UNIVERSIDAD SAN SEBASTIAN

FACULTAD DE INGENIERÍA, ARQUITECTURA Y DISEÑO

CARRERA INGENIERÍA CIBERSEGURIDAD Y AUDITORIA INFORMATICA

SEDE SANTIAGO

PROPUESTA DE PLATAFORMA DE SEGURIDAD DE CORREO ELECTRÓNICO Y CONCIENTIZACIÓN PARA EL ÁREA DE VENTAS DE CONTRUPRO, EMPRESA DEL RUBRO INMOBILIARIO

Proyecto de título para optar al Título de Ingeniero en Ciberseguridad y Auditoría Informática

Profesor guía: Rene Galarce Godoy

Estudiantes: Ignacio Espinoza S.

Alejandro González C.

Santiago, Chile
2025

Hoja de calificación

En _____ Chile, el __ de _____ del 20__, los abajo firmantes dejan constancia que el estudiante _____ de la carrera _____ ha aprobado el proyecto de título para optar al título de _____ con una nota de _____

_____
Profesor Evaluador

_____
Profesor Evaluador

_____
Profesor Evaluador

Agradecimientos Alejandro González Cepeda

A mi madre, Eufemia Cepeda Díaz, por haber sido siempre mi mayor inspiración y pilar incondicional. Su apoyo constante, sus palabras de aliento y la fuerza con la que me impulsó a seguir este camino académico han sido fundamentales para llegar hasta aquí.

A mi padre, Víctor González Torres, por la confianza plena que siempre ha depositado en mí, por creer en mi criterio y transmitirme la seguridad de que con esfuerzo y rectitud se puede alcanzar cualquier meta. Su apoyo y respaldo permanente me han dado la convicción necesaria para perseverar.

A ambos, quiero expresarles que son lo más valioso en mi vida. Su amor, entrega y compañía me han dado la fuerza para superar cada desafío, y todo lo que soy hoy se los debo a ustedes. Los amo profundamente y este logro es también suyo.

Agradecimientos Ignacio Espinoza Sáez

A mi madre, Mariela Sáez Parra, por ser siempre mi mayor apoyo, incluso a la distancia. Gracias por darme las bases de lo que soy hoy, por acompañarme en los altos y bajos de este gran desafío.

A mi tía, Olga Espinoza Domínguez, por motivarme a emprender este camino que terminó convirtiéndose en mi pasión y vocación. Gracias por recordarme una y otra vez que era capaz de lograr lo que me propusiera y por enseñarme a nunca rendirme.

A mi pareja, Catalina De Juan Cantarero, por estar conmigo en cada etapa de estos años de carrera, por ser mi apoyo en las noches de estudio y mi aliento en los momentos más difíciles. Sin duda, ha sido un pilar fundamental en esta travesía.

Y, por último, pero no menos importante, a la familia De Juan Cantarero: a mis suegros y mis cuñadas, por abrirme las puertas de su hogar y apoyarme siempre. Gracias por sus consejos, por las palabras de aliento y, sobre todo, por recibirme y tratarme como un miembro más de su hermosa familia.

Resumen

El presente proyecto de título tiene como propósito diseñar e implementar una propuesta integral de seguridad de correo electrónico para el área de ventas de la empresa ficticia Contrupro, inspirada en una empresa real del rubro de la construcción modular e inmobiliario. Este sector, por la naturaleza de sus operaciones, gestiona información de alto valor como contratos, planos de edificación y datos personales de clientes, lo que lo convierte en un objetivo atractivo para la ciberdelincuencia. La iniciativa surge de la necesidad de mitigar amenazas frecuentes en el correo electrónico, tales como el phishing, la suplantación de identidad y el malware, cuya explotación puede traducirse en pérdidas económicas significativas, daños reputacionales y una afectación directa a la confianza del mercado.

La propuesta no se limita únicamente a fortalecer los aspectos técnicos de la seguridad, sino que también integra un componente de concientización que busca reducir la exposición al factor humano, identificado como una de las principales causas de brechas de seguridad en las organizaciones. De este modo, el proyecto persigue un doble objetivo: por una parte, blindar el flujo de correos mediante herramientas avanzadas de filtrado y autenticación; y por otra, generar una cultura organizacional de seguridad que prepare a los colaboradores para identificar, reportar y reaccionar de manera adecuada frente a amenazas reales. De esta forma, se pretende alcanzar un modelo de defensa integral que combine tecnología y educación para enfrentar los riesgos actuales y futuros.

Para materializar este propósito, el proyecto comenzó con un análisis exhaustivo de la situación actual de ContruPro, evaluando la criticidad de los procesos de negocio y su dependencia del correo electrónico. A través de metodologías como el diagrama de Ishikawa, el análisis de criticidad y la aplicación del marco NIST Cybersecurity Framework, se identificaron las causas raíz de la problemática y los riesgos de mayor impacto. Esta fase permitió establecer un diagnóstico claro, donde se evidenció la inexistencia de políticas formales de seguridad, la falta de

herramientas especializadas y una escasa cultura de concientización entre los trabajadores.

Posteriormente, se diseñó una propuesta de mejora basada en el Ciclo de Deming (Planificar, Hacer, Verificar, Actuar), que permitió estructurar un plan iterativo y sostenible de implementación. En la fase de planificación se definieron los requisitos técnicos y humanos, se seleccionó Proofpoint como solución tecnológica SaaS para protección del correo y se modeló un programa de concientización con campañas de phishing simulado y módulos de capacitación. En la etapa de ejecución se configuró la arquitectura técnica de integración, se establecieron políticas de seguridad específicas y se desarrollaron los materiales de formación. Durante la fase de verificación se validaron los resultados a través de indicadores clave de rendimiento (KPIs), midiendo reducción de incidentes, mejoras en la participación de los usuarios y estabilidad operativa. Finalmente, en la fase de acción se propusieron nuevas líneas de mejora, como la integración de mecanismos de prevención de fuga de datos (DLP) y la formalización de procesos de reporte de incidentes.

El proyecto concluyó con un análisis económico que permitió dimensionar la inversión requerida y evaluar los beneficios, tanto financieros como no económicos. Aunque en el corto plazo los costos superan los beneficios directos, se demostró que la propuesta actúa como una póliza estratégica frente a pérdidas potenciales mucho mayores, además de aportar beneficios intangibles como la mejora de la reputación, la confianza de clientes y socios, y la continuidad operativa del negocio. En definitiva, el trabajo desarrollado entrega una solución robusta, justificada y alineada con las necesidades reales de la empresa, demostrando el rol esencial del Ingeniero en Ciberseguridad en la creación de estrategias que combinan la tecnología y el factor humano para enfrentar los desafíos de seguridad del entorno digital actual.

Abstract

This degree project aims to design and implement a comprehensive email security proposal for the sales department of ContruPro, a company operating in the real estate sector. Due to the nature of its operations, this industry handles highly sensitive information such as contracts, architectural plans, and customers' personal data, making it an attractive target for cybercriminals. The initiative emerges from the need to mitigate the most frequent threats to this communication channel, such as phishing, identity theft, and malware, which, if successfully exploited, could result in significant financial losses, severe reputational damage, and a critical breakdown in client trust.

The proposal goes beyond strengthening only the technical aspects of security and incorporates a user awareness component aimed at addressing the human factor, one of the leading causes of data breaches in organizations. Thus, the project pursues a dual objective: on the one hand, reinforcing the email flow through advanced filtering and authentication tools; and on the other, fostering an organizational security culture that enables employees to identify, report, and react appropriately to real threats. In doing so, the project seeks to establish an integrated defense model that combines technology with education, ensuring long-term resilience against both current and emerging cyber risks.

To achieve this goal, the project began with a thorough analysis of ContruPro current situation, assessing the criticality of its business processes and their dependence on email communications. Using methodologies such as Ishikawa root cause diagrams, criticality analysis, and the NIST Cybersecurity Framework, the main weaknesses and risks were identified. This diagnostic stage revealed a lack of formalized security policies, insufficient technical tools, and a limited cybersecurity culture among employees.

Based on these findings, a comprehensive improvement proposal was developed

following the Deming Cycle (Plan, Do, Check, Act). During the planning phase, technical and organizational requirements were defined, Proofpoint was selected as the SaaS security platform, and a security awareness program was designed with phishing simulation campaigns and training modules. The execution stage included technical integration of the platform, configuration of specific security policies, and development of educational materials. The verification phase validated the outcomes through Key Performance Indicators (KPIs), measuring the reduction of phishing incidents, improved user participation in awareness campaigns, and system stability. Finally, the action stage proposed continuous improvements, such as the introduction of Data Loss Prevention (DLP) measures and the formalization of an incident reporting process to enhance resilience.

The project concluded with an economic analysis to estimate the required investment and to evaluate both tangible and intangible benefits. Although the cost-benefit ratio in the short term was negative, the solution is justified as a strategic investment that prevents high-impact risks and secures the company's continuity. Moreover, it delivers non-financial benefits such as enhanced reputation, improved customer trust, and the establishment of a strong cybersecurity culture. In conclusion, the project provides a robust and well-justified solution aligned with the organization's needs, while highlighting the essential role of cybersecurity engineers in designing strategies that integrate technology and human awareness to meet the challenges of today's digital environment.

ÍNDICE

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

Glosario de términos

PDCA: Ciclo de mejora continua: planificar, ejecutar, verificar y actuar para cerrar el ciclo e iniciar uno nuevo con aprendizajes.

NIST CSF: Marco de ciberseguridad del NIST que organiza actividades en cinco funciones: Identificar, Proteger, Detectar, Responder y Recuperar.

KPI (Indicador Clave de Desempeño): Métrica cuantitativa usada para medir el avance y eficacia de objetivos definidos.

Línea base (Baseline): Valor inicial de un KPI antes de implementar cambios; sirve de referencia para medir mejoras.

Meta progresiva: Objetivo intermedio/escalonado en el tiempo para un.

SIEM: Plataforma que centraliza, correlaciona y visualiza eventos y logs de seguridad para detección y respuesta.

DLP (Data Loss Prevention): Conjunto de controles que previene la filtración o envío no autorizado de datos sensibles.

MFA (Multi-Factor Authentication): Autenticación que exige dos o más factores (algo que sabes, tienes o eres).

MDM/Acceso condicional: Gestión de dispositivos y políticas que condicionan el acceso (ej. a correo) al cumplimiento de requisitos.

Proofpoint (Email Security / SAT): Plataforma SaaS utilizada para filtrado de amenazas de correo y entrenamiento de concientización.

Phishing: Intento de engaño por correo para obtener credenciales o ejecutar acciones maliciosas.

Phishing simulado: Campañas controladas para medir y mejorar la conducta de usuarios frente a phishing.

SAT (Security Awareness Training): Programa de formación para fortalecer la conducta segura de los usuarios.

SPF (Sender Policy Framework): Registro DNS que define qué servidores pueden enviar correo en nombre de un dominio.

DKIM (DomainKeys Identified Mail): Firma criptográfica en el correo que valida que no ha sido alterado y que proviene del dominio autorizado.

DMARC: Política que usa SPF/DKIM para decidir qué hacer con correos que no pasan validaciones (none/quarantine/reject) y genera reportes (RUA/RUF).

Quarantine / Reject (DMARC): Acciones recomendadas ante fallas de autenticación: poner en cuarentena o rechazar el mensaje.

Sandboxing: Ejecución controlada de adjuntos/URLs para observar comportamientos maliciosos sin riesgo al entorno.

URL Defense / Reescritura de enlaces: Técnica que reescribe URLs en correos para inspeccionarlas al momento del clic.

Falso positivo / Falso negativo: Bloqueo de correo legítimo por error / paso de correo malicioso sin detectar.

Lecciones aprendidas: Conjunto de hallazgos y mejoras documentadas después de una fase o incidente.

Playbook de respuesta: Procedimiento paso a paso para gestionar incidentes (roles, acciones, tiempos, evidencias).

TTR (Time to Resolve): Tiempo total para resolver un incidente desde su detección.

SLA: Acuerdo de nivel de servicio (tiempos y niveles de atención comprometidos).

Retención y Archivado: Políticas que definen cuánto tiempo se conservan correos y cómo se almacenan copias a largo plazo.

eDiscovery: Búsqueda y preservación de correos/evidencias para auditorías, investigación o requerimientos legales.

PII / Datos personales: Información que identifica o puede identificar a una persona; foco de controles de DLP y cumplimiento.

Hardening / Tuning: Endurecimiento de configuraciones / ajuste fino de reglas para reducir riesgo y falsos positivos.

Change log / Control de cambios: Registro formal de modificaciones a configuraciones, políticas o entregables del proyecto.

1 Introducción

El siguiente proyecto de título propone una plataforma de seguridad de correo electrónico que contenga una componente de concientización para empresas del rubro inmobiliario centrado en el área de ventas. Se ha considerado como caso de estudio a Contrupro, una empresa ficticia inspirada en una compañía real del rubro de la construcción modular e inmobiliario. Su diseño se sustenta en datos y dinámicas reales del sector, lo que permite representar de manera fiel los desafíos y particularidades que enfrentan estas organizaciones en materia de ciberseguridad.

En la actualidad, el sector inmobiliario enfrenta una creciente amenaza en materia de seguridad informática, especialmente en el uso del correo electrónico como herramienta de comunicación empresarial. Esta plataforma es fundamental para las operaciones diarias y las relaciones comerciales, esto la ha llevado convertirse en el vector favorito para la realización de ataques cibernéticos, tales como son el phishing, la suplantación de identidad y la propagación de malware. Estos sucesos no solo amenazan la privacidad y la integridad de la información crucial de la organización, como lo pueden ser contratos, planos de edificación y datos personales de los clientes, sino que también perjudican la confianza y el prestigio de las entidades involucradas.

