Diseño de una propuesta para el fortalecimiento de la seguridad informática de la infraestructura tecnológica del software Agroexport en Binlab S.A.S.

Trabajo final presentado por:	Jhunior Villamil Arango
Programa:	Especialización en Desarrollo de Software
Docente:	Pedro Fabricio Echeverria Briones
Fecha:	26-07-2026

Índice de contenidos

RESUMEN

El presente trabajo de grado tuvo como objetivo diseñar una propuesta para el fortalecimiento de la seguridad informática de la infraestructura tecnológica que soporta el software Agroexport en Binlab S.A.S. La investigación se desarrolló bajo la metodología de investigación-acción, permitiendo identificar las principales vulnerabilidades presentes en la administración de servidores, la gestión de accesos, el monitoreo de eventos de seguridad y el proceso de gestión de vulnerabilidades.

Teniendo en cuenta el diagnóstico realizado, se formuló un plan de acción orientado a la implementación de controles técnicos y administrativos basados en buenas prácticas de ciberseguridad, incluyendo el fortalecimiento de la autenticación, el endurecimiento de servidores, la gestión periódica de vulnerabilidades, el monitoreo de eventos, la estrategia de copias de seguridad y la documentación de procedimientos. Del mismo modo, se definieron el alcance de la propuesta, los responsables de su ejecución, el cronograma de actividades y el presupuesto estimado para su implementación. La propuesta busca contribuir a la reducción de riesgos de seguridad, mejorar la disponibilidad e integridad de la información y fortalecer la continuidad operativa de la organización, proporcionando una guía para la mejora progresiva de la seguridad informática en Binlab S.A.S.

Palabras clave: seguridad informática, ciberseguridad, gestión de vulnerabilidades, infraestructura tecnológica, investigación-acción.

ABSTRACT

This degree project aimed to design a proposal to strengthen the information security of the technological infrastructure supporting the Agroexport software at Binlab S.A.S. The study was conducted using the action research methodology, which enabled the identification of the main vulnerabilities related to server administration, access management, security event monitoring, and vulnerability management processes. Based on the diagnosis, an action plan was developed to implement technical and administrative controls following cybersecurity

best practices, including stronger authentication mechanisms, server hardening, periodic vulnerability management, security event monitoring, backup strategies, and technical documentation.

Take into account the diagnosis made, the scope of the proposal, the responsible stakeholders, the implementation schedule, and the estimated budget were defined. The proposed solution seeks to reduce security risks, improve the availability and integrity of information, and strengthen the operational continuity of the organization by providing a practical guide for the progressive improvement of information security at Binlab S.A.S.

Keywords: information security, cybersecurity, vulnerability management, technological infrastructure, action research.

1. INTRODUCCIÓN

Este proyecto de aplicación en investigación-acción se centró en la identificación y resolución de las vulnerabilidades de seguridad informática que afectan la infraestructura tecnológica del software Agroexport en Binlab S.A.S., permitiendo integrar teoría y práctica en un entorno real. Mediante un enfoque de investigación-acción, se desarrollaron habilidades de diagnóstico, análisis y planificación orientadas a mejorar la eficiencia y efectividad de un proceso crítico en la organización. La estructura del proyecto incluyó una revisión exhaustiva del contexto organizacional y la implementación de una solución factible que responde a las necesidades de la organización y optimiza su desempeño.

1.1. OBJETIVO GENERAL

El objetivo principal del proyecto fue desarrollar una solución operativa orientada al fortalecimiento de la seguridad informática en el proceso de administración de la infraestructura tecnológica que soporta el software Agroexport en Binlab S.A.S. La intervención se orientó no solo a corregir el problema identificado, sino también a proporcionar una propuesta sostenible que pudiera integrarse a la estructura de la organización, elevando los niveles de eficiencia y alcanzando los estándares de desempeño requeridos en el proceso intervenido.

