TRABAJO DE GRADO
Opción Seminario.

Ciberseguridad Organizacional: Un Enfoque Analítico para la Gestión del Riesgo Digital

Corporación Universitaria Remington.
Nombre de la facultad: Ingenierías
Nombre del programa académico: Ingeniería de Sistemas

Nombres de los estudiantes autores del trabajo de grado.

Darly Julieth Cuberos Rojas

Fabio Alexander Ramos Martínez

Jorge Leonardo Ramírez Restrepo - docente del seminario.
Seminario
2026

Agradecimientos

En el desarrollo de este caso, me gustaría agradecer especialmente a mis hijos por la motivación y las criticas frente a diversos problemas que se han presentado a lo largo de este camino, e sentido que mi vida a tomado otro rumbo diferente, doy gracias a Dios por la familia que tengo y doy gracias por que gracias a esta carrera y al conocimiento que he adquirido les puedo proporcionaron cosas muy valiosas, como tiempo que es algo que ya no se brinda por el mal manejo de la tecnología.

Queremos también agradecer a todos los textos, guías, libros de trabajo, módulos de la universidad y otros materiales que han sido de gran ayuda para el desarrollo de este caso de esta manera seguiremos investigando a lo largo de nuestra carrea universitaria y laboral ya que el crecimiento de la tecnología nos deja abrumados por los rápido cambio, tanto de las cosas buenas como de las malas que se pueden hacer con la tecnología, pero recuerden los buenos somos más y tenemos que proteger nuestros datos personales y familias. Recuerda la seguridad está a un clip de romperse lee y pregunta antes de dar un clip

Alexander Ramos

Tabla de Contenidos

Criterios generales del informe técnico

La transformación digital ha convertido a la información en uno de los activos más valiosos de cualquier organización. En el caso de las empresas de desarrollo de software, esta dependencia es aún más marcada, pues su operación, su ventaja competitiva y la confianza de sus clientes descansan sobre el código fuente, las bases de datos y los servicios tecnológicos que administran. La seguridad de la información, entendida como la protección de la confidencialidad, la integridad y la disponibilidad de los datos, deja de ser un asunto técnico aislado para convertirse en una responsabilidad organizacional que involucra personas, procesos, información y tecnología (ISO/IEC, 2022a).

SoftVision Technologies S.A.S. es una empresa que ha crecido de forma acelerada y que hoy opera bajo un modelo híbrido de trabajo, con más de 40 proyectos simultáneos para clientes de sectores altamente regulados como salud y gobierno. Este crecimiento, sin embargo, no ha estado acompañado de una gestión uniforme de la seguridad: coexisten equipos con distintos niveles de madurez, prácticas informales heredadas de etapas más pequeñas de la compañía y una cultura en la que la rapidez de entrega tiende a prevalecer sobre la revisión de riesgos. El resultado es una superficie de exposición amplia que ya ha generado incidentes con impacto operativo y reputacional.

Este informe presenta un análisis organizacional de la ciberseguridad de SoftVision con enfoque diagnóstico y propositivo. No pretende implementar soluciones tecnológicas específicas, sino identificar los activos de información más relevantes, reconocer las amenazas y vulnerabilidades que los afectan, valorar los riesgos asociados y proponer políticas, controles y estrategias de mejora fundamentadas en buenas prácticas y en el marco normativo aplicable. El documento se estructura siguiendo las etapas metodológicas trabajadas a lo largo del seminario, de manera que cada sección se articula con la anterior y contribuye a una visión integral del estado de seguridad de la organización.

La relevancia de este ejercicio trasciende lo académico. Para una empresa que proyecta expandirse hacia mercados internacionales y adoptar herramientas de inteligencia artificial en sus procesos de desarrollo, demostrar un manejo maduro de la seguridad de la información no es opcional: es un requisito comercial y legal. Un enfoque estructurado de gestión del riesgo permite a SoftVision proteger su información, cumplir sus obligaciones normativas, sostener la continuidad de su operación y fortalecer la confianza de sus clientes (ENISA, 2023).

Resumen

La transformación digital ha convertido la información en uno de los activos más valiosos para las organizaciones, especialmente para aquellas dedicadas al desarrollo de software y la prestación de servicios tecnológicos. Este escenario ha incrementado la necesidad de implementar estrategias de ciberseguridad que garanticen la confidencialidad, integridad y disponibilidad de la información frente a amenazas internas y externas. Asimismo, el cumplimiento de normas internacionales y de la legislación colombiana constituye un elemento esencial para fortalecer la gestión de la seguridad de la información y reducir los riesgos asociados al uso de las tecnologías.

El presente informe desarrolla un análisis técnico basado en el caso de la organización **SOFTVISION TECHNOLOGIES S.A.S.**, empresa colombiana dedicada al desarrollo de soluciones digitales para diferentes sectores económicos. A partir de la información suministrada, se realizó la identificación y valoración de los activos críticos, así como el análisis de las principales amenazas, vulnerabilidades y riesgos que pueden afectar la continuidad de las operaciones y la protección de la información. Como resultado, se formularon políticas, controles y recomendaciones orientadas al fortalecimiento de la ciberseguridad organizacional, alineadas con los lineamientos de la **ISO/IEC 27001:2022**, la **ISO/IEC 27005:2022**, la **Ley 1581 de 2012**, la **Ley 1273 de 2009** y las buenas prácticas propuestas por **ENISA**.

El desarrollo del caso evidencia la importancia de implementar un Sistema de Gestión de Seguridad de la Información (SGSI) basado en la gestión de riesgos y en un proceso de mejora continua, permitiendo fortalecer la protección de los activos de información y garantizar el cumplimiento de los requisitos legales y regulatorios. Finalmente, las propuestas planteadas contribuyen a disminuir la probabilidad e impacto de los incidentes de seguridad, fortalecer la cultura organizacional en materia de ciberseguridad y aumentar la resiliencia de la organización frente a las amenazas del entorno digital.

Palabras clave

- Ciberseguridad
- Gestión de riesgos
- Seguridad de la información
- ISO/IEC 27001
- Vulnerabilidades
- Activos de información
- Cumplimiento normativo
- Control de seguridad
- Riesgo
- Incidentes de seguridad

Marco conceptual y normativo

Conceptos fundamentales de ciberseguridad

Para sustentar el análisis de SoftVision es necesario precisar un conjunto de conceptos que constituyen el lenguaje común de la seguridad de la información. Estos conceptos permiten interpretar de manera técnica las situaciones observadas y justificar las decisiones que se proponen a lo largo del informe.