La problemática se ve agravada debido a la ausencia de medidas de protección adecuadas y la falta de programas efectivos de concientización entre los colaboradores y trabajadores de las empresas, lo que provoca un incremento de la vulnerabilidad ante ataques relacionados con el correo electrónico, que podrían prevenirse con un enfoque integral de seguridad de esta herramienta. En este contexto, nace la necesidad de desarrollar soluciones tecnológicas que mezclen herramientas de protección con estrategias educativas para los usuarios, con el propósito de fortalecer la postura de ciberseguridad del sector inmobiliario.

Este proyecto de título propone la implementación de una plataforma de

seguridad de correo electrónico orientada a empresas inmobiliarias con el enfoque principal en el área de ventas, que integre mecanismos para detectar y mitigar las amenazas más comunes, acompañada de un componente de concientización destinado a educar y preparar a los empleados frente a los riesgos mitigados por la plataforma de seguridad. Esta iniciativa busca, a través de una solución escalable y adaptada a las características propias del sector, proteger la información sensible y reducir la incidencia de fraudes que afectan la continuidad y mantener la eficiencia de las operaciones comerciales.

La implementación de esta plataforma no solo permitirá la mejora de la protección técnica contra amenazas externas, sino también impulsara un cambio cultural en la organización mediante la capacitación continua, lo cual es una tarea fundamental para alcanzar una defensa integral y sostenible. En consecuencia, el proyecto se enmarca en el rol esencial que tiene el Ingeniero en Ciberseguridad y Auditoría Informática, como líder y responsable de diseñar estrategias efectivas que respondan a las necesidades específicas del sector, aportando valor a la seguridad de las empresas del rubro inmobiliario cooperando en mantener la confianza del mercado hacia sus clientes.

2 Antecedentes del proyecto

2.1 Descripción del problema

El sector inmobiliario un componente esencial en la economía, distinguiéndose por la administración de información delicada y la realización de operaciones que requieren de confianza y seguridad. En este escenario, el intercambio de información por medio del correo electrónico es un medio crucial para la coordinación de operaciones y la formalización de contratos. No obstante, esta creciente dependencia ha transformado a esta herramienta en un objetivo prioritario para los ataques cibernéticos.

Según el informe The Human Factor Report generado por Proofpoint (2023), aproximadamente el 90% de los ciberataques comienzan a través de un correo electrónico malicioso. Dentro de estos, los ataques de phishing y suplantación de identidad representan las técnicas más utilizadas para confundir a los usuarios y comprometer la seguridad de las organizaciones. En el caso específico del sector inmobiliario, el cual que gestiona documentación sensible no solo de la empresa, sino que también de los usuarios, un ataque efectivo puede generar graves consecuencias económicas, hurto de propiedad intelectual o daños irreparables a la confianza de los clientes y asociados comerciales.

Esto se suma al informe anual de Cisco (Cybersecurity Report Series, 2025) muestra que en los últimos dos años se ha registrado un incremento del 45% en incidentes relacionados con phishing en la industria inmobiliaria, cifra que evidencia una tendencia preocupante de ataques cada vez más sofisticados y dirigidos. Esta realidad se agudiza por la escasa implementación de sistemas de seguridad específicos para el correo electrónico, así como por la falta de programas efectivos de concientización en las empresas, por lo que se evidencia que un alto porcentaje de los empleados no están preparados para identificar y actuar de forma adecuada ante estos ataques.

En complemento, El Verizon Data Breach Investigations Report (Verizon Business, s. f.) aporta que el 36% de las brechas de seguridad en organizaciones

pequeñas y medianas son provocados directamente de errores humanos, siendo la causa principal la falta de formación y concientización en materias de ciberseguridad. Esto enfatiza la importancia de no solo contar con soluciones tecnológicas robustas que permitan mitigar estos ataques, sino también se debe contar componente educativo que fortalezca las buenas prácticas entre los colaboradores.

Focalizando más la información una empresa del sector modular, este tipo de organizaciones enfrenta volúmenes elevados de comunicación, ciclos de venta y cotización acelerados, lo que multiplica su exposición a riesgos como phishing, malware o suplantación de identidad.

- Alta frecuencia de cotizaciones y comunicaciones comerciales: Las constructoras modulares operan con flujos intensivos debido al bajo costo y rápida entrega de sus soluciones prefabricadas. El mercado global de construcción modular alcanzó los USD 89,4 mil millones en 2024 y se proyecta que crecerá a USD 151,5 mil millones en 2032, lo que refleja un ritmo acelerado de adopción (Fortune Business Insights, 2024).

- Dinámica de ritmo elevado y menor tolerancia a interrupciones: La construcción modular puede reducir los tiempos de entrega hasta en un 50% respecto de los métodos tradicionales (Modular Building Institute, 2023). Por ello, cualquier interrupción provocada por incidentes de ciberseguridad puede generar un impacto inmediato en las finanzas y la continuidad operacional.

Un caso ilustrativo ocurrió recientemente en la empresa Contrupro, donde un vendedor recibió un correo aparentemente legítimo de un cliente habitual con una línea de crédito amplia. La comunicación, que resultó ser un caso de suplantación de identidad, derivó en la entrega fraudulenta de 10 unidades de producto, cada una valorada entre 5 y 8 millones de pesos. A este perjuicio directo se sumaron los costos asociados de transporte y logística, estimados en 5 millones de pesos adicionales, generando así una

pérdida aproximada de 60 millones de pesos en un solo incidente. Este hecho refleja de manera tangible el nivel de exposición y el impacto financiero que puede tener un ataque de este tipo, reforzando la urgencia de implementar mecanismos tecnológicos y programas de concientización para proteger las comunicaciones por correo electrónico

En síntesis, la creciente dependencia del correo electrónico en el sector inmobiliario, sumada a la exposición a ataques de phishing, suplantación de identidad y errores humanos, evidencia la necesidad urgente de implementar soluciones tecnológicas robustas complementadas con programas de concientización, a fin de proteger la información sensible y garantizar la continuidad operativa de las empresas.

2.2 Objetivos del proyecto

2.2.1 Objetivo general

Diseñar una plataforma de seguridad de correo electrónico basada en NIST, orientada a la protección contra phishing, malware y suplantación de identidad, para la empresa ContruPro, junto con un componente de concientización destinado a educar a los usuarios sobre los riesgos detectados y bloqueados por la plataforma.

2.2.2 Objetivo específico

- ✓ Analizar las principales amenazas que afectan al sector inmobiliario a través del correo electrónico, como el phishing, suplantación de identidad y recepción de malware.
- ✓ Definir los requisitos funcionales y no funcionales de una plataforma de seguridad de correo electrónico adaptada al rubro inmobiliario, considerando facilidad de uso, escalabilidad y compatibilidad con sistemas existentes
- ✓ Modelar un componente de concientización que utilice incidentes reales de los ataques detectados para mejorar la preparación y respuesta de los usuarios ante futuros intentos de suplantación, phishing y malware.

- ✓ Estimar los costos para la propuesta de implementación de la plataforma de seguridad de correo electrónico con componente de concientización para empresas del rubro inmobiliario evaluando los distintos servicios asociados
- ✓ Analizar la situación actual de la empresa, evaluando el nivel de seguridad del sistema de correo electrónico, los controles técnicos y administrativos implementados, así como los procesos operativos asociados a la gestión y protección del correo corporativo.

2.3 Alcance y delimitaciones del Proyecto

El proyecto presenta ciertas limitaciones que condicionan su alcance y ejecución. Entre estas se encuentran:

• Presupuesto limitado: La elección de tecnologías y servicios para la plataforma podría estar condicionada por limitaciones presupuestarias, lo que podría restringir la implementación de soluciones comerciales sofisticadas o integraciones complejas.

• Dependencia de infraestructura tecnológica: Para que la plataforma opere adecuadamente, es necesaria una conexión segura y estable entre el servicio de correo electrónico y los sistemas de seguridad, por lo que cualquier fallo en la infraestructura tecnológica puede impactar en el funcionamiento de la solución.

• Alcance geográfico y organizacional: La propuesta está dirigida únicamente a empresas del sector inmobiliario en el área de ventas, por lo que no incluye modificaciones para otras áreas o sectores, ni para pequeñas empresas con estructuras menos formales.

• Resistencia al cambio: La adopción de nuevas herramientas y procedimientos puede encontrar obstáculos entre el personal, lo que podría postergar la adopción efectiva y el éxito del componente de concientización.

• Tiempo de implementación y pruebas: El proyecto no abarca la etapa integral de puesta en marcha operativa en ambientes productivos ni la ejecución de pruebas rigurosas a largo plazo, sino que se centra en la propuesta, diseño y

evaluación inicial.

• Compatibilidad tecnológica: A pesar de que se pretende asegurar la compatibilidad con sistemas actuales, no se contempla la adaptación a todos los posibles ambientes tecnológicos presentes en las empresas inmobiliarias.

Estas delimitaciones permiten focalizar el desarrollo del proyecto en aspectos concretos y manejables, asegurando que los resultados sean alcanzables dentro del tiempo y recursos disponibles.

2.3.1 Procesos a Abordar

El presente proyecto se enfoca en analizar y optimizar los principales procesos de la empresa, identificados como áreas clave para mejorar la eficiencia y la seguridad. Específicamente, el alcance del proyecto está delimitado a los siguientes procesos:

- Proceso de Gestión Comercial: Se revisarán los flujos de comunicación y cotización, desde el contacto inicial con el cliente hasta la formalización del compromiso comercial, con el objetivo de estandarizar la información y los tiempos de respuesta.
- Proceso de Gestión Técnica y Producción: El proyecto intervendrá en la coordinación entre el área técnica y el cliente, desde la evaluación técnica inicial hasta la aprobación del diseño final y el inicio de la fabricación, para asegurar la correcta comunicación de los requerimientos.
- Proceso de Logística y Entrega: Se analizarán los procedimientos relacionados con la finalización del módulo, la coordinación de transporte y la entrega final al cliente, buscando mejorar el seguimiento y la conformidad del producto.

2.4 Marco teórico

En esta sección, se presentarán las referencias y antecedentes que constituyen la base teórica del proyecto. Las herramientas y metodologías que proporcionarán soporte al problema previamente descrito, que establecerán un marco para el desarrollo y análisis del proyecto.

2.4.1 Análisis de causa raíz (Ishikawa)

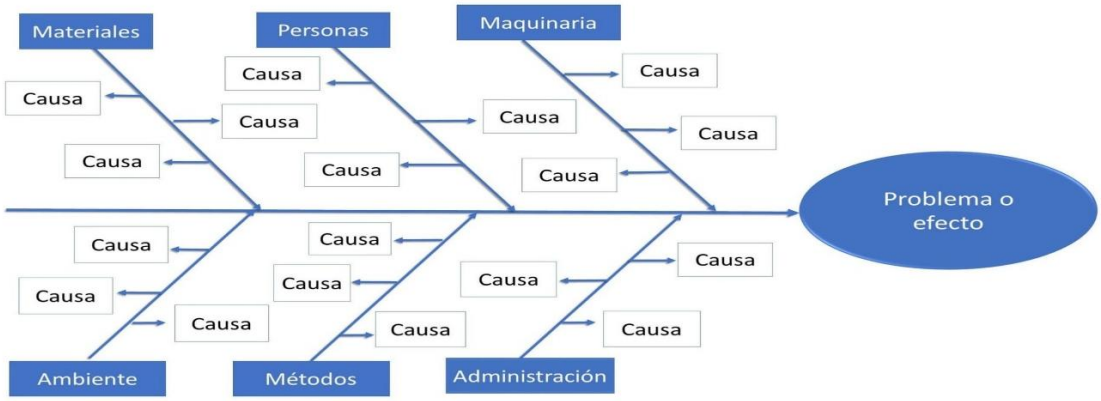
El Análisis de Causa Raíz (también conocido como diagrama de espina de pescado o diagrama de Ishikawa es un instrumento de calidad muy empleado para determinar las causas esenciales de un problema. Se utiliza en circunstancias donde es necesario analizar las distintas posibles causas de un problema particular, con el objetivo de no solo tratar los síntomas, sino alcanzar la raíz del problema. El esquema representa las potenciales causas en categorías y subcategorías, simplificando la interpretación de los elementos implicados.

En el contexto de este proyecto, el estudio de la causa raíz será esencial para comprender los elementos subyacentes que contribuyen a la vulnerabilidad del correo electrónico en las empresas inmobiliarias. Este estudio permitirá determinar si las dificultades de seguridad se originan de elementos tecnológicos, como la ausencia de filtros de correo eficaces, o de elementos humanos, como la ausencia de sensibilización y formación de los trabajadores. Utilizando el método Ishikawa, se podrá abordar cada causa de manera estructurada, diseñando soluciones que aborden las deficiencias fundamentales.

En el marco de este proyecto, el estudio de la causa raíz será esencial para comprender los elementos subyacentes que contribuyen a la vulnerabilidad del correo electrónico en las compañías de bienes raíces. Este estudio permitirá determinar si las dificultades de seguridad se originan de elementos tecnológicos, como la ausencia de filtros de correo eficaces, o de elementos humanos, como la ausencia de sensibilización y formación de los trabajadores. Mediante el uso del método Ishikawa, se podrá tratar cada causa de forma organizada,

elaborando soluciones que atiendan las carencias esenciales.

