TRABAJO DE GRADO
Opción Seminario-Diplomado.

Acceso Remoto Inseguro a Sistemas de Videovigilancia

Corporación Universitaria Remington.
Facultad de Ingeniería
Ingeniería en Sistemas

Juan Pablo Agudelo Aguilera
Jose Alirio Galeano Salazar
Jorge Leonardo Ramirez Restrepo
Seminario en Gestión de Ciberseguridad en las Organizaciones
2026

Tabla de Contenidos

Resumen

El presente informe técnico desarrolla un análisis de ciberseguridad organizacional aplicado a *La Empresa Caso de Estudio*, organización dedicada a la instalación y mantenimiento de sistemas de videovigilancia y soluciones de seguridad electrónica. El propósito principal del trabajo consiste en identificar, analizar y evaluar los riesgos asociados al acceso remoto inseguro a sistemas DVR/NVR, problemática que representa una amenaza significativa para la protección de la información y la continuidad operativa de los clientes.

El desarrollo del informe se fundamentó en los conocimientos adquiridos durante el Seminario en Gestión de Ciberseguridad en las Organizaciones, aplicando conceptos relacionados con activos de información, amenazas, vulnerabilidades, gestión de riesgos y controles de seguridad. Para ello, se realizó inicialmente la identificación de los activos críticos de la organización, incluyendo grabaciones de videovigilancia, credenciales de acceso, infraestructura de red y dispositivos de monitoreo.

Posteriormente, se efectuó un análisis de amenazas y vulnerabilidades, identificando debilidades relacionadas con credenciales inseguras, exposición de puertos a internet, configuraciones deficientes y ausencia de mecanismos de acceso seguro. A partir de estos hallazgos, se elaboró una matriz de riesgos que permitió evaluar la probabilidad e impacto de los riesgos identificados, determinando escenarios críticos como el acceso no autorizado, la pérdida de evidencia digital y la manipulación remota de los sistemas.

Finalmente, se definieron controles y medidas de mitigación basados en buenas prácticas internacionales como ISO/IEC 27001 e ISO 27005, proponiendo soluciones como el uso de VPN, segmentación de red, políticas de contraseñas seguras y actualización periódica de firmware. El informe evidencia la aplicación práctica de la ciberseguridad organizacional en un contexto real, fortaleciendo la comprensión de los riesgos y las medidas necesarias para proteger los activos de información.

Palabras clave

Palabras clave: Ciberseguridad organizacional, gestión de riesgos, activos de información, videovigilancia, controles de seguridad.

Marco conceptual y contextual

Marco conceptual

La ciberseguridad organizacional comprende el conjunto de políticas, controles, procesos y buenas prácticas orientadas a proteger los activos de información frente a amenazas internas y externas que puedan comprometer la operación de una organización. Según la norma ISO/IEC 27001 (2013), la seguridad de la información debe garantizar tres principios fundamentales: confidencialidad, integridad y disponibilidad de los datos (International Organization for Standardization [ISO], 2013).

.

En el contexto de *La Empresa Caso de Estudio*, estos principios adquieren una importancia crítica debido a que la organización administra sistemas de videovigilancia que operan de manera continua y permiten el monitoreo remoto de espacios residenciales y comerciales. La confidencialidad se relaciona con la protección de las grabaciones y accesos a las cámaras frente a terceros no autorizados; la integridad garantiza que las grabaciones no sean alteradas o eliminadas; y la disponibilidad asegura que los sistemas permanezcan operativos cuando el cliente requiera monitoreo en tiempo real.

Los activos de información representan todos aquellos recursos con valor para la organización, incluyendo dispositivos DVR/NVR, cámaras de seguridad, redes, credenciales de acceso, aplicaciones móviles y grabaciones de videovigilancia. Estos activos pueden verse afectados por amenazas como accesos no autorizados, espionaje remoto, robo de credenciales o explotación de vulnerabilidades técnicas.

