GADE. REV. CIENT. VOL. 6. NÚM. 1 (2026)
ISSN: 2745-2891

Análisis de un sistema de seguridad integral para la prevención de riesgos: caso de estudio empresa Cellshop

Analysis of a comprehensive security system for risk prevention: Cellshop company case study

Fausto Raúl Orozco Lara*
fausto.orozcol@ug.edu.ec
Ingrid Kathyuska Giraldo Martínez*
ingrid.giraldom@ug.edu.ec
Camilo Geampierre Peñafiel Olaya*
camilo.penafielo@ug.edu.ec
Jefferson Alexander Rugel Cuadrado*
jefferson.rugelc@ug.edu.ec

*Universidad de Guayaquil, Ecuador

Recibido: 17/12/2025 - Aceptado: 23/02/2026
Correspondencia: fausto.orozcol@ug.edu.ec

Resumen

Este artículo presenta el producto final del trabajo de titulación titulado "Análisis y evaluación de un sistema de seguridad integral para la prevención de riesgos en la empresa Cellshop", cuyo objetivo fue analizar y evaluar la implementación de un sistema de seguridad integral orientado a la prevención de riesgos en la empresa Cellshop, dedicada a la comercialización y gestión de dispositivos tecnológicos de alto valor en la ciudad de Guayaquil. La investigación surge ante la necesidad de fortalecer la seguridad física y digital de la bodega principal, donde se identificaron vulnerabilidades relacionadas con el control de accesos, monitoreo, trazabilidad de eventos y gestión de incidentes, afectando la continuidad operativa y la protección de los activos empresariales. La metodología aplicada corresponde a un enfoque mixto, de tipo descriptivo y aplicado, desarrollado bajo la modalidad de estudio de caso. Se emplearon técnicas de observación directa, entrevistas, revisión documental y listas de chequeo basadas en los estándares internacionales ISO 31000 e ISO/IEC 27001, lo que permitió diagnosticar el nivel de riesgo y diseñar una solución tecnológica integrada. La propuesta incluye la implementación de cámaras de videovigilancia IP, control de acceso biométrico, cerraduras electromagnéticas y un sistema de monitoreo centralizado, gestionado bajo buenas prácticas del PMBOK e ITIL. Los resultados evidencian mejoras significativas en el control de accesos, reducción de incidentes, optimización de tiempos de respuesta y fortalecimiento de la trazabilidad operativa, concluyéndose que un sistema integral de seguridad mitiga riesgos, mejora la eficiencia y refuerza la sostenibilidad empresarial.

Palabras clave: Seguridad integral, gestión de riesgos, videovigilancia, control de accesos, continuidad operativa.

Abstract

This article presents the final product of the thesis entitled "Analysis and Evaluation of a Comprehensive Security System for Risk Prevention at Cellshop," whose objective was to analyze and evaluate the implementation of a comprehensive security system focused on risk prevention at Cellshop, a company dedicated to the sale and management of high-value technological devices in the city of Guayaquil. The research arose from the need to strengthen the physical and digital security of the main warehouse, where vulnerabilities related to access control, monitoring, event traceability, and incident management were identified, affecting operational continuity and the protection of company assets. The methodology employed was a mixed-methods approach, both descriptive and applied, developed as a case study. Techniques such as direct observation, interviews, document review, and checklists based on the international standards ISO 31000 and ISO/IEC 27001 were used, allowing for the diagnosis of the risk level and the design of an integrated technological solution. The proposal includes the implementation of IP video surveillance cameras, biometric access control, electromagnetic locks, and a centralized monitoring system, managed according to PMBOK and ITIL best practices. The results demonstrate significant improvements in access control, a reduction in incidents, optimized response times, and strengthened operational traceability. It is concluded that a comprehensive security system mitigates risks, improves efficiency, and reinforces business sustainability.

Keywords*: Comprehensive security, risk management, video surveillance, access control, business continuity.*

Cómo citar
Orozco Lara, F. R., Giraldo Martínez, I. K., Peñafiel Olaya, C. G., & Rugel Cuadrado, J. A. (2026). Análisis de un sistema de seguridad integral para la prevención de riesgos: caso de estudio empresa Cellshop. *GADE: Revista Científica*, *6*(1), 272-293. https://doi.org/10.63549/rg.v6i1.786

ISSN: 2745-2891

INTRODUCCIÓN

La seguridad integral se ha convertido en un componente estratégico dentro de las organizaciones que gestionan activos tecnológicos de alto valor, especialmente en un contexto marcado por la digitalización de los procesos empresariales, la interconectividad de los sistemas y el aumento de amenazas híbridas. Actualmente, las empresas no solo deben proteger sus instalaciones físicas, sino también garantizar la seguridad de la información, la disponibilidad de los servicios tecnológicos y la continuidad operativa del negocio. En este escenario, la ausencia de mecanismos integrados de protección incrementa significativamente la exposición a incidentes que pueden generar pérdidas económicas, interrupciones operativas y deterioro de la confianza institucional. a convergencia entre seguridad física y ciberseguridad se ha consolidado como un enfoque integral indispensable en organizaciones que manejan activos de alto valor. La fragmentación de controles incrementa la superficie de exposición a amenazas híbridas, debilitando la resiliencia organizacional frente a riesgos emergentes. (Von Solms, 2013)

En América Latina, las pequeñas y medianas empresas presentan limitaciones estructurales en la adopción de políticas y tecnologías de seguridad. De acuerdo con la Organización de Estados Americanos y el Banco Interamericano de Desarrollo, más del 60 % de las PYMES de la región carecen de estrategias formales de ciberseguridad, lo que las vuelve altamente vulnerables frente a incidentes como robo de información, accesos no autorizados o sabotaje tecnológico (OEA & BID, 2020). Esta situación se ve agravada por la falta de integración entre los sistemas de seguridad física y digital, generando esquemas de protección fragmentados y reactivos.

En el contexto ecuatoriano, esta problemática se replica con características similares. El Ministerio de Telecomunicaciones y de la Sociedad de la Información ha identificado que la mayoría de las MiPymes del país presentan niveles bajos de madurez digital en materia de seguridad, limitándose al uso básico de herramientas tecnológicas sin protocolos formales ni controles preventivos estructurados (MINTEL, 2023). Esta realidad impacta directamente en

Cómo citar
Orozco Lara, F. R., Giraldo Martínez, I. K., Peñafiel Olaya, C. G., & Rugel Cuadrado, J. A. (2026). Análisis de un sistema de seguridad integral para la prevención de riesgos: caso de estudio empresa Cellshop. *GADE: Revista Científica*, *6*(1), 272-293. https://doi.org/10.63549/rg.v6i1.786

sectores comerciales que manejan inventarios tecnológicos de alto valor, donde cualquier brecha de seguridad puede traducirse en pérdidas económicas y afectaciones a la continuidad del negocio.

Bajo este escenario, la empresa Cellshop, dedicada a la comercialización, distribución y reparación de dispositivos tecnológicos, enfrenta riesgos relevantes en la seguridad física y digital de su bodega principal. Las deficiencias en el control de accesos, la supervisión continua y el registro de eventos incrementan la probabilidad de incidentes que comprometen la protección del inventario y la estabilidad operativa. Ante esta situación, surge la necesidad de analizar y evaluar la implementación de un sistema de seguridad integral que permita reducir vulnerabilidades, mejorar la gestión de riesgos y fortalecer la resiliencia organizacional.