1.2. OBJETIVOS ESPECÍFICOS

Para cumplir con el objetivo general, se establecieron tres objetivos específicos:

1. Identificar las vulnerabilidades de seguridad informática presentes en la infraestructura tecnológica que soporta el software Agroexport en Binlab S.A.S., determinando sus causas y su impacto sobre la disponibilidad, integridad y continuidad de los servicios.
2. Diseñar un plan de acción que contemple controles y buenas prácticas de seguridad informática, definiendo objetivos, actividades y recursos necesarios para mejorar la protección de la infraestructura tecnológica de la organización.
3. Establecer el alcance de la intervención, definiendo responsables, cronograma y presupuesto, para la implementación de la propuesta de fortalecimiento de la seguridad informática, donde se busca garantizar una ejecución organizada y acorde con las necesidades de Binlab S.A.S.

1.3. METODOLOGÍA

El proyecto se desarrolló mediante la metodología de investigación-acción, la cual facilitó la colaboración continua entre el equipo de estudiantes y docente asesor. Esta metodología permitió un enfoque sistemático para identificar problemas, formular hipótesis y aplicar soluciones en un contexto real, ajustando las estrategias conforme se avanzaba en el proyecto. La investigación-acción proporcionó un marco flexible y participativo para ejecutar el proyecto de manera estructurada, generando una intervención bien fundamentada y con alto potencial de impacto.

El desarrollo del proyecto se estructuró en tres etapas secuenciales, cada una de las cuales abordó un aspecto específico de la intervención. En la primera etapa, se identificó y analizó el problema organizacional, incluyendo una descripción detallada de la organización, su misión, visión y el proceso específico afectado. La segunda etapa se centró en la planificación de la solución, estableciendo objetivos y actividades concretas para abordar el problema. En la tercera fase, se definieron aspectos operativos como el cronograma, el presupuesto y la asignación de roles.

1.3.1. Identificación y Análisis del Problema

En la primera etapa, se realizó un análisis exhaustivo de la organización y del contexto en el cual se desarrolla el proceso afectado. Se documentó el problema identificando sus causas raíz, efectos y puntos críticos que afectaban el desempeño del proceso. Este diagnóstico inicial fue esencial para estructurar la solución y asegurar que la intervención respondiera de manera precisa a las necesidades de la organización.

El diagnóstico se desarrolló mediante la metodología de investigación-acción, empleando un estudio de caso dentro de Binlab S.A.S. Como integrante del equipo de desarrollo y soporte del software Agroexport, fue posible realizar una observación directa del funcionamiento de la infraestructura tecnológica y de los procesos relacionados con la administración de la

plataforma. Esta participación permitió identificar las principales vulnerabilidades de seguridad, analizar incidentes presentados durante la operación del sistema y reconocer oportunidades de mejora en los mecanismos de protección implementados.

Adicionalmente, se efectuó una revisión de la configuración de los servidores, los mecanismos de autenticación, los accesos remotos mediante SSH, las políticas de respaldo y las medidas de seguridad existentes. También se analizaron los registros de incidentes y la experiencia obtenida durante las actividades de desarrollo y soporte brindadas a tres clientes que utilizan Agroexport.

1.3.2. Planificación de la Solución

En la segunda etapa, se desarrolló un plan de acción detallado que incluyó la definición de objetivos específicos y una secuencia de actividades que permitiría mitigar o resolver el problema identificado. Esta fase incluyó el diseño de una estrategia de ejecución organizada y estructurada que facilitara el logro de los objetivos propuestos y maximizara la eficiencia del proceso intervenido. La planificación detallada de actividades y recursos fue clave para asegurar una implementación precisa y efectiva.

1.3.2.1. Definición de Alcance y Recursos

La tercera etapa se enfocó en delimitar el alcance de la intervención y los recursos necesarios. Se establecieron responsables para cada actividad, y se elaboró un cronograma de ejecución para controlar el avance de la implementación. Asimismo, se desarrolló un presupuesto que detalló los costos asociados a cada fase, permitiendo optimizar la asignación de recursos. Esta fase aseguró que todas las variables críticas estuvieran alineadas para una ejecución sin interrupciones.