Dentro del análisis de seguridad, una vulnerabilidad corresponde a una debilidad presente en los sistemas o procesos que puede ser aprovechada por una amenaza. En el caso de estudio, se identificaron vulnerabilidades relacionadas con contraseñas débiles, exposición de puertos a internet, firmware desactualizado y ausencia de controles de acceso robustos. Estas debilidades incrementan el riesgo de incidentes de seguridad que pueden afectar tanto a la organización como a sus clientes.

Por su parte, el riesgo se entiende como la probabilidad de que una amenaza explote una vulnerabilidad y genere un impacto negativo sobre la operación, la reputación o la información de la empresa (ISO, 2018). Para reducir estos riesgos, las organizaciones implementan controles de seguridad técnicos, administrativos y físicos, orientados a minimizar la exposición frente a posibles ataques.

Asimismo, el análisis desarrollado toma como referencia estándares internacionales como ISO/IEC 27001 para la gestión de seguridad de la información e ISO 27005 para la gestión de riesgos, además de la Ley 1581 de 2012 relacionada con la protección de datos personales en Colombia. Estos marcos permiten estructurar el análisis de riesgos y establecer controles alineados con buenas prácticas de ciberseguridad organizacional.

Marco contextual

La Empresa Caso de Estudio es una empresa dedicada a la instalación, configuración y mantenimiento de sistemas de videovigilancia, redes y soluciones de seguridad electrónica para clientes residenciales, comerciales y pequeños negocios. La organización ofrece servicios relacionados con cámaras CCTV, configuración de DVR/NVR, monitoreo remoto, cableado estructurado y soporte técnico preventivo y correctivo.

La operación de la empresa depende directamente de la disponibilidad y correcto funcionamiento de los sistemas tecnológicos implementados, debido a que los clientes utilizan estos servicios como mecanismo principal de vigilancia y control de seguridad en hogares, oficinas, locales comerciales y bodegas. Actualmente, la empresa administra múltiples sistemas de monitoreo remoto, lo que implica el manejo constante de información sensible, como grabaciones de video, configuraciones de red, direcciones IP y credenciales de acceso (Congreso de la República de Colombia, 2012).

Uno de los aspectos más relevantes dentro de la operación de *La Empresa Caso de Estu*dio es la necesidad de facilitar a los clientes el acceso remoto a sus cámaras desde teléfonos móviles y computadores. Sin embargo, durante el análisis realizado se identificó que varios sistemas eran configurados mediante prácticas inseguras, como apertura directa de puertos en routers, uso de credenciales débiles o reutilizadas y ausencia de mecanismos adicionales de protección, como VPN o restricciones de acceso por direcciones IP.

Estas prácticas representan una problemática importante para la organización, ya que incrementan significativamente la superficie de ataque de los sistemas instalados. Un acceso no autorizado a las cámaras podría permitir a un atacante visualizar en tiempo real instalaciones privadas, conocer rutinas de clientes, manipular grabaciones o incluso desactivar sistemas de monitoreo. Esto no solo comprometería la privacidad y seguridad de los clientes, sino que también podría generar pérdida de evidencia digital ante incidentes como robos o actos vandálicos.

Además del impacto técnico, un incidente de seguridad tendría consecuencias operativas y reputacionales para la empresa. La pérdida de confianza por parte de los clientes podría

afectar directamente la continuidad del negocio, disminuir la contratación de servicios y generar afectaciones económicas derivadas de reclamaciones o incumplimientos relacionados con la protección de la información.

En consecuencia, la organización requiere fortalecer sus procesos de gestión de ciberseguridad mediante la implementación de controles técnicos y políticas de seguridad que permitan reducir los riesgos asociados al acceso remoto inseguro y proteger adecuadamente los activos de información involucrados en su operación.

Diagnóstico Inicial de la Situación

El análisis realizado permitió identificar que las principales amenazas presentes en *La Empresa Caso de Estudio* se relacionan con accesos no autorizados a sistemas de videovigilancia, ataques externos a dispositivos expuestos a internet, robo de credenciales y explotación de vulnerabilidades en equipos DVR/NVR. Estas amenazas adquieren un nivel de criticidad elevado debido a que la organización administra sistemas de monitoreo utilizados por clientes residenciales y comerciales como mecanismo principal de seguridad y vigilancia.