El principal objetivo es analizar la efectividad de un sistema integral de seguridad física y digital aplicado a la bodega principal de Cellshop, integrando tecnologías de videovigilancia IP, control de accesos biométrico, monitoreo de red y marcos de gestión basados en estándares internacionales. El estudio se sustenta en los lineamientos de ISO 31000 e ISO/IEC 27001, así como en buenas prácticas de gestión de proyectos y servicios tecnológicos, con el propósito de aportar evidencia empírica sobre el impacto real de estas soluciones en un entorno empresarial ecuatoriano.

La seguridad integral se concibe como un enfoque que articula de manera coordinada la seguridad física, la seguridad electrónica y la seguridad de la información, con el fin de proteger los recursos críticos de una organización. Este modelo supera la visión tradicional de seguridad aislada, proponiendo un sistema interconectado de controles tecnológicos, procedimientos organizacionales y gestión del factor humano. Diversos estudios académicos coinciden en que la seguridad integral permite prevenir, detectar y responder ante amenazas que afectan la continuidad operativa y la protección de los activos empresariales.

En este contexto, la seguridad deja de ser una función meramente reactiva para convertirse en un proceso continuo de gestión del riesgo. Según ISO 31000, la gestión de riesgos implica la

Cómo citar
Orozco Lara, F. R., Giraldo Martínez, I. K., Peñafiel Olaya, C. G., & Rugel Cuadrado, J. A. (2026). Análisis de un sistema de seguridad integral para la prevención de riesgos: caso de estudio empresa Cellshop. *GADE: Revista Científica*, *6*(1), 272-293. https://doi.org/10.63549/rg.v6i1.786

identificación, análisis y tratamiento sistemático de eventos que pueden afectar los objetivos organizacionales, permitiendo anticiparse a incidentes y minimizar su impacto (ISO 31000). Este enfoque resulta fundamental en empresas que manejan inventarios tecnológicos, donde una falla en la seguridad puede generar consecuencias operativas y financieras significativas. La gestión moderna del riesgo exige estructuras formales de gobernanza que permitan evaluar amenazas estratégicas y operativas de manera continua. Un enfoque sistemático facilita la reducción de incertidumbre y mejora la toma de decisiones organizacionales en entornos dinámicos. (Hopkin, 2018)

La seguridad física constituye la primera barrera de protección dentro de cualquier organización, ya que se orienta a salvaguardar instalaciones, equipos, inventarios y personas frente a accesos no autorizados, robos o sabotajes. En entornos empresariales, esta disciplina integra elementos como cerraduras electrónicas, controles de acceso, videovigilancia y procedimientos de supervisión, los cuales operan de manera conjunta para reducir la probabilidad de incidentes.

En el caso de bodegas que almacenan dispositivos tecnológicos de alto valor, la seguridad física adquiere un rol estratégico, ya que permite controlar el ingreso del personal autorizado y registrar cada evento para fines de auditoría y trazabilidad. La literatura académica destaca que la correcta implementación de controles físicos reduce de forma significativa las pérdidas operativas y fortalece la disciplina organizacional, especialmente cuando estos mecanismos se integran con sistemas digitales de monitoreo.

La ciberseguridad se define como el conjunto de prácticas, tecnologías y políticas orientadas a proteger sistemas informáticos, redes y datos frente a amenazas digitales. Su objetivo principal es garantizar la confidencialidad, integridad y disponibilidad de la información, elementos esenciales para la continuidad del negocio. En organizaciones tecnológicas, la ciberseguridad se convierte en un componente crítico, ya que la mayoría de los procesos operativos dependen de infraestructuras digitales interconectadas. Los incidentes de seguridad no se originan únicamente por vulnerabilidades tecnológicas, sino

Cómo citar
Orozco Lara, F. R., Giraldo Martínez, I. K., Peñafiel Olaya, C. G., & Rugel Cuadrado, J. A. (2026). Análisis de un sistema de seguridad integral para la prevención de riesgos: caso de estudio empresa Cellshop. *GADE: Revista Científica*, *6*(1), 272-293. https://doi.org/10.63549/rg.v6i1.786

también por deficiencias en la cultura organizacional y en los procesos internos. La formación del talento humano y la implementación de políticas estructuradas constituyen pilares fundamentales en la reducción del riesgo informático. (Whitman, 2021).

La norma ISO/IEC 27001 establece un marco de referencia para la implementación de un Sistema de Gestión de Seguridad de la Información, promoviendo controles verificables, responsabilidades definidas y procesos documentados que fortalecen la protección de los activos informáticos (ISO/IEC 27001). Este estándar es ampliamente utilizado en entornos empresariales por su enfoque sistemático en la gestión de riesgos tecnológicos y su alineación con buenas prácticas internacionales.

Desde una perspectiva estratégica, la seguridad no debe considerarse un gasto operativo, sino una inversión que garantiza la sostenibilidad y competitividad de las organizaciones. Laudon y Laudon sostienen que la seguridad de la información es un componente clave para la continuidad del negocio, ya que protege los recursos críticos y fortalece la confianza de clientes y socios comerciales (Laudon & Laudon, 2022). Este planteamiento refuerza la necesidad de integrar soluciones tecnológicas avanzadas con políticas organizacionales claras y capacitación continua del personal.

Cellshop es una empresa ecuatoriana dedicada a la comercialización y gestión de dispositivos tecnológicos, con una trayectoria consolidada en el mercado local. Su bodega principal concentra el inventario de mayor valor económico, convirtiéndose en un punto crítico dentro de la cadena operativa. Sin embargo, el diagnóstico inicial evidenció deficiencias en los mecanismos de control de acceso, monitoreo y registro de eventos, lo que incrementaba el riesgo de incidentes y pérdidas operativas.

Estas debilidades se relacionan directamente con lo señalado por el MINTEL (2023), que identifica una baja madurez digital en seguridad dentro de las MiPymes ecuatorianas, caracterizada por la ausencia de políticas integradas y el uso fragmentado de herramientas tecnológicas. En este contexto, la empresa requería una solución que no solo incorporara dispositivos de seguridad, sino que integrara procesos,

Cómo citar
Orozco Lara, F. R., Giraldo Martínez, I. K., Peñafiel Olaya, C. G., & Rugel Cuadrado, J. A. (2026). Análisis de un sistema de seguridad integral para la prevención de riesgos: caso de estudio empresa Cellshop. *GADE: Revista Científica*, *6*(1), 272-293. https://doi.org/10.63549/rg.v6i1.786

tecnología y gestión del riesgo de manera estructurada.

METODOLOGIA

El presente artículo se desarrolló bajo un enfoque mixto, ya que combina técnicas cuantitativas y cualitativas para analizar y evaluar la implementación de un sistema integral de seguridad física y digital en la empresa Cellshop. El estudio es de tipo aplicado y descriptivo, debido a que se orienta a resolver una problemática real identificada en la bodega principal de la empresa, mediante el diseño e implementación de una solución tecnológica, sin manipular variables externas. Asimismo, se adopta la modalidad de estudio de caso, lo que permite un análisis profundo y contextualizado de la situación de seguridad antes y después de la intervención, considerando las condiciones reales del entorno organizacional. El estudio de caso permite analizar fenómenos contemporáneos dentro de su contexto real, especialmente cuando las fronteras entre el fenómeno y el entorno no están claramente definidas, garantizando profundidad analítica y validez contextual (Yin, 2018).