2. IDENTIFICACIÓN Y DESCRIPCIÓN UN PROBLEMA AL INTERIOR DE LA ORGANIZACIÓN

Binlab S.A.S. es una empresa de desarrollo de software especializada en soluciones tecnológicas en diferentes sectores, como el seguimiento satelital, centros deportivos y el de empacadoras de fruta. Entre sus principales productos se encuentra Agroexport, una plataforma que permite gestionar los procesos operativos, administrativos y logísticos relacionados con la exportación de frutas. El sistema es utilizado por diferentes empresas del sector, algunas mediante instalaciones locales y otras a través de una versión web alojada en servidores en la nube.

La problemática identificada se presenta en el proceso de administración y mantenimiento de la infraestructura tecnológica que soporta el software Agroexport, específicamente en la gestión de la seguridad informática de los servidores y de la aplicación web. Debido a la evolución continua del sistema durante aproximadamente siete años, en su desarrollo han participado diferentes integrantes del equipo técnico, lo que ha generado la incorporación de nuevas funcionalidades, cambios en la infraestructura y diversas configuraciones de seguridad que no siempre han sido implementadas bajo criterios estandarizados.

Actualmente, el área de desarrollo y soporte técnico es responsable de realizar el mantenimiento evolutivo y correctivo de la plataforma, así como de atender los requerimientos e incidentes de los clientes. Como parte de estas actividades, se ha evidenciado la necesidad de fortalecer los controles de seguridad informática debido a la ocurrencia de incidentes relacionados con accesos no autorizados a la infraestructura tecnológica, lo que representa un riesgo para la disponibilidad de los servicios, la integridad de la información y la continuidad de la operación de los clientes que utilizan Agroexport.

Entre las principales causas del problema se identifican la ausencia de un modelo integral de seguridad informática, la falta de estandarización en algunas configuraciones de los

servidores, la necesidad de fortalecer las políticas de autenticación y acceso remoto, el crecimiento progresivo de la plataforma sin una estrategia formal de endurecimiento (hardening) de la infraestructura y la inexistencia de un proceso continuo de evaluación y gestión de vulnerabilidades.

Las consecuencias de esta situación incluyen un incremento en el riesgo de incidentes de ciberseguridad, posibles interrupciones del servicio, afectación de la confianza de los clientes, mayor carga operativa para el equipo de soporte y desarrollo, así como posibles impactos económicos y reputacionales para la organización. Por esta razón, se considera necesario diseñar una propuesta de fortalecimiento de la seguridad informática que permita establecer controles técnicos y administrativos orientados a reducir las vulnerabilidades identificadas y mejorar la protección de la infraestructura tecnológica que soporta el software Agroexport.

2.1. DESCRIPCIÓN DE LA EMPRESA A INTERVENIR

2.1.1. Misión

Desarrollar soluciones de software innovadoras y confiables que optimicen los procesos operativos y administrativos del sector agroexportador, brindando servicios de desarrollo, soporte y mantenimiento con altos estándares de calidad, seguridad informática y atención al cliente, contribuyendo al crecimiento y competitividad de las empresas que utilizan nuestras plataformas.

2.1.2. Visión

Ser una empresa reconocida a nivel nacional por el desarrollo de soluciones tecnológicas para el sector agroexportador, destacándose por la innovación, la seguridad informática y la calidad de sus servicios, consolidándose como un aliado estratégico para sus clientes mediante la mejora continua de sus productos y procesos.

2.1.3. Mapa de procesos

El mapa de procesos de Binlab S.A.S se compone de las siguientes categorías:

Procesos estratégicos:

- Dirección estratégica.
- Gestión comercial.

Corresponden a las actividades realizadas por la gerencia y los socios para definir estrategias, captar clientes, negociar proyectos y establecer los objetivos de la empresa.

Procesos misionales:

- Levantamiento de requerimientos.
- Desarrollo de software.
- Implementación y despliegue.
- Soporte y mantenimiento.
- Administración de la infraestructura tecnológica y seguridad informática (proceso a intervenir).

Comprenden las actividades relacionadas con el análisis, desarrollo, implementación, soporte y administración de la infraestructura tecnológica que soporta las soluciones desarrolladas por Binlab S.A.S.

Procesos de apoyo:

- Gestión administrativa
- Gestión del talento humano
- Infraestructura tecnológica
- Gestión documental

Brindan los recursos humanos, tecnológicos y administrativos necesarios para el funcionamiento de la organización.