- **Seguridad de la información:** conjunto de medidas orientadas a proteger la información preservando tres propiedades esenciales: la confidencialidad (que solo accedan a ella las personas autorizadas), la integridad (que se mantenga completa y sin alteraciones no autorizadas) y la disponibilidad (que esté accesible cuando se requiera). Estas tres propiedades conforman la tríada CIA (ISO/IEC, 2022a).
- **Ciberseguridad:** disciplina que forma parte de la seguridad de la información y se concentra en proteger los sistemas, las redes, los servicios y los datos frente a amenazas provenientes del entorno digital, como ataques externos, código malicioso o accesos no autorizados (ENISA, 2023).
- **Activo de información:** todo recurso que tiene valor para la organización y que contribuye al cumplimiento de sus objetivos. Puede ser físico (equipos, servidores), digital (bases de datos, código fuente, servicios en la nube) o humano (el personal que gestiona la información) (ISO/IEC, 2022c).
- **Amenaza:** cualquier evento, situación o acción con la capacidad de afectar un activo y generar consecuencias negativas. Las amenazas pueden ser humanas, tecnológicas, naturales, físicas u operativas (ISO/IEC, 2022c).
- **Vulnerabilidad:** debilidad o condición existente en las personas, los procesos, la tecnología o la infraestructura que puede ser aprovechada por una amenaza para afectar un activo. A diferencia de la amenaza, la vulnerabilidad se encuentra dentro de la organización y puede reducirse mediante controles (ISO/IEC, 2022c).
- **Riesgo:** posibilidad de que una amenaza aproveche una vulnerabilidad y afecte un activo, generando un impacto. Se estima combinando la probabilidad de ocurrencia y la magnitud del impacto (ISO/IEC, 2022c).
- **Control de seguridad:** medida, acción o mecanismo implementado para prevenir, detectar, corregir o reducir un riesgo. Los controles pueden ser administrativos, técnicos o físicos (ISO/IEC, 2022b).
- **Incidente de seguridad:** evento que afecta o tiene el potencial de afectar la confidencialidad, la integridad o la disponibilidad de la información. No siempre

corresponde a un ataque: también puede originarse por error humano, fallas tecnológicas o eventos ambientales (NIST, 2012).

La comprensión de estos conceptos permite entender que las amenazas no afectan a las organizaciones de manera aleatoria, sino que aprovechan vulnerabilidades concretas para comprometer activos valiosos. En SoftVision, por ejemplo, el préstamo de credenciales (vulnerabilidad) facilita el acceso no autorizado (amenaza) a los repositorios de código (activo), generando el riesgo de robo o alteración del software desarrollado para los clientes.

Conceptos fundamentales de ciberseguridad

Ciberseguridad

La ciberseguridad comprende el conjunto de estrategias, procesos y tecnologías que tienen como objetivo proteger los sistemas informáticos, las redes, las aplicaciones y la información frente a amenazas provenientes del entorno digital. En el caso de **SoftVision Technologies S.A.S.**, la ciberseguridad es fundamental para proteger el desarrollo de software, los datos de los clientes y la infraestructura tecnológica, evitando incidentes que puedan afectar la continuidad del negocio.

Seguridad de la información

La seguridad de la información consiste en proteger la información durante todo su ciclo de vida, garantizando que solo las personas autorizadas puedan acceder a ella, que permanezca íntegra y que esté disponible cuando sea necesaria. Para SoftVision, este concepto es esencial debido a que administra información confidencial de clientes, proyectos y procesos internos que deben mantenerse protegidos.

Confidencialidad

La confidencialidad hace referencia a que la información únicamente puede ser consultada por personas autorizadas. Esto evita que terceros accedan a datos sensibles o confidenciales. En SoftVision, este principio cobra importancia al proteger el código fuente, las bases de datos y la información de los clientes frente a accesos no autorizados.

Integridad

La integridad garantiza que la información permanezca completa, correcta y libre de modificaciones no autorizadas. Mantener este principio permite asegurar que los datos utilizados por la organización sean confiables y no hayan sido alterados de forma intencional o accidental.

Disponibilidad

La disponibilidad asegura que la información, los sistemas y los servicios tecnológicos estén accesibles cuando los usuarios autorizados los requieran. En una empresa de desarrollo de software como SoftVision, la indisponibilidad de los servidores o aplicaciones puede generar retrasos en los proyectos y afectar la prestación de los servicios.

Activos de información

Los activos de información son todos aquellos recursos que tienen valor para la organización y que deben protegerse. Incluyen servidores, equipos de cómputo, bases de

datos, aplicaciones, repositorios de código fuente, servicios en la nube y el personal encargado de administrar la información. La identificación de estos activos permite establecer prioridades de protección dentro del análisis realizado.

Amenazas

Las amenazas son eventos o acciones que tienen la capacidad de causar daño a los activos de información. Estas pueden originarse por ataques cibernéticos, errores humanos, fallas tecnológicas o desastres naturales. Durante el análisis de SoftVision se identificaron amenazas como el acceso no autorizado, el robo de información y los ataques de phishing.

Vulnerabilidades

Las vulnerabilidades corresponden a las debilidades presentes en los procesos, las personas, los sistemas o la infraestructura tecnológica que pueden ser aprovechadas por una amenaza. En el caso analizado, se identificaron vulnerabilidades como el préstamo de credenciales, la ausencia de autenticación multifactor, el uso de dispositivos personales y la permanencia de cuentas de usuarios inactivos.

Riesgos

El riesgo representa la posibilidad de que una amenaza aproveche una vulnerabilidad y afecte un activo de información, ocasionando pérdidas económicas, interrupciones operativas, incumplimiento legal o afectaciones a la reputación de la organización. La gestión de riesgos permite priorizar las acciones necesarias para reducir la probabilidad de ocurrencia y minimizar su impacto.