Figura 1: Ishikawa



Fuente: Diagrama de Ishikawa, https://www.webyempresas.com/ejemplos-de-diagrama-de-ishikawa/

2.4.2 Análisis de criticidad

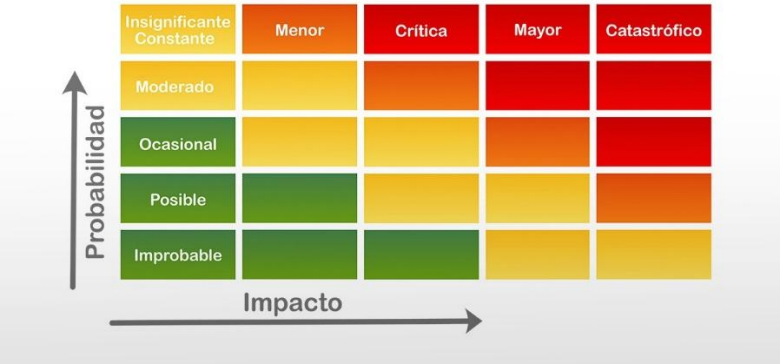
El Análisis de Criticidad es un procedimiento que facilita la valoración y asignación de prioridades a los problemas de acuerdo con su relevancia e impacto. Este estudio es esencial en la administración de riesgos y facilita la toma de decisiones fundamentadas sobre qué elementos necesitan ser atendidos de inmediato y cuáles pueden ser tratados en fases subsiguientes.

Para establecer la relevancia, se utiliza una mezcla de criterios y herramientas, en los que sobresale la aplicación de una matriz de criticidad. Esta perspectiva se fundamenta en dos factores clave: el posible impacto y la posibilidad de que ocurra un riesgo o problema. El impacto analiza las repercusiones de una equivocación o inconveniente en aspectos de seguridad, financieros, operativos, jurídicos y reputacionales. Por otro lado, la probabilidad se calcula a partir de la frecuencia prevista de estos sucesos, basándose en información histórica, estudios estadísticos y opiniones expertas.

La matriz de criticidad es una herramienta útil en este proceso porque ayuda a mostrar y medir cómo se relacionan el impacto de un problema y su probabilidad. En esta matriz, se clasifican los riesgos y se les da prioridad según cuán graves y frecuentes son, lo que hace más fácil identificar los que necesitan atención de

inmediato. Este método ayuda a enfocar los recursos y esfuerzos en las áreas más arriesgadas, lo cual es clave para crear estrategias de mitigación y gestión. Además, permite actualizar y revisar el análisis continuamente, adaptándose a los cambios en el entorno, así la organización se mantiene al tanto de los riesgos más importantes.

Figura 2: Matriz de Criticidad



Fuente: Delgado, D. (2020, julio 6). Cómo una matriz de riesgo puede ayudarte a crecer y agregar valor como profesional del riesgo. LinkedIn. https://www.linkedin.com/pulse/cómo-una-matriz-de-riesgo-puede-ayudarte-crecer-y-del-david/

Para ver cuán crítico es algo, se usa un método que combina la probabilidad de que algo falle con lo que pasaría si eso ocurre. Haciendo este cálculo, podemos obtener una evaluación numérica de la criticidad. La fórmula que se usa es: CRITICIDAD = PROBABILIDAD X IMPACTO

2.4.3 Ciclo de Deming

El Ciclo de Deming, que también se llama PDCA (Planificar-Hacer-Verificar-Actuar), es una forma de gestionar que se usa mucho para mejorar siempre los procesos, productos y servicios. Aunque se creó para la gestión de calidad, hoy en día se usa en muchas otras áreas, como la gestión de proyectos y la seguridad informática.

Este ciclo tiene cuatro etapas principales:

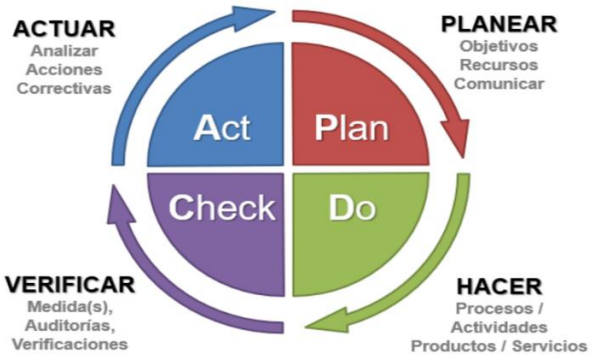
1. Planificar: En esta fase, se establecen los objetivos y se trazan los planes para alcanzarlos. Se trata de identificar los problemas que quieres resolver, qué recursos necesitas, quién se encargará de qué y hacer un cronograma detallado. Para un proyecto de ciberseguridad, esto significa analizar riesgos, elegir las tecnologías adecuadas y definir cómo medirás el éxito.

2. Hacer: Aquí es donde pones en marcha esos planes. Si estás trabajando en la seguridad del correo electrónico, tendrías que desarrollar la plataforma y hacer programas para educar a los usuarios. Es clave documentar bien todo y recopilar información que te ayude a ver cómo van las cosas.

3. Verificar: En esta etapa, se mide y evalúa lo que hiciste en la fase anterior. Comparas los resultados con los objetivos originales para saber si los estás cumpliendo. En seguridad informática, esto puede incluir revisar métricas como la disminución de incidentes, la detección de amenazas y la efectividad de las campañas de concientización.

4. Actuar: A partir de lo que evaluaste, identificas áreas donde puedes mejorar y tomas acciones correctivas o preventivas. El objetivo aquí es siempre buscar cómo mejorar el proceso y la solución, adaptándote a los cambios y nuevas amenazas. Esta etapa no solo cierra el ciclo, sino que también te prepara para empezar uno nuevo y seguir mejorando.

Figura 3: Ciclo de Deming



Fuente: Ciclo de Deming (PDCA), https://www.researchgate.net/figure/Figura-1-Ciclo-de-Deming-PDCA-Fuente-Elaboracion-propia_fig1_359416383

2.4.4 Marco NIST de Ciberseguridad (NIST Cybersecurity Framework - CSF)

NIST Cybersecurity Framework es un conjunto de directrices redactadas para ayudar a su organización a administrar los riesgos derivados de la ciberseguridad. Está compuesto por 5 funciones fundamentales que propician un enfoque global y ajustado, a la vez, para mitigar estos riesgos a los activos de información.

El marco se basa en cinco funciones clave que forman un ciclo completo para manejar la seguridad informática, además de incluir una función transversal relacionada con la gobernanza:

Gobernanza: Aunque no es una función directa dentro del ciclo principal, la gobernanza es un elemento clave que atraviesa toda la organización. Incluye políticas, procedimientos, roles y responsabilidades para manejar la ciberseguridad de manera integral. La gobernanza garantiza que las prácticas de seguridad estén alineadas con los objetivos estratégicos y las normativas vigentes, además de asegurar supervisión constante, rendición de cuentas y una mejora continua en los procesos de seguridad.

Identificar: En esta etapa se trata de conocer y entender los riesgos cibernéticos que pueden afectar a los sistemas y datos. Esto implica hacer un inventario de lo que se tiene, evaluar vulnerabilidades y amenazas, y establecer políticas para gestionar esos riesgos.

Proteger: Aquí se implementan las medidas necesarias para cuidar los activos que ya se identificaron. Esto incluye controles de acceso, cifrado de datos, autenticación segura, capacitar al personal y usar herramientas como firewalls y sistemas de detección de intrusos.

Detectar: Esta función consiste en reconocer eventos o actividades sospechosas, ya sea en tiempo real o lo más rápido posible. Para esto, se realiza un monitoreo constante, se analizan registros y se activan alertas ante cualquier intento de intrusión, malware o comportamiento inusual.

Responder: Cuando ocurre un incidente, esta fase se enfoca en cómo actuar para controlarlo y minimizar daños. Se necesitan protocolos claros para contener el problema, comunicar lo que está pasando y coordinarse con los equipos correspondientes, tanto internos como externos.

Recuperar: Finalmente, se trabaja en restaurar los sistemas y servicios afectados después del incidente. Esto incluye tener planes para asegurar la continuidad del negocio, hacer respaldos, probar la recuperación y aplicar mejoras para evitar que algo similar vuelva a pasar.

El Marco NIST CSF ofrece un enfoque organizado que ayuda a conocer cómo está la ciberseguridad en la empresa, a priorizar qué hacer para mejorar y a alinear los esfuerzos con los objetivos del negocio. Implementarlo facilita enfrentar las amenazas digitales, promoviendo una gestión activa y adaptable en un entorno tecnológico que cada día es más complejo.

Figura 4: NIST CSF

Fuente: El Marco de Seguridad Cibernética (CSF) 2.0 del NIST, https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.spa.pdf

3 Análisis de la situación actual

A continuación, se detallan los procesos internos que permiten el correcto funcionamiento de la empresa en su actividad principal: la fabricación y comercialización de soluciones modulares. Estos procesos abarcan desde el levantamiento de requerimientos por parte del cliente, pasando por el diseño y fabricación, hasta la venta, facturación y entrega de las unidades modulares. Cada área cumple un rol clave para garantizar la eficiencia operativa y la satisfacción del cliente final.

3.1 Descripción de la empresa

La empresa ContruPro es una compañía especializada en la construcción modular basada en contenedores, dedicada a la fabricación y comercialización de oficinas en base a contenedores, baños modulares y unidades personalizadas a pedido del cliente. Su propuesta de valor se enfoca en entregar soluciones modulares rápidas, funcionales y adaptables a distintas industrias, como la construcción, minería y servicios logísticos.

Opera principalmente en el mercado nacional y cuenta con una planta de producción propia, donde se ejecutan los procesos de diseño y fabricación.

Ubicación: La empresa se encuentra ubicada en Lampa, en el sector industrial de Avenida La Montaña, una zona que facilita la logística y distribución eficiente de sus productos modulares.

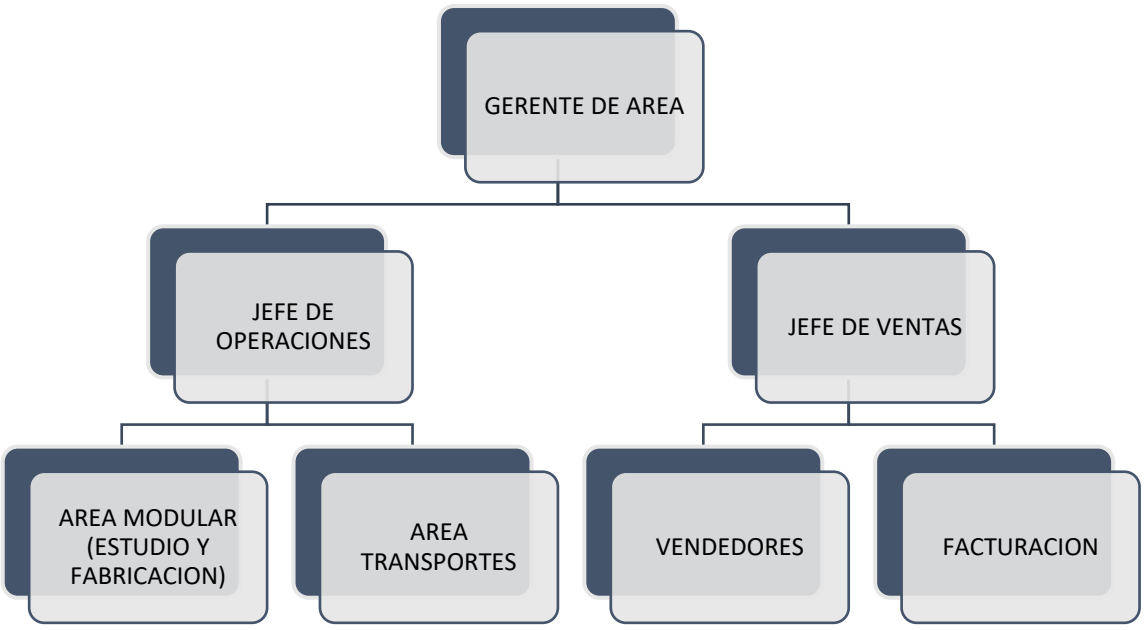
Misión: Diseñar, fabricar y comercializar soluciones modulares innovadoras, funcionales y personalizadas, que respondan a las necesidades de los clientes en distintos sectores productivos, con altos estándares de calidad, eficiencia y compromiso con el medio ambiente.

Visión: Ser líderes en el mercado nacional de construcción modular, reconocidos por la capacidad de innovación, calidad de servicio y compromiso con el desarrollo sustentable.

3.1.1 Organigrama de la empresa

La estructura organizacional de la empresa está compuesta por un equipo jerárquico que permite una gestión eficiente de los procesos técnicos, comerciales y administrativos. A continuación, se muestra el organigrama de la empresa, el cual refleja la distribución de responsabilidades y la relación entre las distintas áreas funcionales.

Figura 5: Organigrama de la empresa



Fuente: Elaboración propia con datos obtenidos de ContruPro

3.2 Procesos actuales de la empresa

En concordancia con lo establecido en el Capítulo 2, Alcance y delimitaciones del proyecto, el análisis de la situación actual se centra en los tres procesos definidos como objeto de estudio: Gestión Comercial, Gestión Técnica y Producción, y Logística y Entrega. Estos procesos fueron seleccionados por constituir el núcleo operativo de la empresa y representar las áreas más críticas en cuanto a su dependencia del correo electrónico y la exposición a riesgos de ciberseguridad.

A continuación, se describen los procesos clave que definen la operativa interna de la empresa. Estos procesos permiten el cumplimiento del ciclo productivo y comercial, desde la recepción de un requerimiento hasta la entrega de la unidad modular al cliente, y se dividen en tres áreas principales: Gestión Comercial, Gestión Técnica - Producción y finaliza con el área de Logística y Entrega. Si bien cada uno se explicará de forma separada para un mejor entendimiento, es importante destacar que el diagrama de procesos posterior los contempla de manera integrada, mostrando cómo interactúan en un único flujo unificado.

3.2.1 Proceso 1: Gestión Comercial

El proceso comercial abarca desde el primer contacto con el cliente hasta la validación del pago. Comienza con la recepción de la solicitud de cotización, la cual es derivada al área técnica para su valoración. Con esa información, el área comercial elabora y entrega una cotización formal al cliente.