Una de las principales vulnerabilidades identificadas corresponde al acceso remoto inseguro mediante apertura directa de puertos en routers (*Port Forwarding*), permitiendo que los dispositivos DVR/NVR sean accesibles desde internet sin mecanismos adicionales de protección. Esta situación incrementa significativamente la probabilidad de ataques automatizados, escaneo de puertos y explotación de credenciales débiles por parte de atacantes externos.

Asimismo, se evidenció el uso de usuarios administradores por defecto y contraseñas reutilizadas o poco robustas, facilitando posibles escenarios de robo de credenciales y

acceso no autorizado a las cámaras de seguridad. En caso de materializarse este tipo de incidente, un atacante podría visualizar grabaciones en tiempo real, monitorear rutinas de los clientes, identificar horarios de ausencia o incluso desactivar cámaras estratégicas dentro de las instalaciones monitoreadas.

El impacto de estas amenazas no se limita únicamente al entorno digital, sino que también puede afectar directamente la seguridad física de los clientes. Un acceso no autorizado a los sistemas de videovigilancia podría ser utilizado para planificar robos, actos vandálicos o actividades delictivas aprovechando la información obtenida mediante las cámaras comprometidas. De igual manera, la manipulación o eliminación de grabaciones afectaría la disponibilidad de evidencia digital ante incidentes de seguridad, dificultando investigaciones posteriores.

Desde el punto de vista organizacional, un incidente de este tipo también tendría consecuencias operativas y reputacionales para *La Empresa Caso de Estudio*. La pérdida de confianza por parte de los clientes podría generar afectaciones económicas, disminución en la contratación de servicios y posibles reclamaciones relacionadas con la protección de la información y la privacidad.

Adicionalmente, se identificó que varios dispositivos presentan firmware desactualizado y ausencia de monitoreo centralizado de accesos, aumentando la exposición frente a vulnerabilidades conocidas y dificultando la detección temprana de incidentes de seguridad.

En consecuencia, el análisis permitió concluir que los riesgos más críticos para la organización están relacionados con la exposición de sistemas a internet sin controles adecuados de seguridad, justificando la necesidad de implementar mecanismos de protección orientados a reducir la superficie de ataque y fortalecer la seguridad de los sistemas de videovigilancia administrados por la empresa.

Desarrollo e Implementación del Aprendizaje

La presente sección evidencia la aplicación práctica de los conocimientos adquiridos en el Seminario en Gestión de Ciberseguridad en las Organizaciones, implementados en La Empresa Caso de Estudio, empresa dedicada a la instalación, configuración y mantenimiento de sistemas de videovigilancia, redes y soluciones tecnológicas de seguridad electrónica.

La problemática seleccionada corresponde al acceso remoto inseguro a sistemas de videovigilancia, situación frecuente en organizaciones del sector tecnológico y de seguridad electrónica, donde los dispositivos DVR/NVR son configurados para permitir monitoreo remoto desde internet sin implementar controles adecuados de protección. Esta situación incrementa significativamente la exposición frente a amenazas externas y genera riesgos relacionados con acceso no autorizado, espionaje remoto, manipulación de grabaciones y afectación de la privacidad de los clientes.

El desarrollo del caso se estructuró siguiendo principios de gestión de riesgos y buenas prácticas internacionales basadas en ISO/IEC 27001, ISO 27005, modelo de Confidencialidad, Integridad y Disponibilidad (CIA), además de lineamientos generales de seguridad perimetral, gestión de accesos y respuesta a incidentes.

Inicialmente, se realizó la identificación y clasificación de los activos de información críticos involucrados en la operación de la empresa, entre los que se encuentran los dispositivos DVR/NVR, grabaciones de videovigilancia, infraestructura de red, credenciales de acceso y aplicaciones móviles de monitoreo. Estos activos fueron clasificados según su nivel de criticidad, considerando el impacto que tendría su pérdida, alteración o compromiso sobre la operación de la empresa y la seguridad de los clientes.