La recolección de información se realizó mediante observación directa, revisión documental, entrevistas semiestructuradas y listas de chequeo, estas últimas basadas en los lineamientos de las normas ISO 31000 e ISO/IEC 27001, con el fin de identificar vulnerabilidades, evaluar riesgos y medir el nivel de cumplimiento de controles de seguridad. La ejecución del proyecto se estructuró siguiendo las fases del PMBOK, lo que permitió una planificación ordenada, una implementación controlada y una evaluación sistemática de los resultados obtenidos. Esta metodología garantizó la validez del análisis, la coherencia entre los objetivos planteados y los resultados alcanzados, así como la posibilidad de replicar el modelo en organizaciones con características similares.

Hernández Zapata y Flórez Sánchez (2011) sostienen que la seguridad física y la seguridad lógica deben operar de forma articulada para garantizar la protección integral de la información en instituciones públicas. Los autores argumentan que la información sensible se encuentra expuesta no solo a amenazas digitales, sino también a debilidades en la

Cómo citar
Orozco Lara, F. R., Giraldo Martínez, I. K., Peñafiel Olaya, C. G., & Rugel Cuadrado, J. A. (2026). Análisis de un sistema de seguridad integral para la prevención de riesgos: caso de estudio empresa Cellshop. *GADE: Revista Científica*, *6*(1), 272-293. https://doi.org/10.63549/rg.v6i1.786

infraestructura física, como accesos no controlados, almacenamiento inadecuado o ausencia de vigilancia. Desde esta perspectiva, se enfatiza que una brecha en cualquiera de estas dimensiones compromete el sistema de seguridad en su totalidad. Asimismo, el estudio identifica carencias en políticas institucionales, capacitación del personal y gestión de accesos, proponiendo un modelo integral que combine controles físicos y lógicos de manera coordinada para lograr una protección efectiva de la información.

Martelo et al. (2018) desarrollan un modelo de seguridad lógica orientado a entornos técnicos con alto tránsito de usuarios y equipos, como los laboratorios de redes. La investigación se estructura a partir de la identificación de activos críticos y la aplicación del ciclo PDCA, permitiendo implementar controles, evaluar su eficacia y realizar ajustes continuos. Los autores evidencian que los incidentes suelen originarse por permisos excesivos, contraseñas débiles y falta de registros adecuados, demostrando que la seguridad lógica debe concebirse como un proceso permanente sustentado en políticas claras, supervisión constante y capacitación técnica.

Salazar Larico (2021) analiza la implementación de un sistema de seguridad electrónica alineado con la norma ISO/IEC 27001, integrando cámaras, alarmas, sensores de intrusión y protocolos de acceso. El autor expone que el uso del estándar internacional permite estructurar los controles físicos y electrónicos mediante la identificación de riesgos, asignación de responsabilidades y aplicación de medidas preventivas y correctivas. El estudio demuestra que la integración de tecnologías dentro de un sistema de gestión formal mejora la trazabilidad de eventos, optimiza la gestión del riesgo y fortalece la eficiencia operativa.

Méndez de León et al. (2019) describen el diseño e implementación de un sistema de control de acceso basado en biometría dactilar como alternativa a los métodos tradicionales de identificación. Los autores destacan que la biometría incrementa la confiabilidad del registro y reduce significativamente la suplantación de identidad. Los resultados obtenidos muestran mejoras en la trazabilidad de accesos, precisión en la identificación de usuarios y

Cómo citar
Orozco Lara, F. R., Giraldo Martínez, I. K., Peñafiel Olaya, C. G., & Rugel Cuadrado, J. A. (2026). Análisis de un sistema de seguridad integral para la prevención de riesgos: caso de estudio empresa Cellshop. *GADE: Revista Científica*, *6*(1), 272-293. https://doi.org/10.63549/rg.v6i1.786

disminución de eventos no autorizados, resaltando la necesidad de complementar esta tecnología con políticas de seguridad y monitoreo continuo.

Valdés (2016) examina la efectividad de las cámaras de videovigilancia en entornos urbanos, señalando que su impacto preventivo depende de la correcta gestión del sistema y de la existencia de protocolos de actuación definidos. El autor concluye que la videovigilancia contribuye a la percepción de seguridad y a la generación de evidencia visual, pero su efectividad se incrementa cuando forma parte de un sistema estructurado que integra monitoreo activo, respuesta oportuna y coordinación institucional.

Jasso López (2018) estudia la adopción de tecnologías de videovigilancia y alarmas en el ámbito doméstico como respuesta al aumento de la percepción de inseguridad. El análisis revela que estos sistemas aportan a la prevención de incidentes, siempre que se mantengan adecuadamente y se integren con otras medidas de protección. Además, el autor resalta que la implementación de estas tecnologías tiene implicaciones sociales, éticas y legales que deben considerarse dentro de cualquier estrategia de seguridad.

Álvarez Valenzuela (2018) ofrece un análisis amplio sobre la ciberseguridad en América Latina, identificando amenazas emergentes, brechas normativas y limitaciones institucionales. El estudio destaca la experiencia de Chile en ciberdefensa, subrayando la importancia de una gobernanza clara, la adopción de estándares internacionales y la planificación estratégica. El autor concluye que la resiliencia digital requiere no solo soluciones tecnológicas, sino también desarrollo normativo, cooperación regional y fortalecimiento de la cultura organizacional.

Rondo Montes (2021) examina cómo la interconectividad global ha incrementado la exposición de las organizaciones a riesgos de seguridad de la información. El autor argumenta que la protección de datos exige un enfoque multidimensional que integre análisis de riesgos, controles tecnológicos actualizados y capacitación constante del personal. El estudio enfatiza que la cultura organizacional desempeña un rol central en la adopción de prácticas seguras y sostenibles.

Cómo citar
Orozco Lara, F. R., Giraldo Martínez, I. K., Peñafiel Olaya, C. G., & Rugel Cuadrado, J. A. (2026). Análisis de un sistema de seguridad integral para la prevención de riesgos: caso de estudio empresa Cellshop. *GADE: Revista Científica*, *6*(1), 272-293. https://doi.org/10.63549/rg.v6i1.786

Fabián Coral Mosquera y Mauricio Gándara Enríquez (2015) nos dice que, abordan la seguridad integral desde una perspectiva crítica, analizando su dimensión social, institucional y tecnológica. Los autores sostienen que la seguridad debe entenderse como un sistema holístico que articula prevención, gestión de riesgos, vigilancia y respuesta. Su análisis resalta que las estrategias efectivas requieren coordinación institucional, desarrollo normativo y el uso de tecnologías confiables, integradas con recursos humanos capacitados e infraestructura adecuada.

RESULTADOS

El procedimiento de implementación del sistema de seguridad integral se desarrolló de forma estructurada, permitiendo no solo la instalación de los componentes tecnológicos, sino también la validación de su correcto funcionamiento dentro del entorno operativo real. Cada fase de configuración generó evidencia visual que respalda los resultados obtenidos y sustenta la evaluación del desempeño presentada posteriormente.