Si el cliente aprueba la cotización, se gestiona el proceso de pago y se formaliza el compromiso comercial. Además, esta área se encarga de mantener la comunicación con el cliente a lo largo del proceso, entregando información de avance, condiciones de entrega y servicios adicionales como transporte.

Este proceso corresponde al primero de los definidos en el alcance del Capítulo 2 y constituye la base de la interacción con clientes.

3.2.2 Proceso 2: Gestión Técnica y Producción

Este proceso inicia cuando la solicitud del cliente es enviada desde el área comercial al área técnica. Aquí, se realiza una evaluación técnica de la solicitud, considerando viabilidad, diseño preliminar, materiales y costos. Esta información permite establecer una base para la cotización del proyecto.

Una vez aprobada la cotización por parte del cliente y efectuado el pago (total o anticipo), el área técnica coordina directamente con el cliente para definir los detalles arquitectónicos y funcionales del módulo. Tras la aprobación del diseño

final, el equipo técnico inicia la fabricación del módulo, cumpliendo con los estándares constructivos establecidos por la empresa.

Este proceso fue también delimitado en el Capítulo 2, ya que concentra la información técnica más sensible.

3.2.3 Proceso 3: Logística y Entrega

Una vez finalizada la fabricación del módulo, se activa el proceso de logística y entrega. En esta etapa, la empresa consulta al cliente si requiere el servicio de transporte por parte de la empresa. En caso afirmativo, se cotiza el traslado y se coordina el despacho al domicilio del cliente. Si el cliente prefiere retirar el módulo directamente desde la planta, se habilita esta opción.

El proceso finaliza con la recepción del módulo por parte del cliente, quien valida la conformidad del producto. Esta etapa es clave para asegurar la satisfacción del cliente y cerrar adecuadamente el ciclo de venta.

Finalmente, este proceso completa los tres definidos como alcance del proyecto, integrando la etapa de logística y entrega dentro del análisis de seguridad.

3.2.4 Diagrama de procesos

A continuación, se presentará un diagrama de flujo que describe el proceso completo de venta de un módulo en base a contenedor, desde la solicitud inicial del cliente hasta la entrega final del producto. Este flujo integra las acciones de las áreas comercial, técnica y de logística, permitiendo visualizar de forma clara la secuencia de actividades, puntos de decisión y responsabilidades involucradas en cada etapa del proceso.

A continuación, se detalla el flujo completo del proceso de venta de un módulo en base a contenedor, desde la solicitud inicial del cliente hasta la entrega del producto. Cada actividad se describe a continuación:

- **Solicita cotización.**

El proceso se inicia cuando un cliente manifiesta su interés en adquirir una solución modular. Esta solicitud puede ser realizada por distintos canales (correo, formulario web, contacto directo) y marca el inicio de la interacción comercial.

- **Envía solicitud al área técnica (Proceso 1: Gestión Comercial).**

Una vez recibida la solicitud, el área comercial deriva el requerimiento al equipo técnico con el fin de evaluar su viabilidad. Esto incluye el levantamiento inicial de necesidades y requisitos funcionales del cliente.

- **Revisa la solicitud y valoriza (Proceso 2: Gestión Técnica y Producción).**

El área técnica analiza la solicitud considerando aspectos como diseño preliminar, tipo de módulo, requerimientos especiales, materiales y costos asociados. A partir de esta valoración técnica, se entrega la información base para la generación de una cotización formal.

- **Genera cotización (Proceso 1: Gestión Comercial).**

Con la información técnica, el área comercial elabora una cotización detallada. Esta incluye el alcance del proyecto, especificaciones técnicas del módulo, plazos estimados de entrega, condiciones comerciales y, si corresponde, opciones de transporte.

- **Revisa cotización.**

El cliente recibe y revisa la cotización enviada por la empresa. En esta etapa, puede realizar consultas, solicitar modificaciones o directamente aprobar la propuesta.

- **¿Aprueba cotización?**

Esta es una etapa de decisión. Si el cliente no aprueba la cotización, el proceso se detiene o se reformula según los nuevos requerimientos. Si aprueba, se avanza al pago.

- **Recibe pago del cliente (Proceso 1: Gestión Comercial).**

Una vez aprobada la cotización, el cliente efectúa el pago según lo acordado. Esto puede corresponder al pago total o a un anticipo, lo que formaliza el compromiso comercial.

- **Gestiona diseño del módulo junto al cliente (Proceso 2: Gestión Técnica y Producción).**

Con el pago confirmado, el área técnica se reúne con el cliente para desarrollar el diseño definitivo del módulo. Esta fase incluye la definición de distribución interior, terminaciones, instalaciones eléctricas, sanitarias, y cualquier requerimiento adicional.

- **Fabricación del módulo (Proceso 2: Gestión Técnica y Producción).**

Con el diseño aprobado, se inicia el proceso de fabricación en la planta de producción. El área técnica coordina la ejecución respetando los estándares de calidad definidos por la empresa, asegurando el cumplimiento de los plazos y requerimientos funcionales del cliente.

- **Consulta al cliente por cotización de transporte con la empresa (Proceso 3: Logística y Entrega).**

Una vez fabricado el módulo, el área logística consulta al cliente si desea incluir el servicio de transporte. En caso afirmativo, se cotiza y gestiona el traslado desde la planta hasta el lugar de destino.

- **¿Se incluye transporte? (Proceso 3: Logística y Entrega).**

El cliente define si utilizará el transporte proporcionado por la empresa o si retirará el módulo por sus propios medios.

- **Despacha a domicilio del cliente (Proceso 3: Logística y Entrega).**

Si el cliente opta por el servicio de transporte, se coordina el despacho al domicilio indicado. El equipo logístico programa el envío según disponibilidad y condiciones pactadas.

- **Retira el módulo en dependencias de la empresa.**

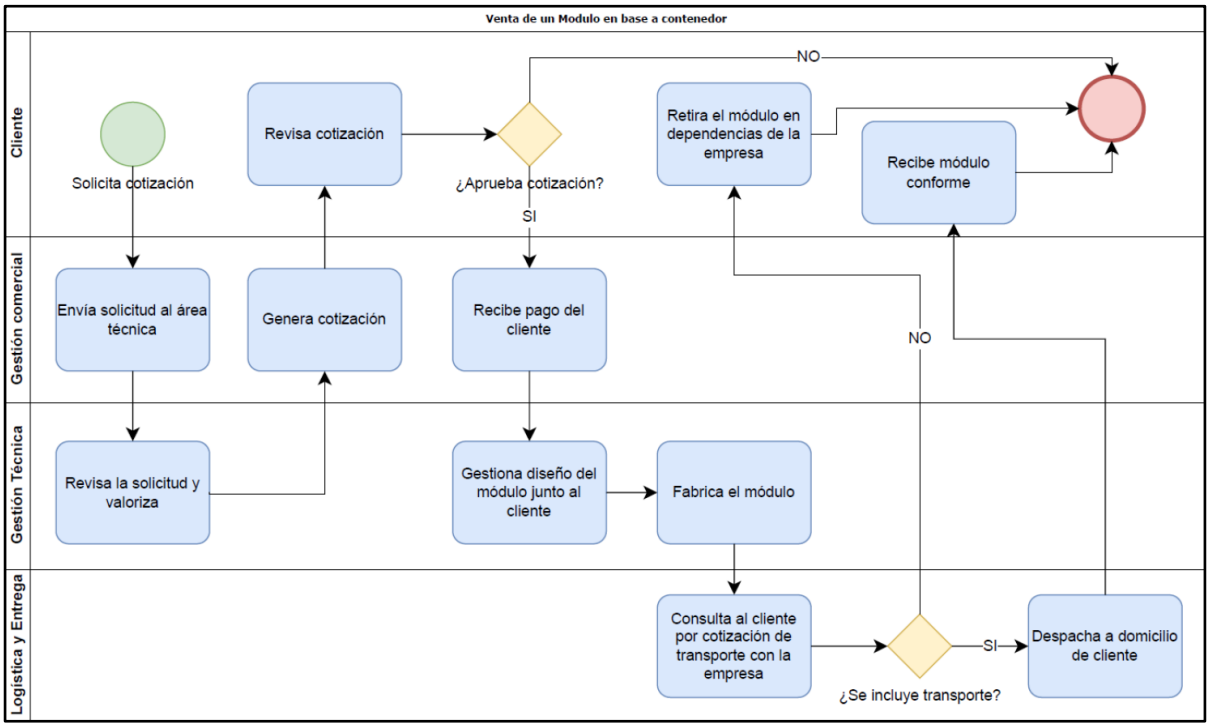
Si el cliente decide no contratar el transporte, se agenda la entrega del módulo en la planta de producción, desde donde el cliente lo retira directamente.

- **Recibe el módulo conforme.**

Una vez recibido el módulo, ya sea en domicilio o en planta, el cliente realiza una revisión para verificar que cumple con lo especificado en el diseño. En caso de conformidad, se da por finalizado el proceso.

Una vez definidas todas las actividades que conforman este flujo de trabajo, a continuación, se presenta el diagrama que permite visualizar gráficamente cómo interactúan entre sí los distintos actores y etapas del proceso, facilitando así su comprensión y análisis.

Figura 6: Diagrama general del proceso



Fuente: Elaboración propia con datos obtenidos de ContruPro.

3.3 Descripción de problemas

El correcto funcionamiento de la empresa y su ciclo de venta de soluciones modulares se sustenta en una serie de procesos que abarcan la Gestión Comercial, la Gestión Técnica y la Logística de entrega. En cada una de estas etapas, desde la solicitud inicial de una cotización hasta la coordinación del despacho final. Esta estructuración posiciona al correo electrónico como la principal herramienta de comunicación e intercambio de información sensible. Esta dependencia crítica, si bien agiliza la operación, el problema se sitúa en que se ha transformado el correo electrónico en una herramienta esencial para el funcionamiento de la empresa, esto provoca que sea un punto atractivo para los cibercriminales, exponiendo a la organización a diversos ciberataques como el fraude, el phishing y la suplantación de identidad.

Para comprender a fondo las causas raíz que originan esta problemática, a continuación, se realizará un análisis detallado mediante un diagrama de Ishikawa, descomponiendo los factores que contribuyen a la inseguridad en cada fase del proceso de negocio.

- **Riesgos en la Gestión Comercial Inicial:** Este se basa en la comunicación por correo electrónico para establecer el primer contacto y enviar la propuesta económica. Esta dependencia abre la puerta a ataques que buscan abusar de la confianza en las etapas tempranas del ciclo comercial.

    - **Recepción de solicitudes de cotización fraudulentas:** Los atacantes pueden enviar correos de phishing que imitan a clientes potenciales para extraer información sobre precios, procesos internos y especificaciones técnicas, utilizando estos datos para planificar ataques más complejos.
    - **Fuga de información sensible en cotizaciones:** Las cotizaciones enviadas por correo electrónico contienen datos valiosos como precios, plazos y especificaciones técnicas del módulo. Si estos

correos son interceptados, la información confidencial de la empresa quedaría expuesta a la competencia o a actores maliciosos.

- **Vulnerabilidades en el Proceso Técnico y de Diseño:** La interacción entre el área comercial, el área técnica y el cliente para definir los detalles del producto es una fase crítica donde se intercambia información de propiedad intelectual y datos específicos del proyecto.

    - **Comunicación insegura entre áreas:** Durante este proceso se intercambian detalles técnicos y funcionales que son propiedad intelectual de la empresa, La falta de protección en estas comunicaciones expone los planos y diseños a robos u modificaciones, que compromete la integridad de la información.
    - **Manipulación de los detalles funcionales:** La intervención de la información del proceso termina generando sobrecostos o productos incorrectos. Que dañan la reputación y prestigio de la empresa

- **Debilidades en el Proceso de Pago:** Esta etapa constituye la fase de mayor exposición a riesgos financieros y operativos, ya que la formalización del compromiso comercial depende del intercambio de información sensible a través del correo electrónico.

    - **Suplantación de Identidad para la Desviación de Fondos:** En esta instancia, existe un riesgo elevado de ataques de suplantación de identidad, donde un actor malicioso se hace pasar por la empresa para enviar al cliente instrucciones de pago fraudulentas. Un ataque exitoso resulta en la desviación de fondos a cuentas de terceros, generando una pérdida económica directa para el cliente y un daño irreparable a la confianza y prestigio de la empresa.

- **Falsificación de información de pago:** Un atacante puede suplantar la identidad del cliente para enviar un comprobante de pago adulterado al área comercial. Si el equipo no verifica la acreditación de los fondos y da por válido el comprobante, se iniciaría el proceso de "Fabricación del módulo" bajo una premisa falsa. Esto ocasionaría una pérdida directa para la empresa.
- **Falsificación de información De la empresa cliente:** los clientes envían información falsa para poder obtener crédito, el nivel de ocurrencia de esto es alto, el impacto es que si se le llaga a dar crédito solo con la información que entregan por correo después no tienen para pagar.