Controles de seguridad

Los controles de seguridad son las medidas implementadas para prevenir, detectar o reducir los riesgos que afectan la información y los sistemas. Estos controles pueden ser administrativos, técnicos o físicos. En SoftVision se proponen controles como la autenticación multifactor, la gestión adecuada de privilegios, la capacitación en ciberseguridad, la realización de copias de seguridad, el monitoreo continuo y la actualización de los sistemas, con el fin de fortalecer la protección de los activos de información.

Relación de los conceptos con el informe

Los conceptos anteriores constituyen la base teórica del presente informe y permiten comprender cómo una amenaza puede aprovechar una vulnerabilidad para afectar un activo de información y generar un riesgo para la organización. A partir de este análisis fue posible identificar las principales debilidades de **SoftVision Technologies S.A.S.** y proponer controles alineados con las buenas prácticas de la **ISO/IEC 27001:2022**, la **ISO/IEC 27005:2022**, la **Ley 1581 de 2012**, la **Ley 1273 de 2009** y las recomendaciones de **ENISA**, con el propósito de fortalecer la seguridad de la información y mejorar la postura de ciberseguridad de la organización.

ENISA. (2023). *ENISA Threat Landscape 2023*. European Union Agency for Cybersecurity. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023

ISO/IEC. (2022a). *ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements*. International Organization for Standardization.

ISO/IEC. (2022b). *ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection — Information security controls*. International Organization for Standardization.

ISO/IEC. (2022c). *ISO/IEC 27005:2022 Information security, cybersecurity and privacy protection — Guidance on managing information security risks*. International Organization for Standardization.

Congreso de Colombia. (2009). *Ley 1273 de 2009. Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado denominado "de la protección de la información y de los datos" y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones*. Diario Oficial No. 47.223.

Congreso de Colombia. (2012). *Ley 1581 de 2012. Por la cual se dictan disposiciones generales para la protección de datos personales*. Diario Oficial No. 48.587.

National Institute of Standards and Technology. (2012). *Computer Security Incident Handling Guide (Special Publication 800-61 Revision 2)*. U.S. Department of Commerce.

Marco normativo

Tabla 1. Normatividad aplicable.

Norma o estándar	***Propósito***	***Aplicabilidad en SOFTVISION***
ISO/IEC 27001:2022	Implementar un SGSI basado en mejora continua.	Permite establecer políticas, controles, gestión de activos y tratamiento de riesgos.
ISO/IEC 27005:2022	Gestión del riesgo en seguridad de la información.	Facilita identificar amenazas, vulnerabilidades y definir planes de tratamiento.
Ley 1581 de 2012	La Protección de datos personales.	Aplica debido al tratamiento de información de clientes y colaboradores.
Ley 1273 de 2009	Protección frente a delitos informáticos.	Protege los sistemas y la información contra accesos no

		autorizados y ataques informáticos.
ENISA	Buenas prácticas de ciberseguridad para blindar la organización.	Proporciona recomendaciones sobre autenticación, respuesta a incidentes, nube y DevSecOps.

Justificación

Las normas y leyes nos permiten seleccionar la constituyen del marco de referencia para fortalecer la seguridad de la información de SOFTVISION TECHNOLOGIES S.A.S. La implementación de las normar **ISO/IEC 27001** permite establecer un Sistema de Gestión de Seguridad de la Información basado en las políticas que ha establecido la organización, los controles y la mejora continua, mientras que la **ISO/IEC 27005** facilita la identificación, análisis y tratamiento de los risgos presentes en la organización.
Por otra parte, la **Ley 1581 de 2012** obliga a proteger los datos personales tratados por la empresa, mientras que la **Ley 1273 de 2009** establece sanciones frente a conductas que afecten la confidencialidad, integridad y disponibilidad de los sitemas y software informáticos. Las recomendaciones de **ENISA** son complementen este marco mediante prácticas internacionales orientadas a fortalecer la resiliencia organizacional frente a las amenazas informáticas y los ataque de ranzonware.

ISO/IEC. (2022b). *ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection — Information security controls*. International Organization for Standardization.

ISO/IEC. (2022c). *ISO/IEC 27005:2022 Information security, cybersecurity and privacy protection — Guidance on managing information security risks*. International Organization for Standardization.

Congreso de Colombia. (2009). *Ley 1273 de 2009. Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado denominado "de la protección de la información y de los datos" y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones*. Diario Oficial No. 47.223.

Congreso de Colombia. (2012). *Ley 1581 de 2012. Por la cual se dictan disposiciones generales para la protección de datos personales*. Diario Oficial No. 48.587.

National Institute of Standards and Technology. (2012). *Computer Security Incident Handling Guide (Special Publication 800-61 Revision 2)*. U.S. Department of Commerce.

Marco contextual
Descripción de la organización

SoftVision Technologies S.A.S. es una empresa colombiana dedicada al diseño, desarrollo, implementación y mantenimiento de soluciones de software para organizaciones públicas y privadas. Con más de doce años de experiencia, atiende a clientes de los sectores salud, educación, logística, comercio y gobierno, y desarrolla de manera simultánea más de 40 proyectos tecnológicos para clientes nacionales. La compañía cuenta con una sede principal y opera bajo un modelo híbrido de trabajo presencial y remoto, con cerca de 210 colaboradores entre desarrolladores, analistas, arquitectos de software, líderes de proyecto, especialistas en infraestructura, personal administrativo y directivos.

La estructura organizacional comprende las áreas de Gerencia General, Dirección de Tecnología, Arquitectura de Software, Desarrollo Frontend, Desarrollo Backend, Calidad y Pruebas, Gestión de Infraestructura, Gestión de Proyectos, Atención al Cliente, Talento Humano, Comercial y Ventas, y Contabilidad y Finanzas. El área tecnológica, responsable directa de buena parte de los activos de información, está conformada por el Director de Tecnología, un Arquitecto de Soluciones, Administradores de Infraestructura, especialistas DevOps, desarrolladores, analistas QA y analistas de seguridad.

Problemática identificada

Una firma consultora especializada realizó una evaluación preliminar y documentó catorce situaciones que evidencian debilidades transversales en la gestión de la seguridad de la información:

1. Algunos desarrolladores comparten credenciales de acceso temporalmente para agilizar tareas técnicas.
2. No existe una política formal de clasificación de la información.
3. Algunos proyectos almacenan documentación en plataformas externas no autorizadas.
4. Existen usuarios con privilegios administrativos superiores a los requeridos por sus funciones.
5. No todos los accesos a plataformas críticas utilizan autenticación multifactor (MFA).
6. Algunos colaboradores utilizan equipos personales para acceder a entornos corporativos.
7. No existe un procedimiento formal documentado para la gestión de incidentes de seguridad.