Posteriormente, se efectuó el análisis de amenazas y vulnerabilidades, identificando debilidades relacionadas con apertura de puertos en routers mediante *Port Forwarding*, uso de credenciales por defecto, contraseñas débiles o reutilizadas, firmware desactualizado y ausencia de controles adecuados de monitoreo y registro de accesos. Estas vulnerabilidades incrementan la probabilidad de ataques externos y facilitan posibles escenarios de acceso no autorizado a los sistemas de videovigilancia.

A partir de este análisis, se aplicaron los lineamientos de la norma ISO/IEC 27001 para establecer controles orientados a la protección de los activos críticos y fortalecimiento de la seguridad organizacional. En este sentido, se propusieron controles técnicos relacionados con autenticación segura, restricción de accesos, segmentación de red,

monitoreo de conexiones y actualización periódica de dispositivos(National Institute of Standards and Technology [NIST], 2020).

Sin embargo, además de los controles técnicos, se identificó la necesidad de fortalecer el componente organizacional mediante la definición de políticas de seguridad que respalden la operación de la empresa. Entre las principales políticas propuestas se encuentran:

- Política de control de accesos, orientada a limitar el acceso a sistemas de videovigilancia únicamente a usuarios autorizados y bajo el principio de mínimo privilegio.
- Política de gestión de credenciales, estableciendo lineamientos para el uso de contraseñas robustas, prohibición de reutilización de claves y eliminación de usuarios predeterminados.
- Política de actualización y mantenimiento de firmware, orientada a garantizar que los dispositivos DVR/NVR permanezcan actualizados frente a vulnerabilidades conocidas.
- Política de acceso remoto seguro, definiendo el uso obligatorio de mecanismos de protección como VPN y restricción de acceso mediante direcciones IP autorizadas.

Asimismo, se empleó la norma ISO 27005 para realizar el análisis y evaluación de riesgos asociados a la problemática identificada. Este análisis permitió determinar que los riesgos relacionados con acceso no autorizado, robo de credenciales y espionaje remoto presentan una alta probabilidad de ocurrencia debido a la exposición directa de los sistemas a internet y las configuraciones inseguras detectadas.

En términos de impacto, se identificó que un incidente de seguridad podría afectar directamente la privacidad de los clientes, comprometer evidencia digital almacenada en las grabaciones e incluso poner en riesgo la seguridad física de las instalaciones monitoreadas. Un atacante con acceso a las cámaras podría visualizar rutinas de los usuarios, identificar horarios de ausencia o desactivar dispositivos estratégicos, facilitando posibles actividades delictivas.

Adicionalmente, se aplicó el modelo de Confidencialidad, Integridad y Disponibilidad (CIA) para evaluar el impacto de las amenazas sobre los activos de información. En términos de confidencialidad, se evidenció el riesgo de visualización no autorizada de cámaras y grabaciones. Respecto a la integridad, se identificó la posibilidad de alteración o eliminación de evidencia digital. Finalmente, en relación con la disponibilidad, se

consideró la interrupción del servicio de monitoreo como un riesgo crítico para la operación de los clientes.

En cuanto a la gestión de incidentes, se estructuró un procedimiento básico de respuesta ante un posible acceso no autorizado a un sistema DVR/NVR comprometido. El proceso contempla las siguientes fases:

- Identificación: detección del acceso sospechoso mediante revisión de registros y comportamiento anómalo del sistema.
- Contención: aislamiento temporal del dispositivo comprometido y bloqueo de conexiones externas.
- Erradicación: eliminación de accesos no autorizados, cambio de credenciales y actualización del firmware afectado.
- Recuperación: restauración segura del sistema y verificación del funcionamiento normal de las cámaras y servicios de monitoreo.
- Lecciones aprendidas: documentación del incidente y actualización de controles para prevenir situaciones similares en el futuro.