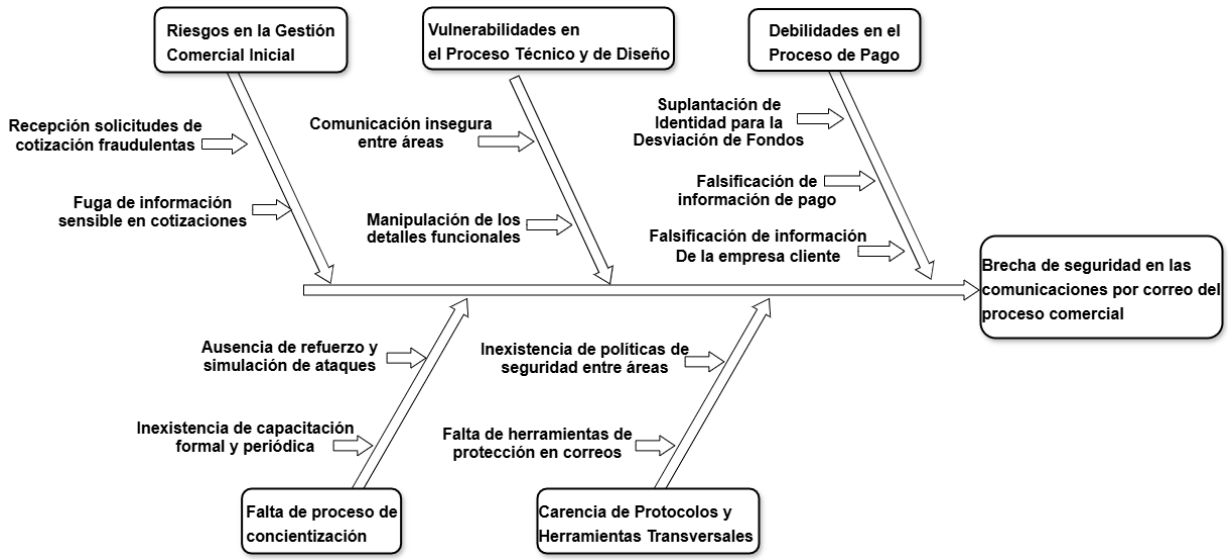
- **Falta de proceso de concientización:** Al no existir una política o herramienta de concientización, los empleados no desarrollan la capacidad de detectar cuando se está frente a un correo fraudulento.

  - **Inexistencia de capacitación formal y periódica:** El personal de las distintas áreas no recibe formación estructurada sobre las tácticas de ingeniería social, como el phishing y la suplantación de identidad. Sin un programa de capacitación que enseñe a identificar las señales de un correo malicioso, los empleados basan su comunicación únicamente en la confianza.
  - **Ausencia de refuerzo y simulación de ataques**: La empresa carece de un sistema de refuerzo, como campañas de phishing simulado, que permita a los empleados poner a prueba sus conocimientos en un entorno seguro.

- **Carencia de Protocolos y Herramientas Transversales:** La ausencia de una estrategia de seguridad integral que proteja el flujo de comunicación interno y externo de la empresa.

- **Inexistencia de políticas de seguridad entre áreas:** No existen protocolos definidos para el intercambio seguro de información entre las áreas comercial, técnica y logística. Esto provoca que cada empleado maneje información sensible según su propio criterio.
- **Falta de herramientas de protección en correos:** La ausencia de medidas de protección adecuadas y la escasa implementación de sistemas de seguridad específicos para el correo electrónico, deja a los empleados sin defensas tecnológicas contra phishing, malware o suplantación de identidad

Figura 7: Diagrama de Ishikawa.

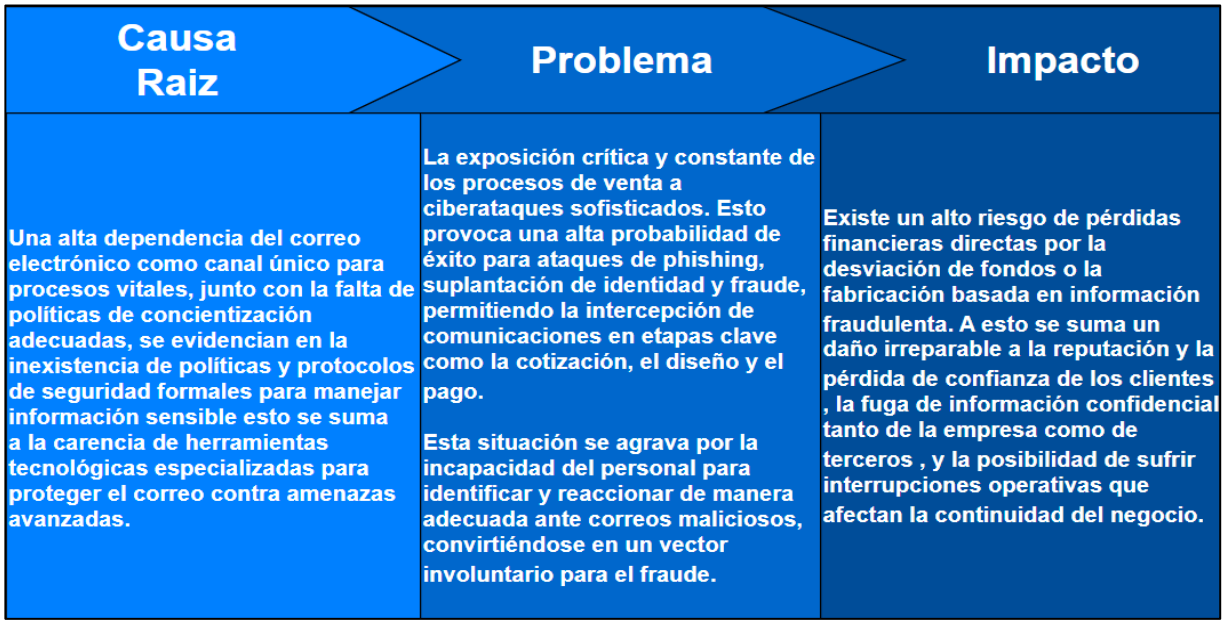


Fuente: Elaboración propia con datos obtenidos de ContruPro.

El análisis demuestra que la principal debilidad de la empresa reside en su alta dependencia del correo electrónico, un canal que carece de las medidas de seguridad adecuadas. Esta vulnerabilidad no es un hecho aislado, sino una condición que afecta a todo el proceso de venta, desde el contacto inicial hasta el pago final. Las causas raíz apuntan a una combinación de factores críticos: la falta de herramientas tecnológicas de protección, la inexistencia de protocolos de seguridad formalizados entre las distintas áreas y una escasa cultura de

ciberseguridad que deja a los empleados sin la capacidad de reconocer y responder a amenazas. Esta situación expone a la organización a un riesgo crítico y constante de sufrir fraudes, pérdidas financieras y daños irreparables a su reputación.

Figura 8: Diagrama de causa-problema-impacto.



Fuente: Elaboración propia con datos obtenidos de ContruPro.

3.4 Clasificación de riesgos o criticidad

En este punto se aborda la identificación y clasificación de los riesgos asociados al uso del correo electrónico en el proceso de ventas de la empresa ContruPro.

Se analizarán las principales vulnerabilidades que comprometen la integridad operativa y la seguridad financiera, detallando cómo estas afectan la continuidad del negocio. Para determinar la criticidad de cada riesgo se realizará un análisis detallado de la frecuencia, probabilidad de ocurrencia y consecuencias

Tabla 1: Probabilidad

Valor	Probabilidad	Descripción
1	Muy Baja	La ocurrencia del incidente es extremadamente rara y requeriría una combinación única y altamente improbable de fallos.
2	Baja	El incidente es posible, pero no se espera que ocurra en condiciones normales. Podría suceder esporádicamente a lo largo de varios años.
3	Moderada	Es probable que el incidente ocurra varias veces al año. Los ataques de phishing y los intentos de fraude son una amenaza conocida y recurrente.
4	Alta	El incidente ocurre con regularidad, probablemente de forma mensual. La organización está constantemente expuesta a correos maliciosos que evaden los filtros básicos.
5	Muy Alta	La ocurrencia es casi constante, con incidentes o intentos de ataque reportados semanalmente. La superficie de ataque es explotada activamente.
6	Inminente	La ocurrencia de un incidente exitoso es inminente y prácticamente garantizada si no se toman medidas. Ocurren intentos de ataque a diario.

Fuente: Elaboración propia con datos obtenidos de ContruPro.

Tabla 2: Impacto

Valor	Impacto	Descripción
1	Bajo	El impacto es menor y contenido. Causa inconvenientes operativos leves o pérdidas financieras insignificantes que no afectan la continuidad del proyecto ni la relación con el cliente.
2	Moderado	El impacto afecta un proyecto de manera notoria. Provoca una interrupción operativa que requiere gestión, pérdidas financieras moderadas o un daño reputacional que afecta la confianza de un cliente específico.
3	Alto	El impacto es grave y afecta a la organización. Genera pérdidas financieras significativas, una interrupción importante de las operaciones y una crisis de reputación que daña la imagen pública de la empresa.
4	Crítico	El impacto amenaza la viabilidad del negocio. Causa pérdidas financieras devastadoras, la paralización de las operaciones o un daño irreparable a la marca, con posibles consecuencias legales.

Fuente: Elaboración propia con datos obtenidos de ContruPro.

Una vez definidas las dimensiones, procedemos a realizar el análisis de riesgo y su magnitud correspondiente. Este proceso se lleva a cabo mediante la multiplicación de los factores de probabilidad e impacto, lo que nos permite obtener la Magnitud del riesgo, tal como se describe en la tabla siguiente:

Tabla 3: Matriz de riesgo

	Bajo (1)	Moderado (2)	Alto (3)	Crítico (4)	Impacto
Inminente (6)	6	12	18	24	
Muy Alta (5)	5	10	15	20	
Alta (4)	4	8	12	15	
Moderada (3)	3	6	9	12	
Baja (2)	2	4	6	8	
Muy Baja (1)	1	2	3	4	
Probabilidad					

Fuente: Elaboración propia con datos obtenidos de ContruPro.

Para categorizar la magnitud es necesario considerar el impacto que tiene en la empresa. Por eso, se ha elaborado la siguiente tabla para establecer una relación clara entre la magnitud del riesgo y su posible afectación en los servicios.

Tabla 4: Magnitud

Valor	Magnitud	Descripcion
(1-5)	Bajo	Riesgo aceptable que requiere monitoreo.
(6-10)	Moderado	Riesgo que requiere medidas de mitigación específicas.
(11-16)	Alto	Riesgo significativo que requiere atención prioritaria.
(17-24)	Critico	Riesgo inaceptable que requiere acción inmediata.

Fuente: Elaboración propia con datos obtenidos de ContruPro.

3.5 Resumen de criticidad

Habiendo establecido en el análisis anterior el alto nivel de riesgo al que se expone la empresa y dada la alta dependencia del correo electrónico en el ciclo comercial, es fundamental realizar una evaluación formal de los riesgos asociados. Este apartado se enfoca en identificar y clasificar las amenazas de ciberseguridad que surgen en el flujo de comunicación con el cliente.

Para asegurar un entendimiento claro y estandarizado de cada riesgo, estos se definirán utilizando una nomenclatura basada en las directrices de NIST, estructurada como: Amenaza + Vulnerabilidad + Activo + Consecuencia. Posteriormente, se cuantificará la criticidad de cada uno a través de un análisis detallado de su probabilidad de ocurrencia y la severidad de su impacto.

Riesgos detectados:

- Suplantación de identidad para desviar pagos de clientes: Un ciberdelincuente puede suplantar la identidad de la empresa, aprovechando la vulnerabilidad de no contar con canales de pago verificados, para engañar al cliente y desviar los fondos destinados al pago, lo que resulta en una pérdida financiera directa y un daño crítico a la reputación.

- Recepción de solicitudes fraudulentas(phishing) para robo de información: Mediante ataques de phishing dirigido, los atacantes explotan la falta de filtros de correo y capacitación del personal para extraer información comercial confidencial, con la consecuencia de que estos datos se fuguen para espionaje comercial o para planificar ataques futuros.

- Recepción de comprobantes de pago falsificados: Un atacante puede suplantar la identidad de un cliente y, debido a la vulnerabilidad de un proceso de validación de pago manual, engañar a la empresa con un comprobante falso para que se utilicen los recursos de producción, generando como consecuencia una pérdida económica por fabricar y entregar un producto sin haber recibido el pago.

- Manipulación de diseños y especificaciones técnicas vía correo: La amenaza de interceptación de comunicaciones aprovecha la vulnerabilidad de intercambiar información de diseño sin cifrado, poniendo en riesgo los planos y especificaciones del módulo, lo que tiene como consecuencia errores de producción, sobrecostos y un grave daño reputacional.

- Suplantación para coordinar entregas fraudulentas del módulo: A través de la suplantación de identidad del personal logístico y aprovechando que la coordinación de la entrega se realiza por canales no verificados, un atacante puede coordinar el retiro del módulo físico terminado, resultando en el robo del producto y la pérdida financiera total.

- Fuga de información sensible en cotizaciones enviadas: La interceptación de correos explota la vulnerabilidad del envío de documentos comerciales sin cifrar, lo que puede exponer la estrategia de precios y las cotizaciones y generar como consecuencia una pérdida de ventaja competitiva para la empresa.

- Falsificación de información de la empresa cliente: Un atacante puede crear una identidad de cliente fraudulenta, aprovechando la vulnerabilidad de un proceso de alta de clientes sin la debida verificación, para consumir los recursos comerciales y técnicos, cuya consecuencia es el desgaste de recursos y el potencial espionaje comercial.

Tabla 5: Resumen de criticidad

Riesgo	Probabilidad	Impacto	Magnitud	Nivel de Riesgo
Suplantación de identidad para desviar pagos de clientes	4	4	16	Alto
Recepción de solicitudes fraudulentas (Phishing) para robo de información	5	2	10	Moderado
Recepción de comprobantes de pago falsificados	4	4	16	Alto
Manipulación de diseños y especificaciones técnicas vía correo	3	3	9	Moderado
Suplantación para coordinar entregas fraudulentas del módulo	2	3	6	Moderado
Fuga de información sensible en cotizaciones enviadas	3	2	6	Moderado
Falsificación de información de la empresa cliente	5	4	20	Critico

Fuente: Elaboración propia con datos obtenidos de ContruPro.