8. Los respaldos se realizan regularmente, pero no hay pruebas documentadas recientes de recuperación.
9. Algunos ambientes de desarrollo contienen copias de bases de datos con información real de clientes.
10. No se realizan campañas periódicas de sensibilización en ciberseguridad.
11. Se identificaron cuentas activas pertenecientes a excolaboradores.
12. No existe un inventario actualizado de activos de información.
13. Algunos proyectos manejan configuraciones de acceso diferentes sin lineamientos comunes.
14. Existen diferencias en las prácticas de seguridad aplicadas entre equipos de desarrollo.

Estas debilidades no son hipotéticas. Durante los últimos tres años se materializaron en cinco incidentes: un ataque de phishing dirigido a un desarrollador, seguido de intentos de acceso no autorizado a los repositorios de código; la indisponibilidad temporal de una aplicación usada por varios clientes por una configuración incorrecta durante una actualización; la exposición accidental de información sensible en un repositorio compartido entre equipos; el hurto de un computador portátil con documentación técnica de proyectos activos; y la eliminación accidental de información en un ambiente de pruebas, que requirió recurrir a los respaldos institucionales. En conjunto, la problemática revela una organización técnicamente capaz pero con controles de gobierno de la seguridad inmaduros y heterogéneos, situación agravada por su crecimiento acelerado (ENISA, 2023).

Identificación y analisis de activos

Inventario de activos

Antes de proteger la información es indispensable identificar qué activos posee la organización y qué valor tienen. A partir de la información del caso se identificaron los siguientes activos, clasificados en físicos, digitales y humanos, con su respectivo nivel de criticidad (Alta, Media o Baja) según su importancia para la operación y las consecuencias de su pérdida o alteración (ISO/IEC, 2022c).

Tabla 2. Inventario de activos

Activo	Tipo	Función dentro de la organización	Criticidad
Repositorios de código fuente	Digital	Almacenan el código de las soluciones desarrolladas para los clientes; constituyen la propiedad intelectual de la empresa.	**Alta**
Infraestructura CI/CD	Digital	Automatiza la integración, las pruebas y el despliegue del software a los ambientes productivos.	**Alta**
Ambientes de producción	Digital	Soportan las aplicaciones en funcionamiento que usan los clientes.	**Alta**
Bases de datos de clientes	Digital	Contienen datos de salud, educación, comercio y gobierno de los clientes.	**Alta**
Plataforma de respaldo (backups)	Digital	Conserva las copias de seguridad de los sistemas e información institucional.	**Alta**
Sistemas ERP y CRM	Digital	Soportan la contabilidad, la facturación, los contratos y la relación con clientes.	**Alta**
Nube pública	Digital	Provee cómputo, almacenamiento y servicios para el desarrollo y la operación.	**Alta**
Ambientes de desarrollo y pruebas	Digital	Espacios donde se escribe y se valida el código nuevo.	**Media**
Computadores portátiles (180)	Físico	Equipos de trabajo del personal en el modelo híbrido.	**Media**

Red WiFi corporativa	Físico	Red inalámbrica que soporta la conectividad en la sede.	**Media**
Personal técnico especializado	Humano	Administradores de infraestructura, DevOps y analistas de seguridad que gestionan accesos y servicios.	**Alta**
Red WiFi corporativa	Físico	Red inalámbrica que soporta la conectividad en la sede.	**Media**

JUSTIFICACIÓN DE LOS ACTIVOS

Los activos seleccionados corresponden a aquellos que soportan los procesos críticos de desarrollo de software mediante el desarrollo, la administración tecnológica y prestación de los servicios descritos en el caso de estudio. La clasificación se realizó considerando el impacto que tendría la pérdida de esta información, la alteración o indisponibilidad sobre la operación de la empresa sería un caos, la continuidad de los proyectos tecnológicos y el cumplimiento de los compromisos adquiridos con clientes nacionales e internacionales no nos permite tener esta clase de errores.

La mayor parte de los activos fueron clasificados con criticidad alta, debido a que almacenan información sensible de nuestros clientes, soportan la infraestructura tecnológica, la organización practica directamente en los procesos estratégicos de la organización para las organizaciones a las cuales les prestamos los servicios de desarrollo. Esta valoración se fundamenta en los principios de confidencialidad, integridad y disponibilidad de los datos definidos por la ISO/IEC 27001 y en la metodología de gestión de riesgos establecida por la ISO/IEC 27005. Adicionalmente, el tratamiento de datos personales que exige el cumplimiento de la Ley 1581 de 2012, mientras que la Ley 1273 de 2009 protege los sistemas frente a delitos informáticos. Finalmente, las recomendaciones de ENISA respaldan la implementación de controles preventivos y correctivos que permitan fortalecer la resiliencia de la organización frente a las amenazas cibernéticas.

Analisis de amenazas y vulnerabilidades

Sobre los activos identificados se analizaron las principales amenazas y las vulnerabilidades que las facilitan. Se mantuvo la coherencia entre las tres columnas, evitando amenazas y vulnerabilidades genéricas y vinculando cada una a las situaciones reales del caso (NIST, 2024).

Activo afectado	Amenaza (¿qué puede pasar?)	Vulnerabilidad (¿qué lo facilita?)
Repositorios de código fuente	Acceso no autorizado y robo o alteración del código.	Credenciales compartidas, ausencia de MFA y cuentas activas de excolaboradores.
Bases de datos de clientes	Fuga o robo de información personal y confidencial.	Uso de datos reales de clientes en ambientes de desarrollo sin enmascaramiento.
Computadores portátiles	Robo físico del equipo y de la información almacenada localmente.	Equipos sin cifrado de disco y almacenamiento local de documentación técnica sensible.
Plataforma de respaldo	Falla en la restauración de la información tras un incidente.	Ausencia de pruebas documentadas de recuperación de los respaldos.
Ambientes de producción	Indisponibilidad del servicio para los clientes.	Configuraciones de seguridad heterogéneas por falta de lineamientos unificados entre equipos.
Correo corporativo / usuarios	Phishing e ingeniería social que comprometen credenciales.	Falta de sensibilización y de campañas periódicas de concientización.
Nube pública y servicios de terceros	Configuraciones inseguras que exponen recursos.	Ausencia de un inventario de activos y de estándares de configuración segura.

datos reales de clientes en ambientes de prueba concentra el riesgo legal más severo, pues traslada información sensible a entornos con menores controles. Estas dos vulnerabilidades —accesos débiles y datos productivos en desarrollo— son las que requieren atención prioritaria (ENISA, 2023).