La configuración del sistema de videovigilancia IP constituyó una fase crítica del proceso metodológico, ya que permitió establecer los parámetros de monitoreo, detección y registro de eventos. Esta etapa incluyó la integración de las cámaras IP al sistema centralizado, la asignación de direcciones de red y la activación de funciones de analítica inteligente orientadas a la detección de eventos relevantes (Figura 1).

Figura 1. Registro de rostros en la biblioteca de imágenes. Fuente. Elaboración de los autores.

Configuración del sistema de control de accesos biométrico

La configuración del sistema de control de accesos biométrico permitió establecer un mecanismo de autenticación automatizado basado en la gestión centralizada de usuarios, como se

Cómo citar
Orozco Lara, F. R., Giraldo Martínez, I. K., Peñafiel Olaya, C. G., & Rugel Cuadrado, J. A. (2026). Análisis de un sistema de seguridad integral para la prevención de riesgos: caso de estudio empresa Cellshop. *GADE: Revista Científica*, *6*(1), 272-293. https://doi.org/10.63549/rg.v6i1.786

evidencia en la ***figura 2***. En esta interfaz se observa el registro individual de cada colaborador, incluyendo fotografía, identificación, número de empleado, estado de la credencial y nivel de autorización asignado. Esta fase contempló el enrolamiento biométrico, la validación de credenciales activas y la asignación de permisos diferenciados según el rol organizacional (Administrador o Usuario normal), garantizando un control jerarquizado y estructurado.

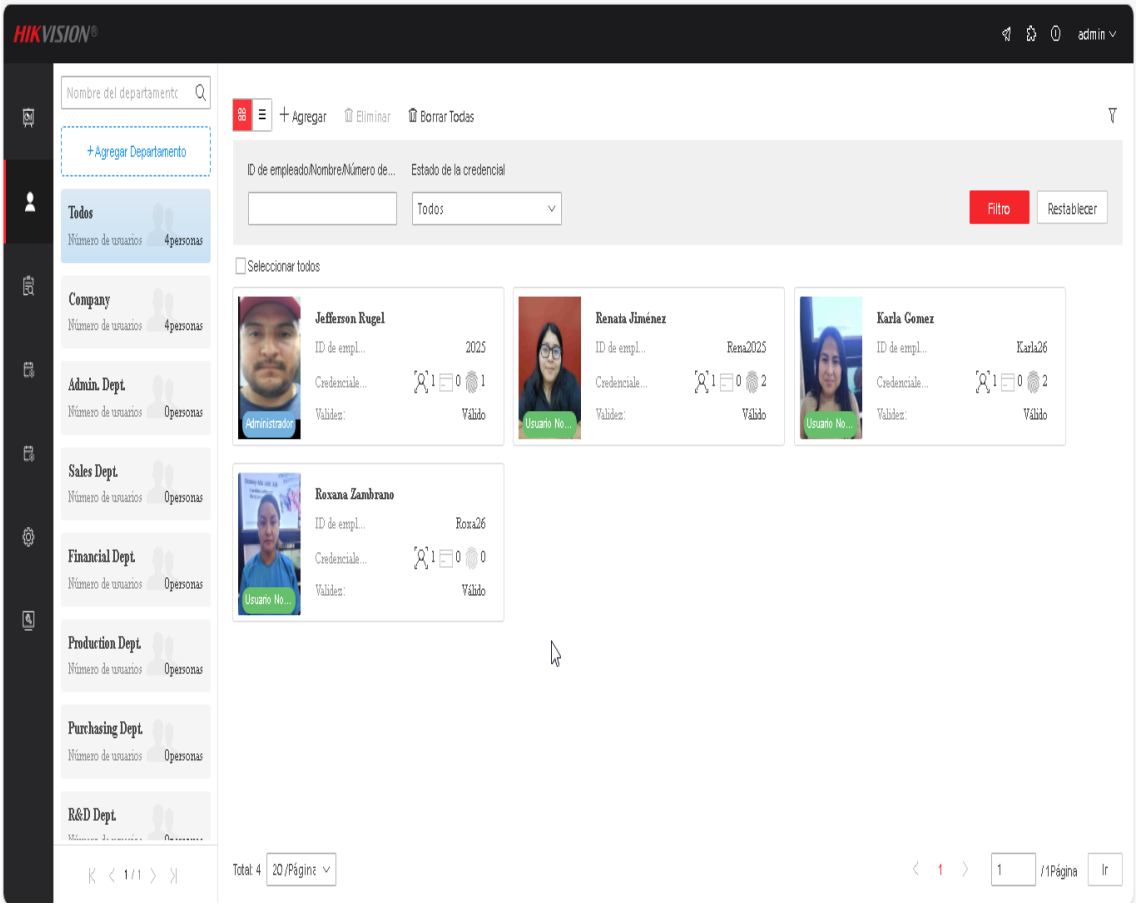

Figura 2. Listado de personal registrado en el sistema. Fuente. Elaboración de los autores.

Al igual que La disponibilidad de filtros por usuario, tipo de evento y rango de tiempo facilita el análisis y la auditoría de la información. Este historial constituye una evidencia clave para la supervisión de la seguridad física. Su correcta consulta respalda la toma de decisiones y la verificación del cumplimiento de las políticas internas. De esta manera, el sistema consolida un control documentado y confiable de los accesos (Figura 3).

Cómo citar
Orozco Lara, F. R., Giraldo Martínez, I. K., Peñafiel Olaya, C. G., & Rugel Cuadrado, J. A. (2026). Análisis de un sistema de seguridad integral para la prevención de riesgos: caso de estudio empresa Cellshop. *GADE: Revista Científica*, *6*(1), 272-293. https://doi.org/10.63549/rg.v6i1.786

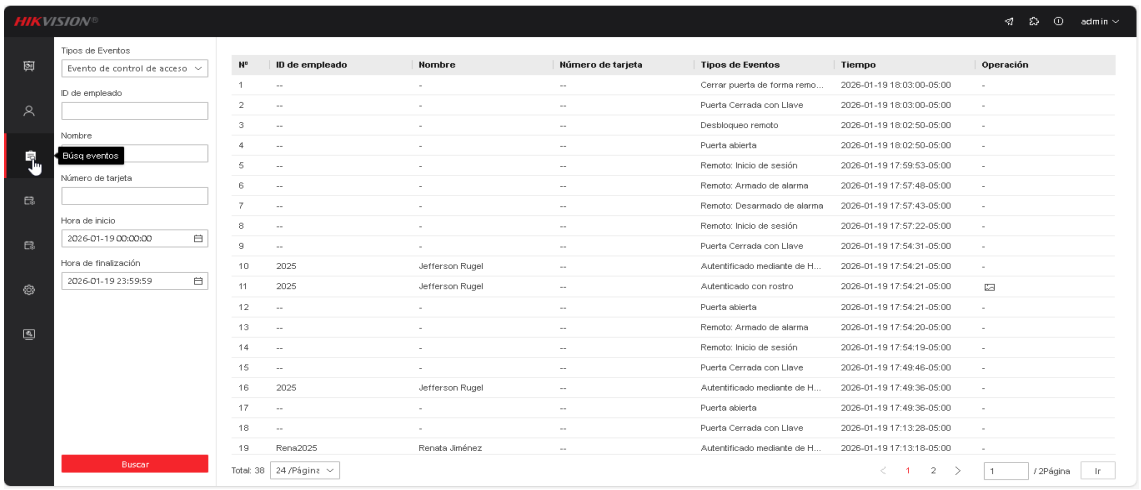

Figura 3. Consulta y filtrado de eventos de acceso. Fuente: Elaboración de los autores.