Finalmente, el análisis permitió evidenciar que la problemática no depende únicamente de aspectos tecnológicos, sino también de factores relacionados con la cultura organizacional y las prácticas de usuarios y técnicos. Se identificó que comportamientos como reutilización de contraseñas, compartir accesos entre usuarios, no actualizar dispositivos o priorizar comodidad operativa sobre seguridad contribuyen significativamente al aumento de riesgos(Whitman & Mattord, 2021).

Por esta razón, se planteó la necesidad de fortalecer la cultura de ciberseguridad dentro de la organización mediante procesos de capacitación y concientización dirigidos tanto a técnicos como a clientes. Estas acciones incluyen recomendaciones sobre buenas prácticas de seguridad, manejo adecuado de credenciales, importancia de las actualizaciones y riesgos asociados a configuraciones inseguras de acceso remoto.

En conjunto, la aplicación de estos marcos conceptuales y organizacionales permitió desarrollar un análisis integral de la problemática, articulando activos, amenazas, vulnerabilidades y riesgos, así como la definición de controles técnicos, políticas organizacionales y estrategias de respuesta orientadas a fortalecer la seguridad de los sistemas de videovigilancia administrados por la empresa.

Figuras y tablas

Identificación de Activos

La identificación de activos permitió reconocer los elementos críticos involucrados en la operación de *La Empresa Caso de Estudio* y determinar cuáles requieren mayores medidas de protección dentro de la organización. Debido a que la empresa presta servicios relacionados con monitoreo y videovigilancia, gran parte de sus activos están directamente asociados con el manejo de información sensible y sistemas que operan de manera continua.

Los activos clasificados con criticidad alta corresponden principalmente a aquellos cuya afectación podría comprometer la privacidad de los clientes, la continuidad del servicio o la integridad de la información almacenada. Entre estos se encuentran las grabaciones de videovigilancia, los dispositivos DVR/NVR, las credenciales de acceso y la infraestructura de red. Estos activos fueron considerados críticos debido a que contienen información sensible o permiten el acceso directo al sistema de monitoreo.

Por ejemplo, las grabaciones de videovigilancia poseen una alta criticidad porque representan evidencia digital ante posibles incidentes de seguridad, robos o actos vandálicos. La pérdida, alteración o eliminación de esta información podría afectar tanto a los clientes como a la reputación de la empresa. De igual manera, las credenciales de acceso fueron clasificadas con criticidad alta debido a que permiten el control administrativo de los sistemas de videovigilancia y, en caso de compromiso, podrían facilitar accesos no autorizados a las cámaras y grabaciones.

Asimismo, la infraestructura de red y los routers representan activos críticos debido a que constituyen el punto principal de conexión entre los sistemas internos y el acceso remoto desde internet. Una vulnerabilidad en estos dispositivos podría comprometer múltiples servicios simultáneamente y ampliar significativamente la superficie de ataque.

La identificación y clasificación de estos activos permitió establecer prioridades dentro del análisis de riesgos y orientar la definición de controles de seguridad hacia los elementos con mayor impacto sobre la operación de la organización.

Tabla 1. Tabla de Activos.