Imagen 1. Mapa de procesos de Binlab S.A.S. Fuente: Elaboración propia con apoyo de ChatGPT (OpenAI) para la estructuración del diagrama.

2.1.4. Descripción del proceso a intervenir

El proceso de administración de la infraestructura tecnológica y seguridad informática comprende las actividades destinadas a garantizar el funcionamiento seguro de los servidores, servicios, aplicaciones y mecanismos de acceso que soportan el software Agroexport. Este proceso inicia con la administración de los servidores donde se encuentra desplegada la plataforma, continúa con la configuración de servicios, usuarios, accesos remotos, certificados digitales, copias de seguridad y monitoreo de la infraestructura tecnológica. Posteriormente se realizan actividades de actualización, aplicación de parches de seguridad, revisión de registros, análisis de vulnerabilidades y atención de incidentes relacionados con la seguridad informática. Finalmente, el proceso incluye el seguimiento continuo de los controles implementados con el propósito de preservar la confidencialidad, integridad y disponibilidad de la información.

2.1.5. Descripción del problema que presenta el proceso

El problema es la inexistencia de un proceso formal para la administración de la seguridad informática de la infraestructura tecnológica que soporta el software Agroexport en Binlab S.A.S. Aunque la organización realiza actividades de desarrollo, mantenimiento y soporte de forma continua, no dispone de procedimientos estandarizados para la gestión de vulnerabilidades, endurecimiento de servidores, administración de accesos privilegiados, monitoreo de eventos de seguridad y aplicación sistemática de controles preventivos.

Como integrante del equipo de desarrollo y soporte técnico, se ha evidenciado que la organización ha enfrentado incidentes relacionados con accesos no autorizados a su infraestructura tecnológica, situación que ha puesto de manifiesto la necesidad de fortalecer las medidas de protección implementadas. Adicionalmente, se identifican oportunidades de mejora en aspectos como el endurecimiento (hardening) de los servidores, la gestión de accesos privilegiados, el monitoreo de eventos de seguridad, la gestión de vulnerabilidades, las políticas de autenticación y la aplicación de buenas prácticas de ciberseguridad siguiendo las recomendaciones del OWASP Top 10 (OWASP Foundation, 2021).

Esta situación incrementa el riesgo de accesos no autorizados, explotación de vulnerabilidades, interrupción del servicio, pérdida o alteración de la información, afectación de la disponibilidad de la plataforma, incremento de costos operativos y posibles impactos económicos y reputacionales para Binlab S.A.S.

3. ESTABLECIMIENTO DE PLANES DE ACCIÓN PARA LA SOLUCIÓN DEL PROBLEMA

3.1. ESTABLECIMIENTO DE OBJETIVOS

Con base en el diagnóstico realizado sobre el proceso de administración de la infraestructura tecnológica y seguridad informática de Binlab S.A.S., se establecieron los objetivos específicos de la propuesta de fortalecimiento, orientados a reducir las vulnerabilidades identificadas y mejorar la protección del software Agroexport y de la infraestructura que lo soporta. Estos objetivos buscan implementar controles de seguridad acordes con las necesidades actuales de la organización, priorizando soluciones técnicamente viables y de fácil adecuación por parte del equipo de desarrollo y soporte.

Para ello se definieron los siguientes objetivos de la propuesta:

- Fortalecer los mecanismos de autenticación y control de acceso a los servidores que soportan el software Agroexport mediante la implementación de buenas prácticas para la administración de usuarios, accesos privilegiados y autenticación segura.
- Estandarizar las configuraciones básicas de seguridad de los servidores y servicios utilizados por la organización, incorporando medidas de endurecimiento (hardening), actualización periódica y protección de los servicios expuestos.
- Establecer un procedimiento básico para la gestión de vulnerabilidades que contemple actividades periódicas de identificación, evaluación y mitigación de riesgos de seguridad sobre la infraestructura tecnológica.
- Implementar mecanismos de monitoreo y registro de eventos de seguridad que permitan detectar oportunamente comportamientos anómalos y facilitar la atención de incidentes.