Análisis y gestión de riesgos

La valoración de los riesgos se realizó siguiendo las directrices de la norma ISO/IEC 27005:2022, que propone un ciclo de identificación, análisis, evaluación, tratamiento y monitoreo del riesgo (ISO/IEC, 2022c). Para cada riesgo se estimaron dos variables:

- **Impacto (I):** magnitud de las consecuencias para la organización si el riesgo se materializa. Se valora en tres niveles: Bajo (consecuencias menores y recuperables), Medio (afecta parcialmente algunos procesos) y Alto (compromete procesos críticos, la continuidad o el cumplimiento legal).
- **Probabilidad (P):** posibilidad de que el riesgo llegue a ocurrir, considerando la frecuencia potencial, la existencia de controles y los antecedentes. Se valora como Baja, Media o Alta. El nivel de riesgo se determina cruzando ambas variables en una matriz de valoración. La interpretación de resultados orienta la prioridad de tratamiento: los riesgos de nivel Bajo se monitorean, los de nivel Medio requieren implementar mejoras y los de nivel Alto deben atenderse de forma prioritaria.

Impacto \ Probabilidad	Baja	Media	Alta
Alto	Medio	Alto	Alto
Medio	Bajo	Medio	Alto
Bajo	Bajo	Bajo	Medio

Matriz de riesgos

Aplicando la metodología descrita a los activos, amenazas y vulnerabilidades identificados, se construyó la siguiente matriz de riesgos para SoftVision. Cada valoración se acompaña de su nivel resultante.

ID	Riesgo	Activo	Impacto	Prob.	Nivel
R1	Acceso no autorizado y robo o alteración del código en los repositorios.	Repositorios	Alto	Alta	**Alto**
ID	**Riesgo**	**Activo**	**Impacto**	**Prob.**	**Nivel**
R2	Fuga de datos personales de clientes por su uso en ambientes de prueba (Ley 1581).	BD clientes	Alto	Alta	**Alto**
R3	Uso indebido de accesos por cuentas activas de excolaboradores.	Repositorios / sistemas	Alto	Media	**Alto**
R4	Imposibilidad de recuperar la operación por respaldos no verificados.	Backups / producción	Alto	Media	**Alto**
R5	Indisponibilidad de servicios por configuraciones incorrectas en el despliegue.	Producción	Alto	Media	**Alto**
R6	Pérdida o exposición de información por hurto de portátiles sin cifrado.	Portátiles	Medio	Media	**Medio**
R7	Compromiso de credenciales por phishing e ingeniería social.	Correo / usuarios	Medio	Alta	**Alto**

Análisis de los riesgos prioritarios: los riesgos R1 y R2 se ubican en el nivel más alto porque combinan un impacto severo con una probabilidad elevada. En ambos casos las vulnerabilidades ya están presentes y activas —credenciales compartidas sin MFA y datos reales en desarrollo— y existen antecedentes de incidentes que confirman su materialización. R7 (phishing) también alcanza nivel alto por su alta frecuencia y por ser la puerta de entrada del incidente que derivó en intentos de acceso a los repositorios. Los riesgos R3, R4 y R5 son de nivel alto por su impacto sobre la continuidad y el cumplimiento, aunque con probabilidad media. R6, asociado al hurto de equipos, se clasifica como medio porque su impacto puede acotarse mediante cifrado. La priorización

indica que SoftVision debe intervenir de forma inmediata sobre la gestión de accesos y la protección de datos personales, ya que allí se concentra la mayor exposición (ISO/IEC, 2022c).

Políticas y controles de seguridad

A partir de los riesgos priorizados se formulan políticas y controles orientados a reducir la probabilidad de ocurrencia y a mitigar el impacto. Las políticas establecen lineamientos generales y los controles concretan las medidas administrativas, técnicas y físicas que los hacen efectivos (ISO/IEC, 2022b).

Cada política se redacta siguiendo la estructura recomendada (nombre, objetivo, alcance, lineamientos y responsables) y responde a un riesgo específico.

Política	Objetivo y lineamientos principales	Riesgo que mitiga
Política de gestión de usuarios y control de accesos	Prohibir el préstamo de credenciales, exigir credenciales individuales y autenticación multifactor en todos los sistemas críticos, aplicar el principio de mínimo privilegio y revisar periódicamente los permisos. Responsables: Dirección de Tecnología y Talento Humano.	R1, R3, R7
Política de privacidad y protección de datos personales	Prohibir el uso de datos reales de clientes en ambientes de desarrollo y pruebas; todo dato productivo debe anonimizarse o enmascararse. Definir el tratamiento conforme a la Ley 1581. Responsables: Dirección de Tecnología y Oficial de Protección de Datos.	R2
Política de clasificación y manejo de la información	Clasificar la información según su nivel de sensibilidad y definir reglas de almacenamiento, prohibiendo el uso de plataformas externas no autorizadas. Responsables: cada líder de proyecto y Dirección de Tecnología.	R2, R6
Política de uso de dispositivos y trabajo remoto	Debido al modelo de trabajo híbrido implementado por la organización, resulta indispensable establecer controles para proteger la información cuando los colaboradores acceden a los recursos corporativos desde ubicaciones externas. En consecuencia, únicamente podrán conectarse a los sistemas	R6

	institucionales los equipos previamente autorizados por el área de Tecnología. (BYOD). Responsables de la Gestión de Infraestructura.	
Política de respaldo y recuperación de la información	Exigir copias de seguridad automáticas y programar pruebas periódicas y documentadas de restauración. Responsables, Administradores de Infraestructura.	R4
Política de gestión de cambios y despliegues	El objetivo de esta política es garantizar que todas las modificaciones realizadas en aplicaciones, servidores o infraestructura tecnológica sean evaluadas antes de implementarse en producción. Ningún cambio podrá ejecutarse sin haber sido previamente documentado, probado y aprobado por los responsables correspondientes.	R5
Política de gestión de incidentes de seguridad	Una vez reportado el incidente, el equipo de seguridad deberá evaluar su impacto, implementar las acciones de contención necesarias y documentar las lecciones aprendidas para prevenir su repetición. Los Analistas de Seguridad serán responsables de coordinar este proceso y presentar informes periódicos a la Dirección de Tecnología: Analistas de Seguridad.	Esta política contribuye a reducir los riesgos **R1, R5 y R7**.