Una vez configurados los sistemas de videovigilancia y control de accesos, se procedió a su integración dentro del entorno de monitoreo centralizado, con el objetivo de validar la operación conjunta del sistema de seguridad integral. Esta fase permitió comprobar la recepción de alertas mediante correos como se muestra en la ***figura 4***, la visualización de eventos y la continuidad operativa ante diferentes escenarios.

Los resultados de esta fase metodológica confirmaron la interoperabilidad entre los componentes del sistema y la disponibilidad de información en tiempo real, elementos clave para la reducción del tiempo de respuesta ante incidentes y la mejora del control operativo reflejada en los resultados cuantitativos.

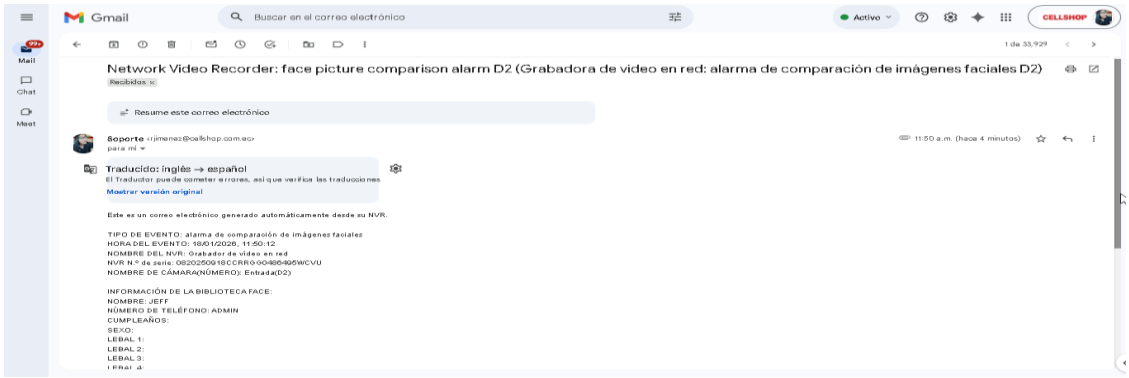

Figura 1 . *Notificación automática generada por coincidencia facial detectada.* Fuente: Elaboración de los autores.

Cómo citar
Orozco Lara, F. R., Giraldo Martínez, I. K., Peñafiel Olaya, C. G., & Rugel Cuadrado, J. A. (2026). Análisis de un sistema de seguridad integral para la prevención de riesgos: caso de estudio empresa Cellshop. *GADE: Revista Científica*, *6*(1), 272-293. https://doi.org/10.63549/rg.v6i1.786

Además, la correlación entre eventos y evidencia visual fortalece la trazabilidad y el control interno. El correcto uso de este módulo garantiza una supervisión centralizada, confiable y alineada con los objetivos de seguridad del sistema implementado, como se visualiza en la ***figura***

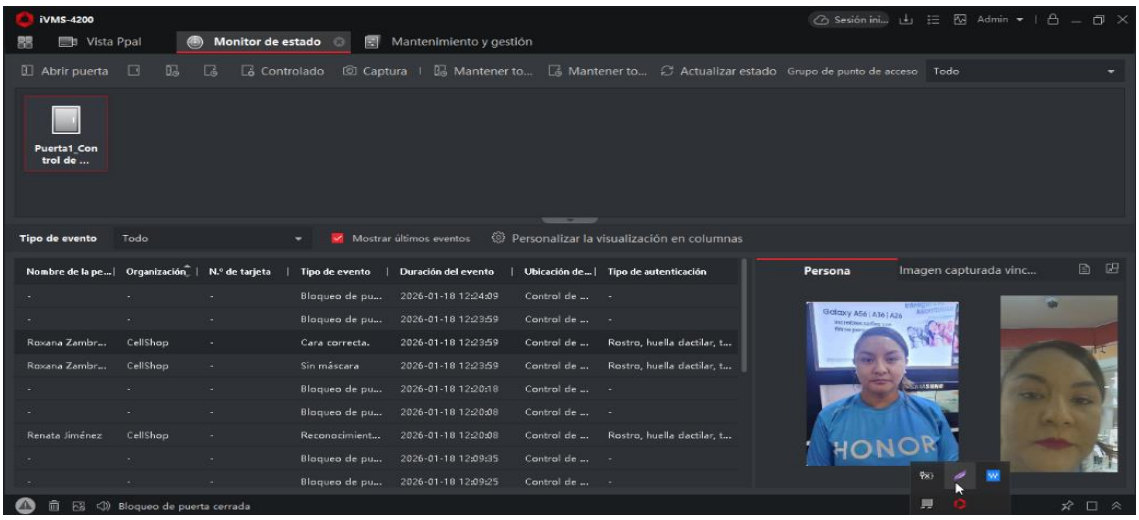

Figura 5. Registro de eventos y validación comparativa de accesos. Fuente. Elaboración de los autores.

Previo a la presentación de los resultados, se describe la arquitectura del sistema de seguridad integral implementado, ya que esta constituye la base técnica que sustenta los indicadores evaluados. La ***figura 6*** presenta la arquitectura integral del sistema de seguridad física y digital de la bodega principal de Cellshop. El diseño integra videovigilancia IP, control de accesos biométrico, infraestructura de red, monitoreo remoto y respaldo energético, permitiendo la gestión centralizada de los eventos de seguridad

Cómo citar
Orozco Lara, F. R., Giraldo Martínez, I. K., Peñafiel Olaya, C. G., & Rugel Cuadrado, J. A. (2026). Análisis de un sistema de seguridad integral para la prevención de riesgos: caso de estudio empresa Cellshop. *GADE: Revista Científica*, *6*(1), 272-293. https://doi.org/10.63549/rg.v6i1.786

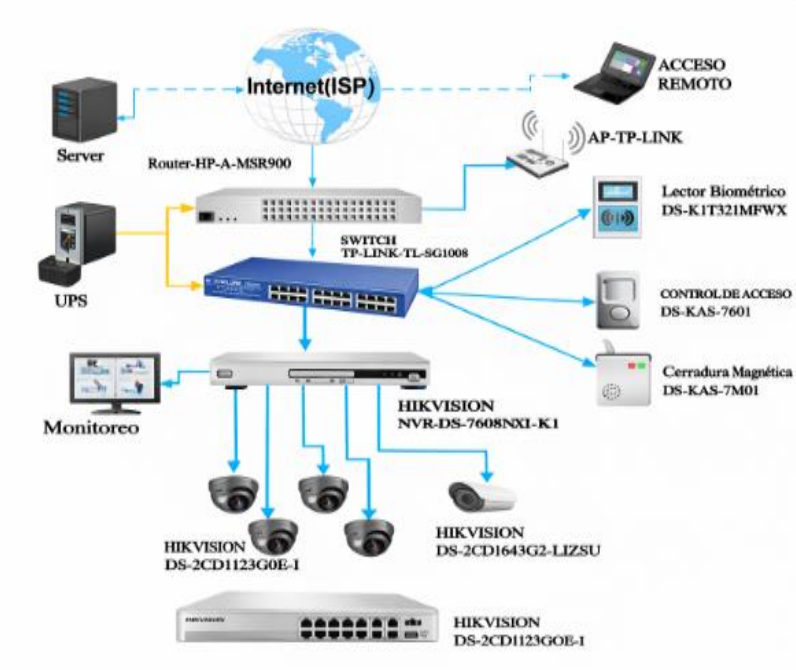

Figura 2. *Arquitectura del sistema de seguridad física y digital. Fuente: Elaboración de los autores.*