Tipo de Activo	***Activo***	***Descripción***	***Ubicación***	***Responsable***	***Criticidad***	***Justificación***
Datos	*Grabaciones de videovigilancia*	*Videos capturados por cámaras de seguridad*	*DVR/NVR y almacenamiento local*	*Cliente / Empresa Caso de Estudio*	*Alta*	*Contienen evidencia crítica ante incidentes*
Datos	*Credenciales de acceso*	*Usuarios y contraseñas de DVR/NVR y apps*	*Dispositivos, bases de datos*	*Técnico / Cliente*	*Alta*	*Permiten el acceso total al sistema*
Datos	*Configuración de red*	*Parámetros de red, IP, puertos*	*Router / DVR*	*Técnico*	*Alta*	*Una mala configuración expone el sistema*
Datos	*Información de clientes*	*Datos personales y ubicación de instalaciones*	*Archivos digitales / registros*	*Administración*	*Alta*	*Información sensible protegida por ley*
Hardware	*DVR/NVR*	*Dispositivo central de grabación*	*Instalaciones del cliente*	*Técnico*	*Alta*	*Controla todo el sistema de vigilancia*
Hardware	*Cámaras de seguridad*	*Dispositivos de captura de video*	*Instalaciones fisicas*	*Cliente*	*Alta*	*Permiten la vigilancia del entorno*
Hardware	*Router / Red*	*Dispositivo de conexión a internet*	*Instalación del cliente*	*Proveedor / Técnico*	*Alta*	*Punto de acceso a la red y sistema*
Software	*Aplicación móvil de monitoreo*	*App para visualizar cámaras remotamente*	*Dispositivos móviles*	*Cliente*	*Media*	*Permite acceso remoto al sistema*
Personas	*Técnicos instaladores*	*Encargados de configuración y mantenimiento*	*Empresa Caso de Estudio*	*Empresa*	*Alta*	*Definen la seguridad del sistema*
Personas	*Cliente*	*Usuario final del sistema*	*Instalaciones del cliente*	*Cliente*	*Alta*	*Responsable del uso del sistema*
Procesos	*Instalación de sistemas*	*Configuración inicial de equipos*	*Sitio del cliente*	*Técnico*	*Alta*	*Define la seguridad inicial*
Procesos	*Mantenimiento técnico*	*Actualización y revisión de equipos*	*Sitio del cliente*	*Técnico*	*Media*	*Previene fallos y vulnerabilidades*
Procesos	*Monitoreo remoto*	*Supervisión del sistema de cámaras*	*Aplicación / red*	*Cliente*	*Media*	*Permite control y vigilancia continua*

Análisis y Evaluación de Riesgos

El análisis de riesgos realizado en *La Empresa Caso de Estudio* permitió identificar las principales amenazas y vulnerabilidades que afectan los sistemas de videovigilancia y acceso remoto implementados por la organización. Para determinar el nivel de riesgo de cada escenario analizado, se consideraron dos factores principales: la probabilidad de ocurrencia y el impacto potencial sobre la operación, la información y la reputación de la empresa.

La probabilidad fue evaluada teniendo en cuenta el nivel de exposición de los sistemas a internet, las vulnerabilidades detectadas y las prácticas de configuración observadas durante el diagnóstico inicial. En este sentido, riesgos relacionados con accesos no autorizados, espionaje remoto y explotación de puertos abiertos fueron clasificados con probabilidad alta debido a que los sistemas utilizan conexiones remotas expuestas directamente a internet y presentan debilidades como contraseñas inseguras o firmware desactualizado.

Por otra parte, el impacto fue determinado considerando las posibles consecuencias operativas, económicas y reputacionales derivadas de un incidente de seguridad. En el caso de un acceso no autorizado a las cámaras, el impacto sería alto debido a la posible afectación de la privacidad de los clientes, pérdida de evidencia digital y daño a la confianza depositada en la empresa. Asimismo, la manipulación o eliminación de grabaciones podría comprometer investigaciones relacionadas con incidentes de seguridad o generar conflictos legales con clientes afectados.

Los riesgos clasificados como altos corresponden principalmente a escenarios donde existe una combinación entre alta exposición y consecuencias críticas para la organización. Esto permitió priorizar la implementación de controles orientados a reducir la superficie de ataque y fortalecer la protección de los activos más sensibles.

Finalmente, el análisis de riesgos permitió evidenciar que la principal debilidad de la organización se encuentra en las configuraciones inseguras de acceso remoto, justificando la necesidad de implementar medidas de seguridad adicionales como VPN, segmentación de red, políticas de autenticación robusta y monitoreo de accesos.

Tabla 2. Análisis de Riesgos.

