante el año 2025 el referido plan fue sometido a las pruebas

correspondientes, las cuales arrojaron resultados satisfactorios. Los mencionados ejercicios de continuidad contemplaron los siguientes aspectos, que soportan la disponibilidad de los diferentes servicios y canales utilizados por los clientes de Visionamos:

- Prueba de traslado e instalación del equipo de recuperación en el centro alterno de trabajo.
- Prueba de traslado y operación desde el sitio de procesamiento alterno.

Es importante aclarar que Visionamos no adelanta pruebas con cada una de las entidades, pues, nuestro Plan de Continuidad está orientado a mantener la continuidad de nuestros servicios para todas nuestros clientes.

Además, contamos los siguientes objetivos de recuperación ante desastres:

- RTO (*Objetivo de Tiempo de Recuperación)* de 0-4 horas, tiempo en que puede tardar en restablecerse un servicio o sistema crítico.
- RPO (*Objetivo de Punto de Recuperación)* de 1 hora, el tiempo en que se puede perder datos sin afectar gravemente las operaciones.

**Seguridad en la Comunicación:**

- **Algoritmos y protocolos de seguridad**

VISIONAMOS — PROCESO ASEGURAMIENTO Y MEJORA / SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN
POLÍTICAS ESPECÍFICAS DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

RESTRINGIDA

**3.4.1. CONTROLES CRIPTOGRÁFICOS ESTABLECIDOS.**

- La información que contenga contraseñas debe ser cifrada para su protección; no debe ser almacenada en texto plano.
- El acceso a los sistemas de información siempre se realizará por medio de protocolos seguros SSH, HTTPS.
- La comunicación e intercambio de información entre VISIONAMOS y sus clientes, colaboradores y proveedores siempre se realizará a través de canales seguros cómo son por ejemplo conexiones Correo Corporativo, SFTP, VPN Sitio a Sitio, VPN Cliente a Sitio.
- Se implementarán para el cifrado de información algoritmos de cifrado robustos, mínimo SHA256 y AES 256. VISIONAMOS se acoge a la política de cifrado de sus clientes teniendo como mínimo aceptable los algoritmos antes mencionados.
- Para las redes inalámbricas en las instalaciones de VISIONAMOS se implementará como mínimo WPA2/PSK AES.

**3.4.2. LINEAMIENTOS PARA LA GESTIÓN DE LLAVES.**

**3.4.2.1. ESCENARIO DE CIFRADO.**

- **CIFRADO EN TRÁNSITO:** La Plataforma de la entidad cuenta con certificados de seguridad SSL instalados en los servidores para todos los ambientes - Desarrollo, Laboratorio y Producción. Esto garantiza que la información no puede ser interceptada para su eventual alteración o modificación durante su tránsito.
- **CIFRADO EN REPOSO:** La información crítica proporcionada por los clientes es cifrada en las cuentas de almacenamiento, utilizando el algoritmo AES-256 proporcionado por el Proveedor Cloud. Dicha información sólo es legible en el momento de su procesamiento.

### 3.4.2.2. ESCENARIO DE CIFRADO APLICACIONES WEB.

Para los servicios en Cloud y aplicaciones que lo soporten las llaves de cifrado serán administradas por servicios de KMS - Key Management Service - para garantizar el cifrado de la información en reposo, ver el Procedimiento Gestionar Llaves de Cifrado

- **INTERCAMBIO DE INFORMACIÓN CON CLIENTES:** Con las Entidades se debe realizar la creación de tres (3) llaves: Llave de compensación, llave de transferencia y llave enrutamiento. Las llaves no se guardan en Visionamos quedan en la entidad, pero se deja registro en un repositorio.

Para el intercambio de información de estas llaves se le debe aplicar el Criptoperiodo cuatro (4) años.

- **INTERCAMBIO DE INFORMACIÓN CON DISPOSITIVOS:** Con los dispositivos se generan las llaves y se matriculan en los Datáfono y Pin Pad, estas llaves quedan grabadas (Solo Pin Pad) en los dispositivos, y se deja evidencia en la siguiente ruta:



| 7. DESARROLLO | | | | |
|---|---|---|---|---|
| ORDEN LÓGICO | TAREA | CARGO RESPONSABLE | MÉTODO (Cómo se hace, cuándo, dónde) | ACTIVIDAD DE CONTROL (x) |
| 1. | Verificar disponibilidad de dispositivos | Analista de Operaciones | | x |
| | | | Una vez identificada la disponibilidad, evalúa la necesidad de solicitar la | |

## Seguridad Dispositivos:

La organización garantiza que la información confidencial ingresada en los dispositivos POS no sea almacenada ni retenida en los puntos de uso mediante controles técnicos y normativos alineados con las mejores prácticas de la industria.

Los dispositivos POS utilizados cuentan con **certificación PCI PTS (PIN Transaction Security)**, lo que asegura que el hardware y el firmware cumplen con controles de seguridad diseñados para prevenir la captura, almacenamiento y exposición no autorizada de datos sensibles, incluyendo la protección contra manipulaciones físicas y lógicas.