En conclusión, el análisis de la situación actual revela que la organización opera con un nivel de riesgo elevado en sus procesos comerciales, originado por la dependencia crítica del correo electrónico como principal canal de comunicación. La evaluación cuantitativa demuestra que la suplantación de identidad para el desvío de fondos de clientes representa un riesgo de nivel Alto, constituyendo una amenaza prioritaria para la estabilidad financiera de la empresa. Adicionalmente, la presencia de múltiples riesgos clasificados como Moderados indica una debilidad sistémica que puede erosionar la confianza del cliente y la eficiencia operativa. Este escenario es el resultado directo de la falta de herramientas tecnológicas de protección, la ausencia de protocolos de seguridad formalizados y una insuficiente cultura de ciberseguridad en el personal. Por lo tanto, se confirma la necesidad imperativa de implementar una solución integral que mitigue estas amenazas y fortalezca las defensas de la organización

4 Propuesta de mejora

Tras el detallado análisis presentado en el capítulo anterior, que evidenció la alta dependencia del correo electrónico y las consecuentes vulnerabilidades críticas en los procesos de negocio. En el presente capitulo se presentará una propuesta de mejora integral diseñada para robustecer la seguridad en la actividad principal de la empresa: la comercialización y fabricación de soluciones modulares. Esta solución abarca desde la implementación de herramientas tecnológicas especializadas para la protección del correo electrónico, hasta el fortalecimiento del factor humano a través de un componente de concientización para el personal. Cada elemento de esta propuesta cumple un rol clave para abordar las causas raíz identificadas y mitigar los riesgos de fraude, suplantación de identidad y fuga de información, garantizando así la integridad, la continuidad operativa y la reputación de la organización

4.1 Identificación de procesos

La propuesta de mejora se aplicará de manera transversal a los tres macroprocesos que componen el ciclo de negocio de la empresa, los cuales fueron descritos en el apartado “3.2.- Procesos actuales de la empresa”. El análisis de la situación actual demostró que, si bien cada proceso tiene funciones distintas, todos coinciden en una debilidad común y crítica: la dependencia de un canal de comunicación inseguro como el correo electrónico. Como se expuso en el diagrama de Ishikawa en la sección “3.3.- Descripción de problemas”, las causas raíz como, por ejemplo: “Falta de herramientas de protección en correos” y “Inexistencia de capacitación formal y periódica” no son exclusivas de un área, sino que se extienden a lo largo de todo el flujo de venta. Por ello, un enfoque aislado sería insuficiente, ya que dejaría expuestas otras fases del ciclo comercial a los mismos ataques. La decisión de intervenir en todos los procesos se fundamenta en esta interconexión, reconociendo que “la seguridad de la cadena es igual a la de su eslabón más débil”.

Los procesos que serán sometidos a mejora son:

- **Proceso 1: Gestión Comercial**: Desde la recepción de solicitudes de cotización hasta la gestión de pagos, esta área intercambia constantemente información sensible que es susceptible a ataques de phishing y fraude financiero.
- **Proceso 2: Gestión Técnica y Producción**: En esta fase se definen y comunican diseños, especificaciones y detalles técnicos, cuya interceptación o manipulación puede derivar en pérdidas económicas, robo de propiedad intelectual y daños reputacionales.
- **Proceso 3: Logística y Entrega**: La coordinación del despacho y la entrega final del producto también depende del correo electrónico, abriendo una ventana de riesgo para la suplantación de identidad con el fin de desviar la entrega física de los activos.

En definitiva, dado que la vulnerabilidad reside en una herramienta transversal a toda la operación, es importante que la solución se implemente de forma general. Limitar la mejora a un solo proceso, como lo es gestión comercial o logística y entrega, crearía una falsa sensación de seguridad, ya que los ciberdelincuentes podrían simplemente pivotar sus ataques hacia las fases de Gestión técnica o producción, que permanecerían desprotegidas. Por lo tanto, solo un enfoque integral que abarque el ciclo de negocio completo puede garantizar una mitigación efectiva de los riesgos identificados. La implementación de esta propuesta en las áreas comercial, técnica y logística busca crear una defensa cohesiva y robusta, cerrando las brechas de seguridad en cada punto de contacto y fortaleciendo la adaptación de la empresa frente a amenazas externas.

4.2 Ciclo de Deming

Para la implementación de la propuesta de mejora se utilizará el Ciclo de Deming, también conocido como PDCA (Planificar, Hacer, Verificar, Actuar), como marco metodológico. Esta metodología se ha seleccionado por su enfoque iterativo y su capacidad para la mejora continua de procesos y sistemas. El enfoque del proyecto combina la implementación de una herramienta crítica con un cambio

en la cultura organizacional a través de la concientización, lo que exige un enfoque estructurado que permita planificar las acciones, ejecutarlas de forma controlada, medir su efectividad y ajustar la estrategia según los resultados obtenidos. La aplicación de este ciclo garantizará que la solución no solo se implemente correctamente, sino que también evolucione y se adapte a las nuevas amenazas, consolidando una postura de seguridad robusta y sostenible en el tiempo para la empresa.

4.2.1 Plan (Planificar)

Esta primera fase es fundamental para el éxito del proyecto, ya que en ella se definen los objetivos, se trazan los planes detallados y se asignan los recursos necesarios para alcanzar las metas propuestas. La etapa de planificación establecerá una hoja de ruta clara para la implementación de la plataforma de seguridad de correo y el componente de concientización, asegurando que todas las acciones posteriores estén alineadas con las necesidades estratégicas de la organización identificadas en el análisis de la situación actual.

A continuación, se presenta el listado detallado de tareas para llevar a cabo esta fase del proyecto:

Fase 1: Constitución del Proyecto y Planificación Inicial (Duración estimada: 2 semanas)

- **Tarea 1.1:** Oficializar y conformar el equipo de trabajo del proyecto.
    - Descripción: Asignar formalmente a los profesionales para los roles de jefe de Proyecto, Especialista en Ciberseguridad, Analista de Infraestructura TI, Analista de Calidad (QA) y Consultor de Concientización.
    - Responsable: Gerencia, Jefe de Proyecto.
    - Duración estimada: 2 días.

- **Tarea 1.2:** Realizar la reunión de lanzamiento del proyecto (kick-off).
    - Descripción: Alinear al equipo completo sobre el alcance, los objetivos, los entregables, el presupuesto y las responsabilidades de cada integrante.
    - Responsable: Jefe de Proyecto.
    - Duración estimada: 1 día.
- **Tarea 1.3:** Desarrollar el Plan de Gestión del Proyecto.
    - Descripción: Elaborar el cronograma maestro, el presupuesto detallado, el plan de gestión de riesgos y el plan de comunicaciones para mantener informada a la gerencia.
    - Responsable: Jefe de Proyecto.
    - Duración estimada: 1 semana.
- **Tarea 1.4:** Definir los Indicadores Clave de Rendimiento (KPIs) del proyecto.
    - Descripción: Establecer las métricas cuantitativas que permitirán medir el éxito de la implementación, como la "tasa de reducción de incidentes de phishing reportados" y el "porcentaje de mejora en las campañas de simulación".
    - Responsable: Jefe de Proyecto, Especialista en Ciberseguridad, Consultor de Concientización.
    - Duración estimada: 3 días.

Fase 2: Investigación, Evaluación y Selección de Herramientas (Duración estimada: 3 semanas)

- **Tarea 2.1:** Realizar un levantamiento detallado de la infraestructura de TI actual.

- Descripción: Documentar la configuración del servicio de correo electrónico, los registros DNS, la gestión de usuarios y los sistemas existentes para asegurar la compatibilidad técnica de la futura plataforma.
- Responsable: Analista de Infraestructura TI.
- Duración estimada: 1 semana.

- **Tarea 2.2:** Investigar y evaluar soluciones de seguridad de correo electrónico del mercado.
  - Descripción: Analizar un mínimo de tres soluciones comerciales líderes, comparando su eficacia en la detección de amenazas, facilidad de integración, soporte y modelo de licenciamiento.
  - Responsable: Especialista en Ciberseguridad.
  - Duración estimada: 2 semanas.
- **Tarea 2.3:** Investigar y seleccionar una plataforma para la gestión de concientización.
  - Descripción: Evaluar herramientas que permitan la ejecución de campañas de phishing simulado y la administración de módulos de capacitación para los empleados.
  - Responsable: Consultor de Concientización.
  - Duración estimada: 1.5 semanas (actividad en paralelo a la Tarea 2.2).
- **Tarea 2.4:** Seleccionar al proveedor y gestionar la adquisición.
  - Descripción: Presentar un informe comparativo a la gerencia con la recomendación final y proceder con la gestión de la compra de las licencias y/o servicios de los proveedores seleccionados.
  - Responsable: Jefe de Proyecto, Especialista en Ciberseguridad.

- Duración estimada: 1 semana.

Fase 3: Diseño Detallado de la Solución (Duración estimada: 4 semanas)

- **Tarea 3.1:** Diseñar la arquitectura técnica y el plan de integración.
  - Descripción: Crear el diagrama de flujo de correo futuro y el plan de acción para la configuración de la nueva plataforma en la infraestructura existente, minimizando el impacto en la operación.
  - Responsable: Especialista en Ciberseguridad, Analista de Infraestructura TI.
  - Duración estimada: 1 semana.
- **Tarea 3.2:** Diseñar las políticas de seguridad en la plataforma.
  - Descripción: Definir y documentar las reglas específicas para la detección de phishing, suplantación de identidad, malware y otras amenazas, basándose en los riesgos críticos identificados para la empresa.
  - Responsable: Especialista en Ciberseguridad.
  - Duración estimada: 2 semanas.
- **Tarea 3.3:** Diseñar el contenido y materiales del programa de concientización.
  - Descripción: Crear los módulos de capacitación, guías rápidas, infografías y videos educativos que se utilizarán para formar a los empleados. Se usarán ejemplos de incidentes reales bloqueados para maximizar el impacto.
  - Responsable: Consultor de Concientización.
  - Duración estimada: 3 semanas.

- **Tarea 3.4:** Diseñar el plan de pruebas de calidad (QA).
    - Descripción: Elaborar un documento exhaustivo con todos los casos de prueba, incluyendo escenarios para validar la correcta detección de amenazas, la identificación de falsos positivos y el flujo normal de correos legítimos.
    - Responsable: Analista de Calidad (QA).
    - Duración estimada: 2 semanas.
- **Tarea 3.5:** Planificar la comunicación y gestión del cambio.
    - Descripción: Preparar los comunicados, la agenda de socialización y los recursos de apoyo para informar a toda la organización sobre los próximos cambios, con el fin de minimizar la resistencia y asegurar una adopción exitosa.
    - Responsable: Jefe de Proyecto, Consultor de Concientización.
    - Duración estimada: 1 semana.

Fase 4: Configuración y Pruebas en Entorno Controlado (Duración estimada: 3 semanas)

- **Tarea 4.1:** Habilitar y configurar el entorno de pruebas.
    - Descripción: Crear un ambiente técnico aislado que replique las condiciones del sistema de correo electrónico de producción, para poder realizar pruebas sin afectar la operatividad del negocio.
    - Responsable: Analista de Infraestructura TI.
    - Duración estimada: 3 días.
- **Tarea 4.2:** Instalar y configurar la plataforma de seguridad en el entorno de pruebas.

- Descripción: Realizar el despliegue inicial de la solución de seguridad y aplicar las políticas de protección (anti-phishing, anti-malware, etc.) que fueron diseñadas en la fase de planificación.
- Responsable: Especialista en Ciberseguridad.
- Duración estimada: 1 semana.

- **Tarea 4.3:** Ejecutar el plan de pruebas de calidad (QA).
  - Descripción: El Analista de Calidad ejecutará todos los casos de prueba definidos para validar que la plataforma detecta y bloquea correctamente las amenazas, y que no interfiere con el flujo de correos legítimos (pruebas de falsos positivos).
  - Responsable: Analista de Calidad (QA).
  - Duración estimada: 1 semana.
- **Tarea 4.4:** Documentar y resolver las incidencias detectadas.
  - Descripción: Registrar cualquier defecto o comportamiento inesperado durante las pruebas y asignarlo al Especialista en Ciberseguridad para su corrección antes de pasar al siguiente paso.
  - Responsable: Analista de Calidad (QA), Especialista en Ciberseguridad.
  - Duración estimada: 3 días (en paralelo con la Tarea 4.3).
- **Tarea 4.5:** Obtener la aprobación formal de QA.
  - Descripción: El Analista de Calidad emite un informe de resultados y da la aprobación formal para proceder con el despliegue en el ambiente productivo.
  - Responsable: Analista de Calidad (QA).
  - Duración estimada: 1 día.

Fase 5: Despliegue en Producción y Lanzamiento (Duración estimada: 2 semanas)

- **Tarea 5.1:** Comunicar oficialmente el inicio del despliegue.
    - Descripción: Enviar la comunicación oficial a toda la organización, informando la fecha y hora de la ventana de implementación para que los usuarios estén al tanto.
    - Responsable: Jefe de Proyecto.
    - Duración estimada: 1 día.
- **Tarea 5.2:** Ejecutar el despliegue técnico en producción.
    - Descripción: Realizar las configuraciones técnicas necesarias (ej. cambio de registros MX del DNS) para que todo el flujo de correo de la empresa sea procesado por la nueva plataforma de seguridad. Esta tarea se debe ejecutar en un horario de bajo impacto.
    - Responsable: Especialista en Ciberseguridad, Analista de Infraestructura TI.
    - Duración estimada: 2 días.
- **Tarea 5.3:** Realizar monitoreo post-implementación.
    - Descripción: Durante los primeros días de funcionamiento, supervisar activamente la plataforma para detectar y resolver de inmediato cualquier anomalía, asegurando la continuidad operativa.
    - Responsable: Especialista en Ciberseguridad, Analista de Infraestructura TI.
    - Duración estimada: 1 semana.