Activo	***Amenaza***	***Vulnerabilidad***	***Riesgo***	***Probabilidad***	***Impacto***	***Nivel***
DVR/NVR	*Acceso no autorizado*	*Credenciales por defecto o débiles*	*Control total del sistema de videovigilancia*	*Alta*	*Alta*	*Alto*
Cámaras de seguridad	*Espionaje remoto*	*Configuración insegura de acceso remoto*	*Visualización no autorizada de instalaciones*	*Alta*	*Alta*	*Alto*
Grabaciones de video	*Eliminación o alteración de datos*	*Falta de control de accesos y cifrado*	*Pérdida de evidencia en incidentes*	*Media*	*Alta*	*Alto*
Red (Router)	*Ataques externos (escaneo de puertos)*	*Puertos abiertos sin restricción*	*Intrusión a la red del cliente*	*Alta*	*Alta*	*Alto*
Aplicación móvil de monitoreo	*Intercepción de datos*	*Uso de conexiones no seguras (HTTP)*	*Fuga de información en tránsito*	*Media*	*Alta*	*Alto*
Credenciales de acceso	*Robo de credenciales*	*Mala gestión de usuarios y contraseñas*	*Suplantación de identidad*	*Alta*	*Alta*	*Alto*
Sistema de almacenamiento	*Fallo o corrupción de datos*	*Falta de copias de seguridad*	*Pérdida total de grabaciones*	*Media*	*Alta*	*Alto*
Equipos (cámaras/DVR)	*Malware o explotación de vulnerabilidades*	*Firmware desactualizado*	*Compromiso del sistema*	*Media*	*Media*	*Medio*
Servicio de monitoreo	*Interrupción del servicio*	*Falta de mantenimiento o fallos técnicos*	*Pérdida de disponibilidad del sistema*	*Baja*	*Alta*	*Medio*
Reputación de Empresa Caso de Estudio	*Incidentes de seguridad en clientes*	*Falta de políticas de seguridad*	*Pérdida de confianza del cliente*	*Media*	*Alta*	*Alto*

Conclusiones

El desarrollo del presente informe permitió aplicar de manera práctica los conocimientos adquiridos en el seminario de ciberseguridad organizacional dentro de un contexto real relacionado con sistemas de videovigilancia.

El análisis realizado evidenció que el acceso remoto inseguro constituye uno de los principales riesgos para la organización, especialmente debido a configuraciones deficientes, uso de credenciales débiles y exposición directa de servicios a internet.

Asimismo, se identificó que los activos más críticos corresponden a las grabaciones de videovigilancia, credenciales de acceso e infraestructura de red, debido a su impacto sobre la privacidad y continuidad operativa de los clientes.

La implementación de controles a través de políticas de autenticación robusta permite reducir significativamente los riesgos identificados y fortalecer la postura de seguridad de la organización.

Finalmente, el trabajo permitió comprender la importancia de integrar procesos de gestión de riesgos y buenas prácticas de seguridad desde la instalación y mantenimiento de sistemas tecnológicos, promoviendo una cultura organizacional orientada a la protección de la información.

Referencias

International Organization for Standardization. (2013). *ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems — Requirements*. ISO.

International Organization for Standardization. (2018). *ISO/IEC 27005:2018 Information technology — Security techniques — Information security risk management*. ISO.

Congreso de la República de Colombia. (2012). *Ley 1581 de 2012: Protección de datos personales*. Diario Oficial de Colombia.

National Institute of Standards and Technology. (2020). *Security and Privacy Controls for Information Systems and Organizations (SP 800-53 Rev. 5)*. NIST.

Stallings, W. (2018). *Cryptography and Network Security: Principles and Practice* (7th ed.). Pearson.

Whitman, M. E., & Mattord, H. J. (2021). *Principles of Information Security* (7th ed.). Cengage Learning.

Cisco Systems. (2021). *Network Security Best Practices for CCTV and IP Surveillance Systems*. Cisco Documentation.

Centro Criptológico Nacional. (2012). *Guía CCN-STIC 401: Seguridad en redes y comunicaciones*. CCN.