- Documentar las actividades y controles propuestos con el fin de establecer una guía de referencia para la administración de la seguridad informática dentro de Binlab S.A.S., favoreciendo la continuidad y mejora del proceso.

3.2. DESCRIPCIÓN DE LA SOLUCIÓN

La solución propuesta consiste en el diseño de un plan para el fortalecimiento de la seguridad informática de la infraestructura tecnológica que soporta el software Agroexport en Binlab S.A.S., mediante la implementación de controles técnicos y administrativos orientados a reducir las vulnerabilidades identificadas durante el diagnóstico del proceso.

Como primer componente de la solución, se propone fortalecer la administración de accesos a los servidores donde se encuentra desplegado Agroexport. Para ello se plantea reforzar el acceso a los usuarios mediante las llaves SSH que ya existen, forzando el uso de usuario y contraseña y limitando la cantidad de usuarios, aplicar el principio de menor privilegio en la asignación de permisos y revisar periódicamente las cuentas con privilegios administrativos. Estas medidas disminuyen el riesgo de accesos no autorizados y fortalecen el control sobre las operaciones realizadas en los servidores.

El segundo componente corresponde al hardening de la infraestructura tecnológica. En este aspecto se propone estandarizar la configuración de los servidores Debian mediante la deshabilitación de servicios innecesarios, la aplicación oportuna de actualizaciones de seguridad, la configuración de un firewall con reglas que permitan únicamente los servicios requeridos y la implementación de herramientas como Fail2Ban para mitigar intentos de acceso por fuerza bruta. Adicionalmente, se recomienda mantener certificados digitales actualizados para los servicios web y establecer una revisión periódica de las configuraciones de seguridad.

Como tercer componente, la propuesta incorpora un procedimiento básico para la gestión de vulnerabilidades. Este procedimiento contempla la realización de escaneos periódicos

utilizando herramientas como Nessus Essentials u OpenVAS, con el propósito de identificar vulnerabilidades presentes en los servidores y servicios desplegados. Los resultados obtenidos permitirán priorizar la aplicación de actualizaciones, corregir configuraciones inseguras y verificar posteriormente que las vulnerabilidades hayan sido mitigadas.

La solución contempla el fortalecimiento del monitoreo de la infraestructura mediante la revisión periódica de registros del sistema, eventos de autenticación y actividad de los servicios críticos. El registro y análisis de estos eventos facilitará la detección temprana de comportamientos anómalos, intentos de acceso no autorizados y posibles incidentes de seguridad. Complementariamente, se propone documentar un procedimiento básico de respuesta ante incidentes que establezca las actividades mínimas para la identificación, contención, recuperación y registro de eventos de seguridad, permitiendo una actuación más organizada ante futuras contingencias, de acuerdo con las fases propuestas por el NIST (National Institute of Standards and Technology, 2012).

Finalmente, se plantea consolidar toda la propuesta mediante la elaboración de documentación técnica que reúna las configuraciones implementadas, los procedimientos de administración de la seguridad, las actividades de mantenimiento y las responsabilidades del personal encargado de la infraestructura tecnológica. La existencia de esta documentación facilitará la estandarización del proceso, disminuirá la dependencia del conocimiento individual de los desarrolladores y contribuirá a la continuidad operativa de la organización.

En conjunto, la propuesta busca establecer un proceso de administración de la seguridad informática que permita a Binlab S.A.S. fortalecer progresivamente la protección del software Agroexport sin generar cambios drásticos en su infraestructura actual. La implementación de controles preventivos, actividades periódicas de revisión y procedimientos documentados permitirá reducir la probabilidad de incidentes de seguridad, mejorar la continuidad del servicio y aumentar la confianza de los clientes que utilizan la plataforma, alineados con los controles establecidos en la norma ISO/IEC 27001:2022 (International Organization for Standardization, 2022).