- **Tarea 5.4:** Lanzar el programa de concientización a toda la empresa.
    - Descripción: Enviar la comunicación de bienvenida al programa, dar acceso a los primeros módulos de capacitación y presentar los objetivos de la iniciativa.
    - Responsable: Consultor de Concientización.
    - Duración estimada: 2 días.
- **Tarea 5.5:** Ejecutar la primera campaña de phishing simulado.
    - Descripción: Lanzar una campaña de phishing controlado a todos los usuarios para establecer una métrica base (baseline) del nivel de riesgo inicial. Los resultados no serán punitivos, sino que servirán para medir la efectividad futura de las capacitaciones.
    - Responsable: Consultor de Concientización.
    - Duración estimada: 1 semana.

Carta Gantt

A continuación, se presenta la planificación temporal del proyecto a través de una carta Gantt. Esta herramienta de gestión entrega una perspectiva clara de la secuencia lógica del desarrollo:

Tabla 6: Tareas y fechas Carta Gantt

ITEM	Nombre de tarea	Duración	Comienzo	Fin
	PROPUESTA DE PLATAFORMA DE SEGURIDAD DE CORREO ELECTRÓNICO CON COMPONENTE DE CONCIENTIZACIÓN PARA EMPRESAS DEL RUBRO INMOBILIARIO EN ÁREA DE VENTAS	**73 días**	**lun 14-07-25**	**mié 22-10-25**
1	**Fase 1: Constitución del Proyecto y Planificación Inicial**	**8 días**	**lun 14-07-25**	**mié 23-07-25**
1.1	Oficializar y conformar el equipo de trabajo	2 días	lun 14-07-25	mar 15-07-25
1.2	Realizar la reunión de lanzamiento (kick-off)	1 día	mié 16-07-25	mié 16-07-25
1.3	Desarrollar el Plan de Gestión del Proyecto	1 sem	jue 17-07-25	mié 23-07-25
1.4	Definir los Indicadores Clave de Rendimiento (KPIs)	3 días	lun 21-07-25	mié 23-07-25
2	**Fase 2: Investigación, Evaluación y Selección de Herramientas**	**20 días**	**jue 24-07-25**	**mié 20-08-25**
2.1	Realizar un levantamiento detallado de la infraestructura de TI	1 sem	jue 24-07-25	mié 30-07-25
2.2	Investigar y evaluar soluciones de seguridad	2 sem.	jue 31-07-25	mié 13-08-25
2.3	Investigar y seleccionar plataforma de concientización	2 sem.	jue 31-07-25	mié 13-08-25
2.4	Seleccionar al proveedor y gestionar la adquisición	1 sem	jue 14-08-25	mié 20-08-25
3	**Fase 3: Diseño Detallado de la Solución**	**25 días**	**jue 21-08-25**	**mié 24-09-25**
3.1	Diseñar la arquitectura técnica y el plan de integración	1 sem	jue 21-08-25	mié 27-08-25
3.2	Diseñar las políticas de seguridad en la plataforma	2 sem.	jue 28-08-25	mié 10-09-25
3.3	Diseñar el contenido del programa de concientización	3 sem.	jue 21-08-25	mié 10-09-25
3.4	Desarrollar el Plan de Pruebas de calidad (QA)	2 sem.	jue 11-09-25	mié 24-09-25
3.5	Planificar la comunicación y gestión del cambio	1 sem	jue 11-09-25	mié 17-09-25
4	**Fase 4: Configuración y Pruebas en Entorno Controlado**	**17 días**	**jue 18-09-25**	**vie 10-10-25**
4.1	Habilitar y configurar el entorno de pruebas (Staging)	3 días	jue 18-09-25	lun 22-09-25
4.2	Instalar y configurar la plataforma en pruebas	1 sem	mar 23-09-25	lun 29-09-25
4.3	Ejecutar el plan de pruebas de calidad (QA)	1 sem	mar 30-09-25	lun 06-10-25
4.4	Documentar y resolver las incidencias detectadas	3 días	mar 07-10-25	jue 09-10-25
4.5	Obtener la aprobación formal de QA	1 día	vie 10-10-25	vie 10-10-25
5	**Fase 5: Despliegue en Producción y Lanzamiento**	**8 días**	**lun 13-10-25**	**mié 22-10-25**
5.1	Comunicar oficialmente el inicio del despliegue	1 día	lun 13-10-25	lun 13-10-25
5.2	Ejecutar el despliegue técnico en producción	2 días	mar 14-10-25	mié 15-10-25
5.3	Realizar monitoreo intensivo post-implementación	1 sem	jue 16-10-25	mié 22-10-25
5.4	Lanzar el programa de concientización a la empresa	2 días	mar 14-10-25	mié 15-10-25
5.5	Ejecutar la primera campaña de phishing simulado	1 sem	jue 16-10-25	mié 22-10-25

Fuente: Elaboración propia con datos obtenidos de ContruPro.

4.2.2 Do (hacer)

Concluida la fase de 'Planificar', en la cual se establecieron los cimientos estratégicos y el diseño detallado de la solución, se inicia la etapa de 'Hacer' del Ciclo de Deming. Esta fase se centra en la ejecución material de las tareas definidas, llevando a cabo la implementación controlada del plan de acción para transformar los componentes teóricos en una solución funcional y operativa.

El objetivo principal es materializar la propuesta de mejora mediante la correcta realización de las actividades planificadas. Esto contempla la implementación de la plataforma de seguridad en un entorno de pruebas, la ejecución de un plan de calidad exhaustivo y el posterior despliegue en el ambiente productivo. Para minimizar los riesgos y asegurar una transición fluida, se considera la ejecución de una prueba piloto con un grupo de usuarios representativo, lo que permitirá validar el funcionamiento y realizar ajustes antes de su implementación a gran escala. Esta etapa es fundamental para asegurar que la solución implementada sea robusta, segura y se alinee con los requerimientos definidos en la planificación.

4.2.2.1 Fase 1: “Constitución del Proyecto y Planificación Inicial”

- **Tarea 1.1:** Oficializar y conformar el equipo de trabajo del proyecto.

  Para garantizar el éxito en la implementación de la propuesta de mejora, es fundamental conformar un equipo de trabajo multidisciplinario con roles y responsabilidades claramente definidos. La naturaleza de la solución, que integra un componente tecnológico robusto con una estrategia de fortalecimiento del factor humano, exige la colaboración de perfiles que cubran desde la gestión del proyecto hasta la ejecución técnica, el aseguramiento de la calidad y el soporte operativo interno. A continuación, se detalla la estructura del equipo de cinco roles requerido, describiendo el perfil profesional y las funciones específicas que cada integrante desempeñará.

Jefe de Proyecto:

- **Descripción del cargo:** Profesional responsable de la planificación, ejecución, supervisión y cierre del proyecto. Actúa como el principal punto de comunicación entre el equipo de trabajo, los proveedores de tecnología y la gerencia de la empresa, asegurando que el proyecto se complete a tiempo, dentro del presupuesto y cumpliendo los objetivos establecidos.
- **Perfil profesional:**
    - **Profesión:** Ingeniero Informático, Ingeniero Industrial o Ingeniero Comercial.
    - **Grados académicos:** Título profesional. Deseable postítulo en Gestión de Proyectos.
    - **Certificaciones:** Se valora positivamente contar con certificaciones en gestión de proyectos como Project Management Professional o similar.
    - **Experiencia:** Mínimo de 5 años de experiencia liderando proyectos de implementación tecnológica, preferentemente en el ámbito de la ciberseguridad.
- **Rol en el proyecto:**
    - Definir el alcance, los objetivos y los entregables del proyecto en conjunto con la gerencia.
    - Desarrollar y gestionar el cronograma, el presupuesto y la asignación de recursos.
    - Coordinar las actividades del equipo de trabajo y supervisar el cumplimiento de las tareas.
    - Gestionar la relación con proveedores externos para la adquisición de la plataforma de seguridad.

- Informar periódicamente a la gerencia sobre los avances, riesgos y desviaciones del proyecto.

Especialista en Ciberseguridad

- **Descripción del cargo:** Experto técnico encargado de la arquitectura, implementación, configuración y mantenimiento de la plataforma de seguridad de correo electrónico. Es el responsable de asegurar que la solución tecnológica funcione de manera óptima y se integre correctamente con la infraestructura existente de la empresa.
- **Perfil profesional:**
  - **Profesión:** Ingeniero en Ciberseguridad y Auditoría Informática, Ingeniero en Conectividad y Redes o afín.
  - **Grados académicos:** Título de Ingeniero en Ciberseguridad o carrera equivalente.
  - **Certificaciones:** Certificaciones técnicas en seguridad de redes (ej. CompTIA Security+, CISSP) y en plataformas de seguridad de correo (ej. de Proofpoint, Mimecast) son altamente deseables.
  - **Experiencia:** Al menos 3 años de experiencia práctica en la administración de soluciones de seguridad perimetral, específicamente en firewalls, filtros antispam y plataformas de protección contra phishing y malware.
- **Rol en el proyecto:**
  - Investigar y evaluar las distintas soluciones de seguridad de correo electrónico del mercado para seleccionar la más adecuada.
  - Liderar el proceso de implementación técnica y configuración de la plataforma seleccionada.
  - Definir y aplicar las políticas de seguridad para la detección de phishing, suplantación de identidad y malware.

- Establecer los procedimientos de monitoreo, gestión de alertas y respuesta ante incidentes detectados por la plataforma.
- Colaborar con el Consultor de Concientización, proporcionando datos sobre amenazas bloqueadas para ser usados en las capacitaciones.

Analista de Infraestructura TI

- **Descripción del cargo:** Profesional del equipo de TI interno de la empresa, responsable de dar soporte en la integración de la nueva plataforma de seguridad con la infraestructura tecnológica existente. Actúa como contraparte técnica interna y punto de contacto para el Especialista en Ciberseguridad.
- **Perfil profesional:**
  - **Profesión:** Ingeniero o Técnico en Informática, Administrador de Sistemas.
  - **Grados académicos:** Título técnico o profesional en áreas de TI.
  - **Certificaciones:** Deseables certificaciones en administración de plataformas de correo (ej. Microsoft 365) o redes.
  - **Experiencia:** Mínimo de 2 años de experiencia en la administración de la infraestructura de TI de la empresa, incluyendo el servicio de correo, DNS y gestión de usuarios.
- **Rol en el proyecto:**
  - Proveer la información necesaria sobre la infraestructura actual para asegurar la compatibilidad.
  - Colaborar activamente durante la fase de integración y realizar las configuraciones requeridas en los sistemas internos.
  - Participar en las pruebas técnicas y de aceptación del usuario.

- Ser el receptor de la transferencia de conocimiento para el soporte de primer nivel post-implementación.

Analista de Calidad (QA)

- **Descripción del cargo:** Profesional técnico responsable de asegurar la calidad y el correcto funcionamiento de la solución. Su función es diseñar y ejecutar un plan de pruebas exhaustivo para validar que la plataforma cumple con los requisitos funcionales y de seguridad, y no impacta negativamente la operatoria del negocio, evitando, por ejemplo, el bloqueo de correos legítimos.
- **Perfil profesional:**
  - **Profesión:** Ingeniero en Informática, Analista de Sistemas o carrera afín con especialización en calidad de software.
  - **Grados académicos:** Título técnico o profesional en áreas de TI.
  - **Certificaciones:** Se valoran certificaciones en testing de software como ISTQB (International Software Testing Qualifications Board).
  - **Experiencia:** Mínimo 3 años de experiencia en roles de aseguramiento de calidad (QA), preferentemente probando soluciones de software empresariales.
- **Rol en el proyecto:**
  - Diseñar el plan de pruebas, incluyendo casos de prueba para escenarios de ataque y de uso normal del correo.
  - Ejecutar pruebas funcionales para verificar que las políticas de seguridad se aplican correctamente.
  - Identificar, documentar y reportar defectos (bugs), con especial foco en la detección de falsos positivos.
  - Validar que la solución no interrumpe el flujo de trabajo de las áreas de negocio.

- Emitir un informe de calidad y dar el visto bueno para el paso a producción.

Consultor de Concientización

- **Descripción del cargo:** Especialista en el factor humano, responsable de diseñar e implementar el programa de concientización y capacitación. Su objetivo es educar al personal para reducir el riesgo asociado a errores humanos, como caer en ataques de phishing.
- **Perfil profesional:**
  - **Profesión:** Psicólogo Organizacional, Comunicador Social, o profesional de TI con especialización en capacitación.
  - **Grados académicos:** Título profesional. Deseable postítulo en comunicación estratégica o desarrollo organizacional.
  - **Certificaciones:** No excluyentes, pero se valora experiencia comprobable.
  - **Experiencia:** Mínimo de 3 años de experiencia en el diseño y ejecución de programas de capacitación corporativa, idealmente en ciberseguridad.
- **Rol en el proyecto:**
  - Diseñar el plan y los materiales del programa de concientización.
  - Ejecutar campañas de phishing simulado para medir la resiliencia de los empleados.
  - Utilizar incidentes reales (bloqueados por la plataforma) para crear capacitaciones relevantes y de alto impacto.
  - Medir la efectividad del programa y fomentar una cultura de seguridad.

la conformación de este equipo de cinco roles asegura que la propuesta se aborde desde una perspectiva integral y robusta. La estructura garantiza la gestión táctica (Jefe de Proyecto), la excelencia en la implementación (Especialista en Ciberseguridad), la viabilidad operativa (Analista de Infraestructura TI), la validación funcional (Analista de Calidad) y el fortalecimiento del eslabón humano (Consultor de Concientización). Esta sinergia es crucial para lograr una implementación exitosa y una mejora sostenible en la postura de seguridad de la empresa.

- **Tarea 1.2: Realizar la reunión de lanzamiento del proyecto (kick-off).**

La reunión de lanzamiento o kick-off marca el inicio formal del proyecto. Su propósito es alinear al equipo de trabajo completo, junto con los principales interesados y la gerencia, sobre los elementos fundamentales que guiarán la ejecución del plan. Durante esta sesión, el jefe de Proyecto presenta la visión general, asegurando que cada miembro comprenda su rol y cómo su contribución se integra en el objetivo global.