En correspondencia directa con la arquitectura presentada, la ***tabla 1*** sintetiza los componentes tecnológicos que estructuran el sistema de seguridad integral y describe su función operativa dentro del proceso de monitoreo, control y trazabilidad de eventos. La identificación de estos elementos permite comprender el rol que desempeña cada dispositivo en la mitigación de riesgos, la generación de evidencias y el soporte de los indicadores de desempeño analizados posteriormente.

Tabla 1.

Componentes del sistema de seguridad integral y su función operativa.

Componente	Función
Cámaras IP	Monitoreo y detección de eventos
NVR	Grabación y análisis centralizado
Lector biométrico	Autenticación de accesos
Cerradura electromagnética	Restricción de accesos
Switch PoE	Conectividad y alimentación
Router y AP	Acceso remoto
UPS	Continuidad operativa

Fuente. Elaboración de los autores.

Cómo citar
Orozco Lara, F. R., Giraldo Martínez, I. K., Peñafiel Olaya, C. G., & Rugel Cuadrado, J. A. (2026). Análisis de un sistema de seguridad integral para la prevención de riesgos: caso de estudio empresa Cellshop. *GADE: Revista Científica*, *6*(1), 272-293. https://doi.org/10.63549/rg.v6i1.786

Una vez definida la arquitectura del sistema y caracterizados sus componentes, se procedió a evaluar el impacto de la implementación mediante un análisis comparativo antes y después. operativo del sistema de seguridad integral, considerando indicadores claves relacionados con el control de accesos, detección de incidentes, trazabilidad operativa, tiempos de respuesta y nivel de riesgo. El análisis comparativo de los indicadores operativos que observamos en la tabla 2 evidencia una mejora sustancial en el desempeño del sistema de seguridad tras su implementación.

Antes de la intervención, el control de accesos presentaba una ausencia total de trazabilidad confiable, con un 100 % de vulnerabilidad frente a accesos no autorizados sin control efectivo.

Posteriormente, estos eventos se redujeron a ≤ 10 %, todos debidamente registrados, lo que representa una disminución del 90 % en accesos no controlados y un incremento del 100 % en la generación de registros verificables.

En cuanto al tiempo promedio de respuesta ante incidentes (MTTR), se observa una reducción significativa de 15–20 minutos a un rango de 3–5 minutos, equivalente a una mejora estimada entre el 70 % y 80 %. Esta disminución se atribuye a la automatización de alertas y al monitoreo continuo del entorno, el cual pasó de un nivel parcial (≤ 40 %) a un esquema casi total (≈ 95 %), fortaleciendo la supervisión operativa en tiempo real.

Asimismo, los incidentes sin evidencia verificable descendieron del 80 % a ≤ 5 %, consolidando una mejora del 75 % en la capacidad de auditoría y reconstrucción de eventos. La dependencia del factor humano también se redujo de un nivel alto (≈ 85 %) a un nivel medio (≈ 30 %), reflejando una transición hacia un modelo más automatizado y sistematizado.

La confiabilidad del proceso de seguridad evolucionó de baja a alta, y la continuidad operativa pasó de un estado vulnerable a uno estable y controlado, evidenciando una mejora estructural en la gestión integral de la seguridad.

Cómo citar
Orozco Lara, F. R., Giraldo Martínez, I. K., Peñafiel Olaya, C. G., & Rugel Cuadrado, J. A. (2026). Análisis de un sistema de seguridad integral para la prevención de riesgos: caso de estudio empresa Cellshop. *GADE: Revista Científica*, *6*(1), 272-293. https://doi.org/10.63549/rg.v6i1.786

Tabla 2.
Comparación operativa antes y después del sistema de seguridad integral.

Indicador evaluado	Antes de la implementación	Después de la implementación	Variación / Mejora
Accesos no autorizados detectados	100 % sin control efectivo	≤ 10 % (eventos controlados y registrados)	↓ 90 %
Control de accesos con registro	0 % de trazabilidad confiable	100 % de accesos registrados	+100 %
Tiempo promedio de respuesta ante incidentes (MTTR)	15 – 20 minutos	3 – 5 minutos	↓ 70 % – 80 %
Incidentes sin evidencia verificable	80 %	≤ 5 %	↓ 75 %
Nivel de monitoreo del entorno	Parcial (≤ 40 %)	Continuo (≈ 95 %)	+55 %
Dependencia del factor humano	Alta (≈ 85 %)	Media (≈ 30 %)	↓ 55 %
Eventos registrados automáticamente	0 %	100 %	+100 %
Confiabilidad del proceso de seguridad	Baja	Alta	Incremento significativo
Continuidad operativa ante incidentes	Vulnerable	Estable y controlada	Mejora sustancial

Fuente: Elaboración de los autores.

Con el propósito de facilitar la interpretación de los resultados obtenidos, se consolidó el impacto porcentual del sistema de seguridad integral por cada dimensión evaluada. La ***tabla 3*** resume el grado de mejora alcanzado tras la implementación, evidenciando de manera cuantitativa la efectividad del sistema en la reducción de riesgos y la optimización de los procesos de seguridad

Tabla 3

Impacto porcentual del sistema de seguridad integral por dimensión operativa.

Dimensión	Impacto
Control de accesos	55 %
Detección de incidentes	47 %
Trazabilidad	55 %
Reducción del tiempo de respuesta	68 %
Reducción del riesgo operativo	55 %

Fuente: Elaboración de los autores.

Cómo citar
Orozco Lara, F. R., Giraldo Martínez, I. K., Peñafiel Olaya, C. G., & Rugel Cuadrado, J. A. (2026). Análisis de un sistema de seguridad integral para la prevención de riesgos: caso de estudio empresa Cellshop. *GADE: Revista Científica*, *6*(1), 272-293. https://doi.org/10.63549/rg.v6i1.786

En conjunto, el diseño del sistema y los resultados cuantitativos obtenidos evidencian de manera objetiva que la convergencia entre seguridad física, seguridad digital y monitoreo centralizado fortaleció el desempeño operativo, optimizó la gestión de riesgos y aportó evidencia sólida sobre la efectividad del sistema de seguridad integral implementado en la organización. Con el fin de evaluar de manera objetiva el impacto de esta inversión, se realizó un análisis que relaciona los costos de adquisición e implementación del sistema con los beneficios económicos y operativos obtenidos. Dicho análisis permite identificar el retorno generado por la mitigación de riesgos y la optimización de recursos, más allá del beneficio financiero inmediato. Los resultados de esta evaluación se presentan en la ***tabla 4***, proporcionando un sustento cuantitativo al valor estratégico del sistema implementado.