Controles propuestos

Los controles se organizan en tres categorías —administrativos, técnicos y físicos— para asegurar una defensa en profundidad que combine reglas organizacionales, mecanismos tecnológicos y protección del entorno físico (ISO/IEC, 2022b; NIST, 2024).

Controles administrativos

Riesgo	Control administrativo	¿Por qué sirve?
R1, R3	Procedimiento formal de altas y bajas (onboarding/offboarding) sincronizado con Talento Humano y revisión periódica de roles y privilegios.	Elimina cuentas de excolaboradores el mismo día de su salida y evita la acumulación de privilegios innecesarios.
R7	Programa permanente de sensibilización con simulacros de phishing trimestrales y acuerdos de confidencialidad.	Reduce la probabilidad de éxito de la ingeniería social al fortalecer el criterio de los colaboradores.
R2	Capacitación en protección de datos personales y designación de un responsable del tratamiento de datos.	Fortalece el cumplimiento de la Ley 1581 y la responsabilidad demostrada (SIC, 2020).

Controles técnicos

Riesgo	Control técnico	¿Por qué sirve?
R1, R7	Inicio de sesión único (SSO) con MFA obligatorio, integrado con los repositorios (GitHub/GitLab).	Anula el uso de credenciales compartidas y frena los accesos externos derivados de phishing.
R2	Herramientas de enmascaramiento y anonimización de datos para los ambientes de desarrollo y pruebas.	Permite probar con datos de estructura equivalente sin exponer información real de clientes.
R4	Respaldos automatizados con pruebas de restauración programadas y almacenamiento de copias inmutables fuera de la red.	Garantiza que los backups sean recuperables antes de una emergencia real.
R5	Integración de análisis estático de seguridad (SAST) y validaciones automáticas en el pipeline CI/CD (enfoque DevSecOps).	Detecta configuraciones y vulnerabilidades antes de llegar a producción (OWASP Foundation, 2022).
R6	Cifrado de disco en todos los portátiles y controles de fuga de información (DLP).	Reduce el impacto del hurto de equipos al inutilizar la información almacenada.
Riesgo	**Control técnico**	**¿Por qué sirve?**
R2, R7	Cifrado de bases de datos y comunicaciones, filtros antispam y autenticación de correo (SPF, DKIM, DMARC).	Protege la confidencialidad de los datos y dificulta la suplantación por correo.

Controles físicos

Riesgo	Control físico	¿Por qué sirve?
R6	Registro y control de salida de equipos, videovigilancia (CCTV) e inventario actualizado de activos.	Disuade y permite rastrear el hurto o extravío de equipos con información sensible.
R4, R5	Sistemas de respaldo eléctrico (UPS) y control ambiental en las áreas que soportan infraestructura crítica.	Reduce la indisponibilidad por fallas eléctricas o ambientales.

R1	Control de acceso físico a las áreas donde se administran servicios críticos mediante tarjeta o biometría.	Restringe la manipulación no autorizada de la infraestructura sensible.

Justificación: el conjunto de políticas y controles busca reducir el riesgo sin frenar la operación. Al automatizar procesos como el bloqueo de cuentas, la generación de datos enmascarados y las validaciones de seguridad en el pipeline, SoftVision protege sus activos y cumple con la Ley 1581 de 2012 mientras conserva la agilidad que exige el desarrollo de software. Este enfoque es coherente con la intención estratégica de la empresa de fortalecer sus prácticas DevSecOps (OWASP Foundation, 2022).

Gestión de incidentes y continuidad del negocio

Aun cuando una organización implemente políticas de seguridad, controles tecnológicos y buenas prácticas para proteger sus activos de información, siempre existe la posibilidad de que ocurra un incidente de seguridad. Ningún sistema es completamente inmune a amenazas internas o externas, por lo que resulta indispensable contar con un proceso estructurado que permita responder de manera oportuna y garantizar la continuidad de las operaciones. En el caso de SoftVision Technologies S.A.S., empresa dedicada al desarrollo de software y la prestación de servicios tecnológicos, la gestión de incidentes y la continuidad del negocio representan elementos fundamentales para minimizar el impacto de eventos que puedan comprometer la información, los servicios o la infraestructura tecnológica.

Durante el análisis realizado se identificaron diferentes riesgos que podrían materializarse en incidentes de seguridad si no se implementan los controles adecuados. Entre ellos se encuentran el acceso no autorizado a los sistemas debido al uso compartido de credenciales, la exposición de información confidencial por el almacenamiento de archivos en plataformas no autorizadas, la pérdida de datos ocasionada por fallas en las copias de seguridad, errores durante los despliegues de nuevas versiones de software y ataques de ingeniería social, como campañas de phishing dirigidas a los colaboradores de la organización.

Ante cualquiera de estas situaciones, la empresa debe contar con un procedimiento claramente definido que permita identificar el incidente, registrar la información relevante, evaluar su nivel de criticidad y ejecutar acciones inmediatas para contener el problema. Posteriormente, será necesario analizar las causas que originaron el incidente, recuperar los servicios afectados y documentar las lecciones aprendidas con el fin de evitar que situaciones similares vuelvan a presentarse. Este proceso debe estar coordinado por el equipo de seguridad informática en conjunto con las áreas de infraestructura, desarrollo y dirección tecnológica, garantizando una respuesta organizada y eficiente.

Incidente potencial	¿Cómo ocurre?	Impacto para la empresa
Phishing exitoso	Un desarrollador entrega sus credenciales al caer en un correo fraudulento.	Alto. Acceso a proyectos privados, robo de propiedad intelectual o inyección de código malicioso.
Caída de un servicio	Un error de configuración se despliega a producción.	Crítico. Clientes sin servicio, incremento de solicitudes de soporte y posible incumplimiento contractual.
Hurto de portátil	Un equipo con documentación técnica es sustraído fuera de la sede.	Medio. Pérdida del equipo y exposición de información si no estaba cifrada.
Exposición de datos	Información sensible queda accesible en un repositorio compartido.	Alto. Riesgo de fuga de datos personales y sanciones bajo la Ley 1581.