Adicionalmente, la operación de estos dispositivos se encuentra alineada con los requisitos establecidos en el **estándar PCI DSS versión 4.0.1**, el cual contempla controles específicos orientados a:

- impedir el almacenamiento de datos sensibles de autenticación,

- proteger la información durante su ingreso,
- Reducir el riesgo de exposición visual o acceso por parte de terceros en los puntos de interacción.
- Se aplican controles operativos y de concientización que refuerzan el uso adecuado de los dispositivos, asegurando que la información confidencial sea procesada exclusivamente de forma transitoria y segura, sin retención local en los equipos POS.
- Se Implementa el intercambio dinámico de llaves entre los sistemas de cifrado, con la frecuencia necesaria para dotar de seguridad a las operaciones realizadas.
- Los dispositivos POS se instalan y operan bajo medidas de seguridad física alineadas con las especificaciones del fabricante, garantizando su integridad y correcto funcionamiento. Asimismo, se implementan controles que preservan la privacidad de las transacciones, evitando la exposición de información sensible a terceros.
- El canal de transacciones informa al usuario sobre la fecha y hora del último ingreso registrado, apoyando la detección de accesos no autorizados y fortaleciendo la seguridad de las sesiones.

Cordialmente,

Daniel Londoño
Oficial de Seguridad de la Información

Certificado CO19/9022

El sistema de gestión de

# VISIONAMOS SISTEMA DE PAGO COOPERATIVO

Cra. 43A #34-95 La Candelaria, Almacentro, torre sur piso 7, Medellín, Antioquia

ha sido evaluado y certificado que cumple con los requisitos de

**ISO/IEC 27001:2022**

Para las siguientes actividades

SERVICIO DE ADMINISTRACIÓN, ACTUALIZACIÓN Y MONITOREO: DE PLATAFORMAS TECNOLÓGICAS Y DE TELECOMUNICACIONES, MEDIOS DE PAGOS Y CANALES TRANSACCIONALES PARA EL SECTOR SOLIDARIO Y COOPERATIVO DE ACUERDO CON LA DECLARACIÓN DE APLICABILIDAD EN LA VERSIÓN 4

Este certificado es válido desde 19 de noviembre de 2025 hasta 11 de agosto de 2028 y su validez está sujeta al resultado satisfactorio de las auditorías de seguimiento.

Edición 5. Certificada desde 12 de agosto de 2019

Expiración del ciclo anterior 11 de agosto de 2025
Auditoría de renovación 28 de agosto de 2025

Autorizado por

Diego Grajeda
Business Assurance Business Manager
Central America, Colombia & Caribbean Region (COL-CAM)

SGS COLOMBIA S.A.S.
Carrera 100 No. 25C-11
t (+57-601) 6069292 - www.sgs.com.co

ISO/IEC 17021-1:2015
09-CSG-005

PCI DSS LEVEL-1

ControlCase

# CERTIFICATE OF COMPLIANCE

## Visionamos Sistema de Pago Cooperativo - Payment Processing Infrastructure

Cra. 43A #34-95 La Candelaria, Almacentro, torre sur piso 7, Medellín, Antioquia, Colombia

has been validated by ControlCase and found to be in compliance with requirements of **Payment Card Industry Data Security Standard (PCI DSS) Version 4.0.1** as per Report on Compliance issued on **May 29, 2025**

**ControlCase is a Qualified Security Assessor (QSA) certified by the PCI Security Standards Council**

Please note that this certificate does not substitute for the need to register with the card brands directly in order to be listed on their websites and for them to confirm you as compliant per their individual programs.

| REFERENCE NO.: | 05292025MDEVSDPC | EXPIRATION DATE: | May 28, 2026 | ASSESSED BY: | ControlCase |
|---|---|---|---|---|---|

**Pregunta # 1**

Documento que detalle las políticas de seguridad específicas para el uso de

sistemas POS, incluyendo el cumplimiento de los estándares PCI-DSS para la

lectura de tarjetas.

**Pregunta # 2**

Procedimientos que expliquen cómo los administradores de tecnología validan la autenticación de los datáfonos conectados y los controles criptográficos que se utilizan para proteger los canales de comunicación.

**Pregunta #3**

Documentación que identifique a los responsables de los datáfonos en los establecimientos comerciales, incluyendo procedimientos para confirmar la identidad de los funcionarios autorizados para el mantenimiento.

**Pregunta #4**

Documentación que describa las políticas y procedimientos para garantizar que la información confidencial no sea almacenada o retenida en los lugares de uso de los POS, así como para reducir el riesgo de que terceros vean la información sensible ingresada.

**Pregunta #5**

Documento que establezca las políticas de seguridad específicas para transacciones realizadas a través de Internet, incluyendo el uso de algoritmos y protocolos de comunicación segura.

**Pregunta #6**

Procedimientos que describan los mecanismos implementados para proteger la información de las transacciones y minimizar el riesgo de capturas por terceros no autorizados.

**Pregunta #7**

Procedimiento de notificación al usuario que informe la fecha y hora del último ingreso al canal de transacciones al inicio de cada sesión.