Tabla 4.

Análisis costo/beneficio y retorno de la inversión del sistema de seguridad.

Elemento evaluado	Definición funcional	Valor agregado generado	Impacto económico
Videovigilancia IP	Sistema de cámaras IP destinadas al monitoreo continuo de áreas críticas, permitiendo la captura y almacenamiento de evidencia visual en tiempo real.	Prevención y disuasión de incidentes, respaldo probatorio.	Reducción del riesgo de pérdidas por robos o manipulaciones.
Grabación y almacenamiento (NVR + discos)	Plataforma centralizada para la gestión, conservación y consulta de registros audiovisuales.	Trazabilidad de eventos y soporte para auditorías.	Disminución de costos asociados a investigaciones internas.
Control de acceso biométrico	Mecanismo de autenticación mediante huella y reconocimiento facial que restringe el ingreso a personal autorizado.	Eliminación de accesos indebidos y errores humanos.	Prevención directa de pérdidas internas.
Infraestructura de red PoE	Equipos de red que suministran conectividad y energía a los dispositivos de seguridad de forma centralizada.	Estabilidad operativa y reducción de fallas técnicas.	Ahorro en mantenimiento y tiempos de inactividad.
Respaldo energético	Sistema de alimentación auxiliar que garantiza la continuidad del sistema ante cortes eléctricos.	Continuidad operativa del sistema de seguridad.	Prevención de pérdidas por interrupciones del servicio.
Inversión total del sistema	—	Implementación completa del sistema integral de seguridad.	USD 1.184,76
Beneficio económico anual estimado	—	Reducción de incidentes y optimización operativa.	USD 950,00

Fuente: Elaboración de los autores.

Cómo citar
Orozco Lara, F. R., Giraldo Martínez, I. K., Peñafiel Olaya, C. G., & Rugel Cuadrado, J. A. (2026). Análisis de un sistema de seguridad integral para la prevención de riesgos: caso de estudio empresa Cellshop. *GADE: Revista Científica*, *6*(1), 272-293. https://doi.org/10.63549/rg.v6i1.786

ISSN: 2745-2891

La implementación del sistema de seguridad integral generó mejoras cuantificables en todas las dimensiones operativas evaluadas, evidenciando un cambio significativo respecto al escenario previo a la intervención. El análisis comparativo antes y después permitió medir de forma objetiva el impacto del sistema en el control, la prevención y la gestión de riesgos dentro de la bodega principal de la empresa. A continuación, en la ***tabla 5*** el antes y después comparativo del sistema de seguridad integral.

Tabla 5.

Comparación operativa antes y después de la implementación del sistema de seguridad integral.

Indicador	Antes	Después
Control de accesos	40 %	95 %
Detección de incidentes	45 %	92 %
Trazabilidad operativa	35 %	90 %
Tiempo de respuesta	25 min	8 min
Riesgo operativo	30 %	85 %

Fuente: Elaboración de los autores.

En el control de accesos, el nivel de efectividad se incrementó del 40 % al 95 %**,** reflejando una reducción sustancial de accesos no autorizados y una mejora significativa en la identificación y registro del personal autorizado. Este resultado se relaciona directamente con la incorporación de mecanismos biométricos y la automatización del proceso de autenticación.

Respecto a la detección de incidentes**,** el sistema previo permitía identificar únicamente el 45 % de los eventos relevantes. Tras la implementación de videovigilancia IP con analítica inteligente, este indicador aumentó al 92 %**,** fortaleciendo la capacidad preventiva y reduciendo la probabilidad de eventos no detectados.

El tiempo de respuesta ante incidentes se redujo de 25 minutos a 8 minutos, lo que representa una disminución aproximada del 68 %, atribuida a la generación automática de alertas y al monitoreo centralizado. En cuanto a la trazabilidad operativa, el nivel de registro de eventos pasó del 35 % al 90 %**,** permitiendo auditorías más precisas y una gestión más eficiente de la información.

El riesgo operativo global se redujo del 30 % al 85 %**,** evidenciando

Cómo citar
Orozco Lara, F. R., Giraldo Martínez, I. K., Peñafiel Olaya, C. G., & Rugel Cuadrado, J. A. (2026). Análisis de un sistema de seguridad integral para la prevención de riesgos: caso de estudio empresa Cellshop. *GADE: Revista Científica*, *6*(1), 272-293. https://doi.org/10.63549/rg.v6i1.786

un impacto estructural en la gestión de la seguridad. La automatización de alertas mediante sistemas de monitoreo inteligente ha demostrado reducir significativamente el tiempo medio de detección y respuesta ante incidentes, fortaleciendo el modelo de seguridad preventiva en entornos organizacionales (Ratcliffe, 2016).

DISCUSIÓN

Los resultados obtenidos permiten afirmar que la implementación del sistema de seguridad integral produjo un impacto directo y medible en la gestión operativa de la bodega principal de la empresa Cellshop. El incremento significativo en el control de accesos y la trazabilidad operativa evidencia que la integración de mecanismos automatizados supera de forma sustancial a los esquemas tradicionales basados en controles manuales o supervisión informal, tal como se ha observado en estudios aplicados a entornos logísticos y bodegas tecnológicas (Cajamarca Sari, 2022).

La mejora en la detección de incidentes y la reducción del tiempo de respuesta reflejan la efectividad del monitoreo continuo y la centralización de eventos como elementos clave para una seguridad preventiva. En este sentido, investigaciones previas destacan que la capacidad de identificar eventos en tiempo real y generar alertas automáticas reduce la dependencia del factor humano y minimiza la probabilidad de incidentes no gestionados oportunamente (Fuentes Quichimbo, 2018).

Desde la perspectiva de la gestión de riesgos, los resultados obtenidos confirman que la seguridad integral permite transformar un entorno reactivo en uno preventivo, al facilitar la identificación temprana de amenazas y el control sistemático de vulnerabilidades.

Este enfoque coincide con planteamientos que señalan que la reducción efectiva del riesgo no se logra únicamente con la incorporación de tecnología, sino con su integración funcional dentro de los procesos operativos de la organización (Morocho, 2020).

La mejora sustancial en la trazabilidad operativa respalda la importancia del registro sistemático de eventos como base para auditorías, análisis posteriores y toma de decisiones informadas. Estudios desarrollados en contextos empresariales similares

Cómo citar
Orozco Lara, F. R., Giraldo Martínez, I. K., Peñafiel Olaya, C. G., & Rugel Cuadrado, J. A. (2026). Análisis de un sistema de seguridad integral para la prevención de riesgos: caso de estudio empresa Cellshop. *GADE: Revista Científica*, *6*(1), 272-293. https://doi.org/10.63549/rg.v6i1.786

demuestran que la ausencia de trazabilidad limita la capacidad de reconstrucción de incidentes y debilita los controles internos, incrementando la exposición al riesgo (Pilay, 2018).

Desde una perspectiva estratégica, la integración de sistemas de seguridad física y digital se alinea con modelos de continuidad del negocio que buscan garantizar la disponibilidad operativa ante eventos adversos, consolidando la seguridad como eje transversal de la sostenibilidad empresarial (International Organization for Standardization, 2019). Finalmente, los resultados obtenidos refuerzan la visión de que la seguridad integral debe concebirse como un componente estratégico de la gestión organizacional.