3.3. SECUENCIA DE ACTIVIDADES PARA EJECUCIÓN DE LA SOLUCIÓN

Con el propósito de implementar la propuesta de fortalecimiento de la seguridad informática en Binlab S.A.S., se definió una secuencia de actividades organizada de manera lógica y progresiva. Esta planificación permite ejecutar los controles propuestos de forma ordenada, iniciando con la evaluación del estado actual de la infraestructura, continuando con la implementación de medidas preventivas y finalizando con actividades de validación, documentación y seguimiento.

Fase	**Actividad**	**Descripción**
Diagnóstico	Inventario de la infraestructura tecnológica	Identificar los servidores, servicios, aplicaciones y componentes que soportan el software Agroexport.
Diagnóstico	Revisión de configuraciones de seguridad	Evaluar las configuraciones actuales de servidores, accesos remotos, firewall, usuarios y servicios expuestos.
Implementación	Fortalecimiento de los mecanismos de acceso	Reforzar la autenticación existente de llaves SSH y aplicar el principio de menor privilegio.
Implementación	Endurecimiento de servidores	Configurar firewall, deshabilitar servicios innecesarios, instalar mecanismos de protección contra ataques de fuerza bruta y aplicar actualizaciones de seguridad.

Implementación	Estrategia de copias de seguridad	Verificar y estandarizar los respaldos automáticos, así como realizar pruebas de restauración de la información.
Implementación	Gestión de vulnerabilidades	Realizar escaneos periódicos con herramientas especializadas, analizar resultados y corregir las vulnerabilidades identificadas.
Implementación	Monitoreo y registros	Configurar la revisión periódica de registros del sistema y eventos de seguridad para detectar actividades anómalas.
Validación	Verificación de controles implementados	Comprobar el funcionamiento de los controles de seguridad y validar que las vulnerabilidades hayan sido mitigadas.
Documentación	Elaboración de procedimientos	Documentar las configuraciones realizadas, los controles implementados y las actividades de administración de la seguridad informática.
Seguimiento	Revisión periódica	Establecer revisiones periódicas para mantener actualizados los controles de seguridad y garantizar la mejora continua del proceso.

Tabla 1. Secuencia de actividades para la ejecución de la solución. Fuente: fuente propia

3.4. DESCRIPCIÓN DE RECURSOS NECESARIOS PARA LA EJECUCIÓN DE LA SOLUCIÓN

La implementación de la propuesta de fortalecimiento de la seguridad informática requiere la disponibilidad de recursos humanos, tecnológicos y documentales que permitan ejecutar las actividades planteadas de manera organizada. Debido a que la propuesta está orientada a una

pequeña empresa de desarrollo de software, se busca aprovechar principalmente la infraestructura y el talento humano ya existente, minimizando la necesidad de realizar inversiones adicionales.

Recursos humanos.

El desarrollo de las actividades requiere la participación del personal que actualmente interviene en la administración y mantenimiento del software Agroexport. Cada integrante desempeña funciones específicas dentro del proceso de implementación, favoreciendo una distribución adecuada de responsabilidades.

- Gerencia: Aprobar la propuesta, definir prioridades y realizar seguimiento a la implementación.
- Equipo de desarrollo y soporte: Implementar las configuraciones de seguridad, realizar actualizaciones, aplicar controles técnicos y documentar las actividades ejecutadas.
- Responsable del servidor: Administrar los servidores, configurar mecanismos de acceso, realizar respaldos y supervisar el funcionamiento de la infraestructura tecnológica.

Recursos tecnológicos.

La propuesta aprovecha la infraestructura tecnológica con la que actualmente opera Binlab S.A.S., incorporando herramientas de seguridad de libre uso o ya disponibles dentro del entorno de trabajo.

- Servidores Debian: Plataforma sobre la cual se ejecuta Agroexport y donde se implementarán los controles de seguridad.
- Apache y PostgreSQL: Servicios que soportan la aplicación y la base de datos del sistema.
- OpenSSH: Administración remota segura de los servidores.
- UFW (Uncomplicated Firewall): Configuración de reglas básicas de protección de red.
- Fail2Ban: Protección frente a intentos de acceso no autorizados mediante fuerza bruta.
- Nessus Essentials u OpenVAS: Identificación y evaluación periódica de vulnerabilidades.
- Git: Control de versiones y respaldo de los cambios realizados sobre el software.