Finalmente, la gestión de incidentes y la continuidad del negocio no deben entenderse como actividades independientes, sino como procesos permanentes que forman parte del Sistema de Gestión de Seguridad de la Información (SGSI). Su adecuada implementación permitirá que **SoftVision Technologies S.A.S.** responda de manera rápida y organizada frente a cualquier evento de seguridad, reduzca el impacto sobre sus activos de información, garantice la continuidad de sus servicios y fortalezca la confianza de sus clientes y demás partes interesadas. Además, estas acciones contribuyen al cumplimiento de las buenas prácticas establecidas en la **ISO/IEC 27001:2022**, la **ISO/IEC 27005:2022** y la legislación colombiana en materia de protección de la información y gestión de riesgos, consolidando una cultura organizacional orientada a la prevención, la resiliencia y la mejora continua.

Cultura organizacional en ciberseguridad

El diagnóstico evidenció que el mayor desafío de SoftVision no es exclusivamente tecnológico, sino cultural. La cultura organizacional —el conjunto de valores, hábitos y prácticas compartidas— determina cómo las personas protegen la información, cumplen las políticas y reportan los incidentes. El factor humano puede actuar como el principal control o como la principal vulnerabilidad (ENISA, 2023).

Estado actual

Las entrevistas revelaron comportamientos que debilitan la seguridad: muchos desarrolladores consideran que la seguridad ralentiza el desarrollo; existe una confianza excesiva en el conocimiento técnico individual como única defensa; se prioriza la rapidez de entrega sobre la revisión de riesgos; no todos reportan oportunamente los incidentes menores; las capacitaciones son esporádicas; y la responsabilidad de la seguridad se asocia únicamente a los especialistas del área. La siguiente tabla relaciona estas situaciones con el riesgo que generan.

Situación observada	Riesgo asociado
Se percibe la seguridad como un obstáculo para la entrega.	Evasión de controles y despliegue de código vulnerable para cumplir plazos.
Confianza desmedida en el conocimiento técnico individual.	Baja sospecha ante esquemas de ingeniería social dirigidos a la persona.
La seguridad se asume como responsabilidad exclusiva del área especializada.	Omisión en el reporte de incidentes menores e inacción ante brechas evidentes.
Capacitaciones esporádicas y sin continuidad.	Persistencia de malas prácticas y errores humanos recurrentes.

Fortalezas

Pese a lo anterior, SoftVision cuenta con fortalezas aprovechables: un equipo técnico altamente calificado, la existencia de analistas de seguridad en la estructura, el interés declarado de la alta dirección por fortalecer prácticas DevSecOps y una intención estratégica de crecimiento que exige madurar la seguridad. Estas condiciones facilitan la adopción de una cultura de seguridad si se canalizan adecuadamente.

Oportunidades de mejora

Las principales oportunidades consisten en transformar la percepción de la seguridad como una barrera y en distribuir la responsabilidad más allá del área especializada. La siguiente tabla propone acciones concretas frente a los hallazgos culturales.

Hallazgo	Acción de mejora

Se prioriza la entrega sobre el análisis de riesgos.	Integrar pruebas de seguridad automáticas (SAST) en el pipeline, de modo que la seguridad no dependa de pasos manuales adicionales.
La seguridad se ve como una molestia.	Implementar la estrategia de Security Champions: un desarrollador líder de seguridad por equipo.
Poca preparación ante engaños.	Realizar simulacros de phishing trimestrales y reconocer a quienes reporten correctamente.
Bajo reporte de incidentes menores.	Habilitar un canal de reporte sin temor a represalias y promover el aprendizaje organizacional.

Recomendaciones y beneficios esperados

Se recomienda a SoftVision establecer un programa permanente de capacitación y sensibilización, procesos de inducción y reinducción en seguridad desde la vinculación, campañas de concientización, y la participación visible de la alta dirección en las iniciativas de seguridad. Al implementar estas acciones, la seguridad deja de ser una imposición y se convierte en un hábito. Contar con un Security Champion en cada equipo hace que las buenas prácticas formen parte natural del trabajo diario, de manera que los desarrolladores cuiden el código por convicción y no por temor. El beneficio esperado es una reducción sostenida de los incidentes por error humano, una respuesta más rápida ante situaciones de riesgo y una organización más resiliente, capaz de sostener su crecimiento y su expansión internacional sobre una base de confianza (ENISA, 2023; NIST, 2024).

Metodología de análisis

La valoración de los riesgos se realizó siguiendo las directrices de la norma ISO/IEC 27005:2022, que propone un ciclo de identificación, análisis, evaluación, tratamiento y monitoreo del riesgo (ISO/IEC, 2022c). Para cada riesgo se estimaron dos variables:

- **Impacto (I):** magnitud de las consecuencias para la organización si el riesgo se materializa. Se valora en tres niveles: Bajo (consecuencias menores y recuperables), Medio (afecta parcialmente algunos procesos) y Alto (compromete procesos críticos, la continuidad o el cumplimiento legal).
- **Probabilidad (P):** posibilidad de que el riesgo llegue a ocurrir, considerando la frecuencia potencial, la existencia de controles y los antecedentes. Se valora como Baja, Media o Alta. El nivel de riesgo se determina cruzando ambas variables en una matriz de valoración. La interpretación de resultados orienta la prioridad de

tratamiento: los riesgos de nivel Bajo se monitorean, los de nivel Medio requieren implementar mejoras y los de nivel Alto deben atenderse de forma prioritaria.

Impacto \ Probabilidad	Baja	Media	Alta
Alto	Medio	Alto	Alto
Medio	Bajo	Medio	Alto
Bajo	Bajo	Bajo	Medio

Matriz de riesgos

Tabla 4. Matriz de riesgos
Aplicando la metodología descrita a los activos, amenazas y vulnerabilidades identificados, se construyó la siguiente matriz de riesgos para SoftVision. Cada valoración se acompaña de su nivel resultante.