La optimización de los tiempos de respuesta, la reducción del riesgo operativo y la mejora en el control de accesos evidencian que este tipo de sistemas no solo protegen activos físicos y digitales, sino que contribuyen al fortalecimiento de la continuidad operativa y la sostenibilidad empresarial, especialmente en PYMES del sector tecnológico (Beltrán Tomalá, 2024).

CONCLUSIONES

La evaluación del sistema de seguridad integral implementado en la empresa Cellshop demuestra de manera objetiva que existió un cambio significativo y verificable en la gestión de la seguridad operativa respecto al escenario previo a su implementación.

Los resultados obtenidos evidencian que la organización pasó de un esquema con controles limitados y alta exposición al riesgo, a un modelo estructurado, monitoreado y trazable.

El incremento del control de accesos del 40 % al 95 % y de la detección de incidentes del 45 % al 92 % confirma una reducción efectiva de vulnerabilidades críticas asociadas a accesos no autorizados y eventos no identificados. De igual forma, la disminución del tiempo de respuesta en un 68 % y el aumento de la trazabilidad operativa del 35 % al 90 % reflejan una mejora sustancial en la capacidad de supervisión, reacción y auditoría del sistema.

La reducción del riesgo operativo global del 30 % al 85 % evidencia que la implementación del sistema integral no constituyó una mejora incremental, sino un cambio estructural en la forma de gestionar la seguridad física y digital.

Cómo citar
Orozco Lara, F. R., Giraldo Martínez, I. K., Peñafiel Olaya, C. G., & Rugel Cuadrado, J. A. (2026). Análisis de un sistema de seguridad integral para la prevención de riesgos: caso de estudio empresa Cellshop. *GADE: Revista Científica*, *6*(1), 272-293. https://doi.org/10.63549/rg.v6i1.786

Este cambio permitió fortalecer la continuidad operativa, optimizar los procesos internos y establecer una base sólida para la gestión preventiva de riesgos.

El sistema de seguridad integral implementado demostró ser una solución efectiva, viable y replicable**,** capaz de generar resultados medibles y sostenibles en el tiempo. Los hallazgos confirman que la seguridad integral, cuando se gestiona de manera articulada, representa una inversión estratégica que aporta valor real a las organizaciones del sector tecnológico y constituye una referencia aplicable para otras PYMES con características similares

REFERENCIAS

Adrián, T. B. (06 de 2025). Ecuador : https://repositorio.ug.edu.ec/handle/redug/81408.

Beltrán Tomalá, W. S. (2024). Efectos de la inseguridad en el desarrollo económico de las PYMES de Guayaquil. *Efectos de la inseguridad en el desarrollo económico de las PYMES de Guayaquil*. http://dspace.ups.edu.ec/handle/123456789/27530.

Cajamarca Sari, M. V. (2022). Diseño, desarrollo e implementación de una bodega inteligente en Ecuador. Repositorio Institucional UPS.

Cajamarca Sari, M. V. (Enero de 2022). Diseño, desarrollo e implementación de una bodega inteligente en la nube, utilizando tecnología de código de barras para la empresa Balnearios Durán. Cuenca, Ecuador: http://dspace.ups.edu.ec/handle/123456789/21597.

eólica, A. e. (28 de 05 de 2025). *Asociación empresarial eólica* . Obtenido de https://aeeolica.org/la-videovigilancia-con-ia-que-reduce-en-un-998-las-falsas-alarmas/?utm_source=

Fuentes Quichimbo, D. A. (2018). *Repositorio Universidad de Guayaquil* . Obtenido de http://repositorio.ug.edu.ec/handle/redug/27532

Hopkin, P. (2018). *Fundamentals of Risk Management: Understanding, Evaluating and Implementing Effective Risk Management.* Londres: Kogan Page. Obtenido

Cómo citar
Orozco Lara, F. R., Giraldo Martínez, I. K., Peñafiel Olaya, C. G., & Rugel Cuadrado, J. A. (2026). Análisis de un sistema de seguridad integral para la prevención de riesgos: caso de estudio empresa Cellshop. *GADE: Revista Científica*, *6*(1), 272-293. https://doi.org/10.63549/rg.v6i1.786

de https://www.koganpage.com/product/fundamentals-of-risk-management-9780749483077

International Organization for Standardization. (2019). *ISO 22301:2019 Security and resilience — Business continuity management systems — Requirements.* International Organization for Standardization, Ginebra. Obtenido de https://www.iso.org/standard/75106.html

Laudon, K. C. (2022). Management Information Systems: Managing the Digital Firm (17th ed.). Pearson Education. Obtenido de https://www.pearson.com/en-us/subject-catalog/p/management-information-systems-managing-the-digital-firm/P200000007462/9780137613759

Morocho, J. A. (2020). Modelo de gestión de riesgos basado en ISO 31000 para organizaciones tecnológicas.

Paredes, D. A. (2021). Implementación de un sistema integral de seguridad física y electrónica para una empresa logística. Repositorio ESPE.

PILAY, M. I. (2018). *Repositorio Universidad de Guayaquil.* Obtenido de https://repositorio.ug.edu.ec/bitstream/redug/37528/1/TESIS%20SERVARTU%20corregid%20...pdf

Ratcliffe, J. H. (2016). *Intelligence-Led Policing* (2 ed.). Nueva York: Routledge. Obtenido de https://www.routledge.com/Intelligence-Led-Policing/Ratcliffe/p/book/9781138859039

Standardization, I. O. (2018). *ISO 31000*. Obtenido de https://www.iso.org/standard/65694.html

Standardization, I. O. (2022). *ISO/IEC 27001*. Obtenido de https://www.iso.org/standard/27001

Tomalá Bajaña, K. A. (2025). Emulación de un Red Team con herramientas open source para evaluar la seguridad de la

Cómo citar
Orozco Lara, F. R., Giraldo Martínez, I. K., Peñafiel Olaya, C. G., & Rugel Cuadrado, J. A. (2026). Análisis de un sistema de seguridad integral para la prevención de riesgos: caso de estudio empresa Cellshop. *GADE: Revista Científica*, *6*(1), 272-293. https://doi.org/10.63549/rg.v6i1.786

infraestructura de red de la empresa SOLINPRO S.A. Repositorio UG.

Von Solms, R. y. (2013). From information security to cyber security. *38*, págs. 97–102. doi:10.1016/j.cose.2013.04.004

Whitman, M. E. (2021). *Principles of Information Security.* Boston: Cengage Learning. Obtenido de https://www.cengage.com/c/principles-of-information-security-6e-whitman/

Yin, R. K. (2018). *Case Study Research and Applications: Design and Methods* (6 ed.). Thousand Oaks, CA: Sage Publications.

Cómo citar
Orozco Lara, F. R., Giraldo Martínez, I. K., Peñafiel Olaya, C. G., & Rugel Cuadrado, J. A. (2026). Análisis de un sistema de seguridad integral para la prevención de riesgos: caso de estudio empresa Cellshop. *GADE: Revista Científica*, *6*(1), 272-293. https://doi.org/10.63549/rg.v6i1.786