Recursos documentales.

La documentación constituye un elemento fundamental para asegurar la continuidad del proceso y facilitar futuras actividades de mantenimiento y administración de la seguridad informática.

- Procedimiento de administración de la seguridad informática: Estandarizar las actividades relacionadas con la administración de la infraestructura tecnológica.
- Inventario de activos tecnológicos: Identificar los servidores, servicios y componentes que soportan Agroexport.
- Registro de vulnerabilidades: Documentar las debilidades identificadas, las acciones correctivas aplicadas y su estado.
- Procedimiento de respuesta ante incidentes: Definir las actividades básicas para la atención de eventos de seguridad.
- Bitácora de cambios y actualizaciones: Registrar las modificaciones realizadas sobre la infraestructura tecnológica y los controles implementados.

Los recursos descritos permiten implementar la propuesta sin requerir cambios significativos en la estructura organizacional ni inversiones elevadas en infraestructura tecnológica. La utilización de herramientas de libre distribución, junto con el aprovechamiento del conocimiento del equipo de desarrollo y soporte, favorece la viabilidad técnica y económica de la propuesta. Asimismo, la elaboración de documentación estandarizada contribuirá a preservar el conocimiento organizacional, facilitar las actividades de mantenimiento y fortalecer el proceso de administración de la seguridad informática en la empresa.

4. DEFINICIÓN DEL ALCANCE DE LA SOLUCIÓN, PARTES INTERESADAS, CRONOGRAMA Y PRESUPUESTOS.

4.1. ALCANCE FINAL DE LA SOLUCIÓN

La propuesta de fortalecimiento de la seguridad informática para el software Agroexport en Binlab S.A.S. tiene como alcance el diseño de un conjunto de controles técnicos y administrativos orientados a mejorar la protección de la infraestructura tecnológica que soporta la plataforma. La propuesta comprende la definición de buenas prácticas para la administración de accesos privilegiados, el endurecimiento de servidores, la gestión periódica de vulnerabilidades, el monitoreo de eventos de seguridad y la documentación de procedimientos para la administración de la seguridad informática, siguiendo las recomendaciones de la norma ISO/IEC 27002:2022 (International Organization for Standardization, 2022).

La intervención está enfocada en la infraestructura tecnológica utilizada por Binlab S.A.S. para la operación del software Agroexport y busca servir como una guía para la implementación gradual de controles de seguridad, sin modificar la arquitectura de la aplicación ni afectar la continuidad de los servicios prestados a los clientes.

Dentro del alcance también se contempla la definición de responsables, recursos, cronograma y presupuesto necesarios para facilitar la ejecución de la propuesta, permitiendo que la organización pueda planificar su implementación de manera organizada y acorde con sus capacidades técnicas y operativas.

Como parte de las limitaciones del proyecto, la propuesta no incluye la implementación completa de todas las medidas de seguridad planteadas, el desarrollo de nuevas funcionalidades del software, la adquisición de infraestructura adicional ni la realización de

auditorías de seguridad certificadas. El trabajo se limita al diseño de una propuesta de fortalecimiento basada en el diagnóstico realizado y en buenas prácticas de seguridad informática aplicables al contexto de Binlab S.A.S.

4.2. IDENTIFICACIÓN DE RESPONSABLES DE LAS ACTIVIDADES PARA EJECUCIÓN

Para garantizar una implementación organizada de la propuesta de fortalecimiento de la seguridad informática, se asignan responsables para cada una de las actividades definidas en el plan de acción. La distribución de responsabilidades busca facilitar la coordinación entre las áreas involucradas y asegurar el cumplimiento de las actividades programadas.