ID	Riesgo	Activo	Impacto	Prob.	Nivel
R1	Acceso no autorizado y robo o alteración del código en los repositorios.	Repositorios	Alto	Alta	**Alto**
ID	**Riesgo**	**Activo**	**Impacto**	**Prob.**	**Nivel**
R2	Fuga de datos personales de clientes por su uso en ambientes de prueba (Ley 1581).	BD clientes	Alto	Alta	**Alto**
R3	Uso indebido de accesos por cuentas activas de excolaboradores.	Repositorios / sistemas	Alto	Media	**Alto**
R4	Imposibilidad de recuperar la operación por respaldos no verificados.	Backups / producción	Alto	Media	**Alto**
R5	Indisponibilidad de servicios por configuraciones incorrectas en el despliegue.	Producción	Alto	Media	**Alto**
R6	Pérdida o exposición de información por hurto de portátiles sin cifrado.	Portátiles	Medio	Media	**Medio**

R7	Compromiso de credenciales por phishing e ingeniería social.	Correo / usuarios	Medio	Alta	**Alto**

Análisis de los riesgos prioritarios: los riesgos R1 y R2 se ubican en el nivel más alto porque combinan un impacto severo con una probabilidad elevada. En ambos casos las vulnerabilidades ya están presentes y activas —credenciales compartidas sin MFA y datos reales en desarrollo— y existen antecedentes de incidentes que confirman su materialización. R7 (phishing) también alcanza nivel alto por su alta frecuencia y por ser la puerta de entrada del incidente que derivó en intentos de acceso a los repositorios. Los riesgos R3, R4 y R5 son de nivel alto por su impacto sobre la continuidad y el cumplimiento, aunque con probabilidad media. R6, asociado al hurto de equipos, se clasifica como medio porque su impacto puede acotarse mediante cifrado. La priorización indica que SoftVision debe intervenir de forma inmediata sobre la gestión de accesos y la protección de datos personales, ya que allí se concentra la mayor exposición (ISO/IEC, 2022c).

Conclusiones

1. SoftVision Technologies S.A.S. presenta un nivel de exposición al riesgo alto, derivado de priorizar la velocidad de entrega del software sobre la protección elemental de sus accesos y credenciales, en un contexto de crecimiento acelerado que ha generado prácticas de seguridad heterogéneas entre equipos.

2. La ausencia de controles básicos —autenticación multifactor obligatoria y baja inmediata de cuentas de excolaboradores— constituye la brecha más peligrosa de la organización, y fue precisamente la que habilitó los intentos de acceso no autorizado a los repositorios tras el incidente de phishing.

3. El uso de datos reales de clientes en ambientes de desarrollo incumple la Ley 1581 de 2012 y expone a la empresa a sanciones de la Superintendencia de Industria y Comercio, además de comprometer la privacidad de usuarios finales de sectores sensibles como salud y gobierno.

4. La matriz de riesgos confirma que la gestión de accesos (R1, R3, R7) y la protección de datos personales (R2) deben atenderse de forma prioritaria, por combinar alto impacto con alta probabilidad y contar con antecedentes de materialización.

5. Para sostener su expansión internacional y la incorporación de inteligencia artificial en el desarrollo, es indispensable que SoftVision adopte un enfoque DevSecOps, integrando validaciones de seguridad automáticas en cada fase del ciclo de desarrollo.

6. El éxito de cualquier mejora tecnológica depende de la cultura organizacional: mientras la seguridad se perciba como una molestia que ralentiza el trabajo, los incidentes por error humano seguirán ocurriendo. La transformación cultural, apoyada en el liderazgo de la alta dirección, es la condición que hace sostenibles todos los demás controles.

Referencias

Borges, J.L. (2013). *Ficciones*. Buenos Aires, Argentina: Debolsillo.

Bastidas, L.R. (2007). *El inicio del siglo XXI*. Planeta. Sitio web: http://www.rbastidasl.com/libro-inicio-del-sigloxxi.

Congreso de la República de Colombia. (2009). *Ley 1273 de 2009. Por medio de la cual se modifica el Código Penal y se crea un nuevo bien jurídico tutelado denominado "de la protección de la información y de los datos"*. Diario Oficial No. 47.223.

Congreso de la República de Colombia. (2012). *Ley 1581 de 2012. Por la cual se dictan disposiciones generales para la protección de datos personales*. Diario Oficial No. 48.587.

European Union Agency for Cybersecurity [ENISA]. (2023). *ENISA Threat Landscape 2023*. Publications Office of the European Union.

International Organization for Standardization & International Electrotechnical Commission [ISO/IEC]. (2022a). *ISO/IEC 27001:2022. Seguridad de la información, ciberseguridad y protección de la privacidad — Sistemas de gestión de la seguridad de la información — Requisitos*. ISO.

International Organization for Standardization & International Electrotechnical Commission [ISO/IEC]. (2022b). *ISO/IEC 27002:2022. Seguridad de la información, ciberseguridad y protección de la privacidad — Controles de seguridad de la información*. ISO.

International Organization for Standardization & International Electrotechnical Commission [ISO/IEC]. (2022c). *ISO/IEC 27005:2022. Seguridad de la información, ciberseguridad y protección de la privacidad — Directrices para la gestión de riesgos de seguridad de la información*. ISO.

International Organization for Standardization [ISO]. (2019). *ISO 22301:2019. Seguridad y resiliencia — Sistemas de gestión de la continuidad del negocio — Requisitos*. ISO.

Ministerio de Tecnologías de la Información y las Comunicaciones [MinTIC]. (2021). *Modelo de Seguridad y Privacidad de la Información (MSPI)*. Gobierno de Colombia.

National Institute of Standards and Technology [NIST]. (2012). *Computer Security Incident*

Handling Guide (Special Publication 800-61, Rev. 2). U.S. Department of Commerce.

National Institute of Standards and Technology [NIST]. (2024). *The NIST Cybersecurity Framework (CSF) 2.0 (NIST CSWP 29)*. U.S. Department of Commerce.

OWASP Foundation. (2022). *OWASP DevSecOps Guideline*. Open Worldwide Application Security Project.

Superintendencia de Industria y Comercio [SIC]. (2020). *Guía para la implementación del principio de responsabilidad demostrada (accountability)*. República de Colombia.