Actividad	**Responsable**
Inventario de la infraestructura tecnológica	Equipo de desarrollo y soporte
Revisión de configuraciones de seguridad	Administrador de infraestructura
Fortalecimiento de mecanismos de autenticación y acceso	Administrador de infraestructura
Endurecimiento (hardening) de servidores	Administrador de infraestructura
Configuración y validación de copias de seguridad	Administrador de infraestructura
Ejecución de escaneos de vulnerabilidades	Equipo de desarrollo y soporte
Implementación de monitoreo y revisión de registros	Administrador de infraestructura
Verificación de los controles implementados	Equipo de desarrollo y soporte

Elaboración de procedimientos y documentación técnica	Equipo de desarrollo

Tabla 2. Identificación de responsables para actividades. Fuente: fuente propia

4.3. CRONOGRAMA DE EJECUCIÓN

Con el propósito de organizar la implementación de la propuesta de fortalecimiento de la seguridad informática, se estableció un cronograma de ejecución que distribuye las actividades en una secuencia lógica y progresiva de diez semanas. La planificación permite desarrollar las tareas de diagnóstico, implementación, validación y seguimiento de manera ordenada, facilitando el control del avance del proyecto y la asignación adecuada de los recursos durante cada etapa de la intervención.

Actividad	**S1**	**S2**	**S3**	**S4**	**S5**	**S6**	**S7**	**S8**	**S9**	**S10**
Inventario de infraestructura	●									
Revisión de configuraciones de seguridad	●	●								
Fortalecimiento de autenticación y accesos		●	●							
Hardening de servidores			●	●						
Estrategia de copias de seguridad				●	●					
Gestión de vulnerabilidades					●	●				
Monitoreo y registros						●	●			
Validación de controles							●	●		

Documentación técnica								●	●	
Seguimiento final									●	●

Tabla 3. Cronograma de actividades. Fuente: fuente propia

4.4. PRESUPUESTO

Como la propuesta se basa principalmente en la implementación de buenas prácticas y herramientas de libre uso, el presupuesto puede plantearse de forma realista considerando el tiempo del personal.

Concepto	**Cantidad (Horas)**	**Valor estimado (COP)**
Análisis y diagnóstico	20	$1.000.000
Configuración y fortalecimiento de servidores	30	$1.500.000
Gestión de vulnerabilidades y pruebas	20	$1.000.000
Elaboración de documentación técnica	15	$750.000
Capacitación básica al personal	10	$500.000
Herramientas de software (OpenVAS, Fail2Ban, UFW, OpenSSH)	-	$0
Total estimado		$4.750.000

Tabla 4. Presupuesto. Fuente: fuente propia

La implementación de la propuesta prioriza el uso de herramientas de código abierto, como OpenVAS, Fail2Ban, UFW y OpenSSH, por lo que no se contemplan costos asociados a licencias de software. El presupuesto estimado corresponde principalmente al tiempo de dedicación del personal encargado de ejecutar las actividades de implementación, validación y documentación de los controles de seguridad.

5. REFERENCIAS BIBLIOGRÁFICAS

OWASP Foundation. (2021). *OWASP Top 10: The Ten Most Critical Web Application Security Risks*. https://owasp.org/www-project-top-ten/

REDSUMMA Education (sf). *Fundamentos de Seguridad, Criptografía básica y OWASP Top 10*. REDSUMMA Education.

REDSUMMA Education (sf). *JavaScript Esencial, DOM y Seguridad en el Front (XSS).* REDSUMMA Education.

REDSUMMA Education (sf). *Seguridad en Redes — Protocolos, Cifrado y Defensa Perimetral.* REDSUMMA Education.

REDSUMMA Education (sf). *Gestión de Vulnerabilidades y Respuesta ante Incidentes.* REDSUMMA Education.

Sime, R., Sezgin, N., & Ağgün, F. (2025). *An Integrated Web Security Application: Integration Of Nginx Reverse Proxy, Fail2ban, Waf, Postgresql and Laravel*. Balkan Journal of Electrical and Computer Engineering, 13(1), 106-111. https://doi.org/10.17694/bajece.1547456.

Kara, M. (2026). *Scanning Capabilities of Nessus, Qualys and OpenVAS Vulnerability Scanner Tools for Vulnerable Operating Systems and Web Applications*. EMO Bilimsel Dergi, 16(2), 103-112. https://izlik.org/JA37UJ35NS.

National Institute of Standards and Technology. (2012). *Computer Security Incident Handling Guide (NIST Special Publication 800-61 Revision 2).* https://doi.org/10.6028/NIST.SP.800-61r2.

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

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