Los puntos clave a tratar en esta reunión son:

- Presentación de los miembros del equipo: Formalizar la presentación de cada uno de los roles definidos en la Tarea 1.1 y sus responsabilidades específicas.
- Revisión del alcance y objetivos**:** Exponer en detalle el alcance, los objetivos generales y específicos del proyecto, y los entregables esperados para evitar desviaciones futuras.
- Presentación del presupuesto y cronograma**:** Comunicar el presupuesto asignado y revisar el cronograma maestro, destacando los hitos más importantes.
- Definición de canales de comunicación: Establecer los protocolos y herramientas de comunicación que se utilizarán para el seguimiento de tareas, la notificación de avances y la gestión de incidencias.

- Alineación de expectativas**:** Crear un espacio para que los miembros del equipo y los stakeholders puedan resolver dudas, asegurando un entendimiento común desde el comienzo.

- **Tarea 1.3: Desarrollar el Plan de Gestión del Proyecto**

  Una vez realizado el lanzamiento, el Jefe de Proyecto es responsable de elaborar el Plan de Gestión del Proyecto. Este documento es la hoja de ruta formal que detalla cómo se ejecutará, monitoreará y controlará el proyecto desde su inicio hasta su cierre. Su finalidad es centralizar toda la información crítica para la toma de decisiones y la gestión proactiva de los recursos. Este plan se compone de varios documentos subsidiarios clave:

  - **Cronograma Maestro:** Documento que detalla todas las fases, tareas, dependencias y duraciones estimadas. Se utiliza una carta Gantt para visualizar la línea de tiempo del proyecto, asignar recursos a cada actividad y monitorear el progreso con respecto a los plazos establecidos, Para comprender el formato esperado se puede visualizar en el Anexo 1: “Formato cronograma maestro”
  - **Presupuesto Detallado:** Desglose exhaustivo de todos los costos asociados al proyecto, incluyendo la adquisición de licencias para las plataformas de seguridad y concientización, los honorarios del equipo de trabajo y cualquier otro gasto operativo. Este documento es esencial para el control financiero.
  - **Plan de Gestión de Riesgos:** Identifica los posibles riesgos que podrían afectar al proyecto (técnicos, operativos, de presupuesto, de plazos, o de resistencia al cambio por parte de los usuarios). Para cada riesgo, se evalúa su probabilidad e impacto y se definen estrategias de mitigación o planes de contingencia.
  - **Plan de Comunicaciones:** Define cómo, cuándo y a quién se reportará la información relevante del proyecto. Especifica la frecuencia y el formato de los informes de avance para la gerencia, las reuniones de seguimiento del equipo y las comunicaciones generales a la organización para gestionar el cambio.

- **Tarea 1.4: Definir los Indicadores Clave de Rendimiento (KPIs) del proyecto.**

  Para medir de forma objetiva el éxito del proyecto y el impacto real de la solución implementada, es imprescindible definir Indicadores Clave de Rendimiento (KPIs) desde la fase de planificación. Estas métricas cuantitativas permitirán evaluar la efectividad tanto de la herramienta tecnológica como del programa de concientización, y serán la base para la fase de "Verificar" del Ciclo de Deming. Los indicadores definidos para este proyecto incluyen:

  - **Tasa de reducción de incidentes de phishing reportados:** Mide la disminución porcentual de correos maliciosos que llegan a los usuarios y son reportados por ellos, después de la implementación de la plataforma. Este KPI evalúa directamente la eficacia del filtro de seguridad.
  - **Porcentaje de mejora en las campañas de simulación:** Compara los resultados de la primera campaña de phishing simulado (línea base) con los de campañas posteriores. Un menor porcentaje de clics en enlaces maliciosos o de envío de credenciales indicará una mejora en la concientización del personal.
  - **Tasa de reportes de amenazas:** Mide el porcentaje de usuarios que reportan activamente un correo sospechoso utilizando las herramientas proporcionadas. Un aumento en esta tasa refleja una mayor cultura de seguridad y compromiso por parte de los empleados.
  - **Reducción de falsos positivos:** Cuantifica la cantidad de correos electrónicos legítimos que son incorrectamente clasificados como maliciosos por la plataforma. Un KPI clave para asegurar que la solución no interfiere con la continuidad del negocio

4.2.2.2 Fase 2: “Investigación, Evaluación y Selección de Herramientas”

- **Tarea 2.1: Realizar un levantamiento detallado de la infraestructura de TI actual**

  Antes de evaluar cualquier solución externa, es esencial contar con un conocimiento exhaustivo del entorno tecnológico existente en la empresa. Esta tarea consiste en documentar en detalle la configuración del servicio de correo electrónico, la gestión de los registros DNS, los sistemas de administración de usuarios y cualquier otro componente tecnológico relevante. El objetivo es asegurar la compatibilidad técnica de la futura plataforma y planificar una integración sin contratiempos.

  El levantamiento, a cargo del Analista de Infraestructura TI, debe documentar los siguientes aspectos:

  - **Servicio de correo actual:** Proveedor (ej. Microsoft 365, Google Workspace), licenciamiento y configuración.
  - **Configuración de dominios y DNS:** Un análisis de los registros MX (Mail Exchange), SPF (Sender Policy Framework), DKIM (DomainKeys Identified Mail) y DMARC (Domain-based Message Authentication, Reporting, and Conformance) para entender el flujo de correo actual y los controles de autenticación existentes.
  - **Gestión de identidades:** Sistema utilizado para la administración de usuarios y grupos (ej. Active Directory, Azure AD).
  - **Sistemas de seguridad perimetral existentes:** Firewalls, filtros antispam actuales u otras herramientas que puedan interferir o deban Claro, aquí está el levantamiento de la infraestructura TI on-premise en formato de listado:

  A continuación, se presenta el desglose de la infraestructura tecnológica actual de la empresa, conforme a la Tarea 2.1 del plan de proyecto.

Infraestructura General y Servidores

- Ubicación: Rack de servidores centralizado en las oficinas de Lampa.
- Equipos: Dos servidores físicos principales.
- Virtualización: Se utiliza la tecnología Hyper-V para la gestión de máquinas virtuales.

Distribución de Cargas:

- Servidor 1 (Principal): Aloja las máquinas virtuales del Controlador de Dominio y del sistema ERP.
- Servidor 2 (Comunicaciones): Aloja una máquina virtual dedicada exclusivamente al servidor de correo electrónico.

Servicio de Correo Actual (On-Premise)

- Software: Microsoft Exchange Server 2019 (Standard Edition).
- Configuración: Implementación de servidor único que gestiona todos los buzones del dominio corporativo contrupro.cl.
- Protección Actual: Las funciones anti-malware y anti-spam son las que vienen integradas por defecto en Exchange. Estas se consideran insuficientes para combatir amenazas como el phishing dirigido y la suplantación de identidad.

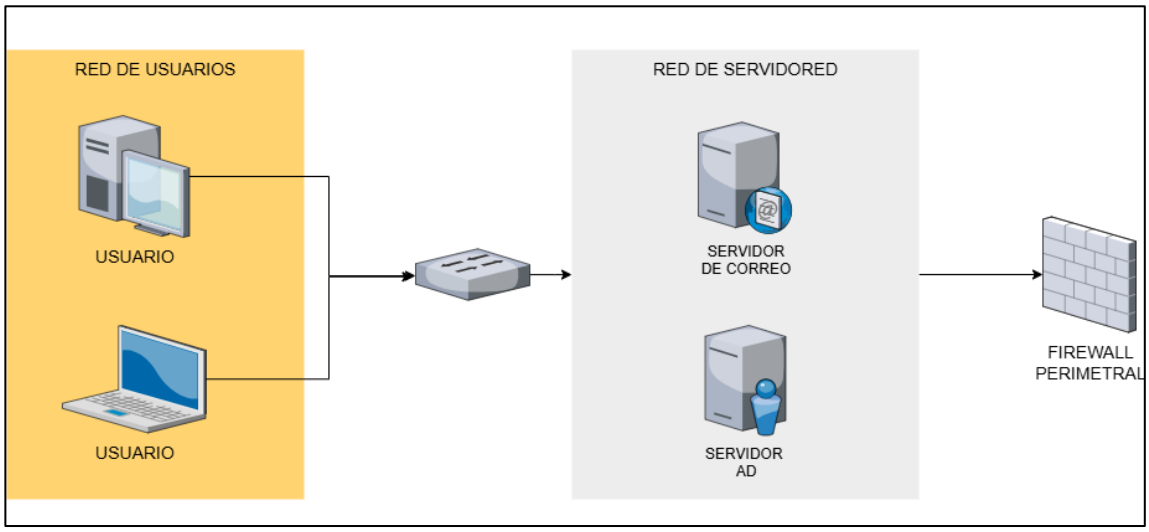
Gestión de Dominios y DNS

- DNS Interno: Rol de DNS de Windows Server para la resolución de nombres de la red local.
- DNS Externo: Los registros públicos del dominio se administran a través de NIC.

Estado de Registros de Seguridad:

- Registro MX: Apunta directamente a la dirección IP pública del firewall de la empresa.
- Registro SPF: Existe un registro, pero su configuración es básica, autorizando únicamente la IP del servidor Exchange.
- Registros DKIM y DMARC: No se encuentran implementados. Esta ausencia representa una vulnerabilidad crítica que facilita los ataques de suplantación de identidad.

Figura 9: Diagrama de red



Fuente: Elaboración propia con datos obtenidos de ContruPro.

- **Tarea 2.2: Investigar y evaluar soluciones de seguridad de correo electrónico del mercado**

  Con la información del levantamiento técnico, el Especialista en Ciberseguridad lidera la investigación de las plataformas de seguridad de correo electrónico. El plan exige el análisis de un mínimo de tres soluciones comerciales líderes en el sector. La evaluación no se limita a las características del producto, sino que considera un conjunto de

criterios para asegurar una elección informada y alineada con las necesidades de la empresa.

Los criterios de evaluación son:

- **Eficacia en la detección de amenazas:** Capacidad para bloquear phishing, suplantación de identidad, malware y otras amenazas avanzadas.
- **Facilidad de integración:** Compatibilidad con la infraestructura de TI documentada en la tarea anterior.
- **Modelo de licenciamiento:** Análisis de costos, estructura de precios (por usuario, por volumen) y escalabilidad.
- **Soporte técnico:** Calidad y disponibilidad del soporte ofrecido por el proveedor.

- **Tarea 2.3: Investigar y seleccionar una plataforma para la gestión de concientización**

  El propósito es encontrar una herramienta que permita administrar eficazmente los módulos de capacitación y ejecutar campañas de phishing simulado para medir y mejorar la resiliencia de los empleados ante ataques de ingeniería social.

  Los criterios para la selección de esta plataforma incluyen:

  - **Calidad y variedad del contenido de capacitación:** Disponibilidad de módulos interactivos, videos y material de apoyo en español.
  - **Capacidad de simulación de phishing:** Variedad y personalización de las plantillas de phishing, y capacidad para segmentar campañas por áreas o roles.
  - **Sistema de reportería:** Habilidad para generar métricas detalladas que se alineen con los KPIs definidos (ej. tasa de clics, tasa de reportes).

- **Facilidad de uso:** Interfaz intuitiva tanto para los administradores del programa como para los empleados.

- **Tarea 2.4: Seleccionar al proveedor y gestionar la adquisición.**

  Esta tarea consolida los resultados de las investigaciones anteriores. El Jefe de Proyecto y el Especialista en Ciberseguridad presentan un informe comparativo a la gerencia, el cual incluye la recomendación final tanto para la plataforma de seguridad como para la de concientización. Dicho informe debe justificar la elección basándose en el análisis técnico, funcional y de costos realizado.

  Una vez que la gerencia aprueba la recomendación, el Jefe de Proyecto procede con la gestión formal de la compra. Este proceso incluye la negociación de los términos del contrato con los proveedores seleccionados, la tramitación de las órdenes de compra y la adquisición final de las licencias y/o suscripciones a los servicios. Con esta tarea se concluye la fase de selección y se obtienen los recursos tecnológicos necesarios para iniciar la fase de diseño detallado e implementación.

  Selección de la Plataforma

  Tras un riguroso proceso de evaluación de las soluciones de mercado (Tarea 2.2) y considerando la infraestructura on-premise de la empresa, se ha determinado seleccionar a Proofpoint como proveedor de la plataforma de seguridad de correo electrónico. Específicamente, se opta por su solución en la nube, la cual se integra redirigiendo el flujo de correo a través de un cambio en los registros MX, sin necesidad de instalar hardware o software adicional en los servidores de ContruPro.

  La elección de Proofpoint se fundamenta en los siguientes puntos clave:

  - Eficacia contra Amenazas Críticas: La plataforma es reconocida por su alta efectividad en la detección y bloqueo de las amenazas más críticas para la empresa, como la suplantación de identidad para el desvío de

fondos, el phishing dirigido y la recepción de comprobantes de pago falsificados.

- Componente de Concientización Integrado: La solución de Proofpoint incluye un robusto módulo de concientización y simulación de ataques, cumpliendo con el requisito de abordar el factor humano y la falta de capacitación formal identificada como una causa raíz del problema. Esto permite consolidar la compra en un único proveedor.
- Facilidad de Integración: Al ser una solución en la nube, se simplifica enormemente la integración con la infraestructura on-premise existente. La implementación no interfiere con el servidor Microsoft Exchange actual, sino que actúa como una capa de filtrado previa, lo que minimiza los riesgos y la complejidad del despliegue técnico.

4.2.2.3 Fase 3: "Diseño Detallado de la Solución"

- **Tarea 3.1: Diseñar la arquitectura técnica y el plan de integración**

  Esta tarea consiste en crear el plano técnico que especifica cómo la nueva plataforma de seguridad se integrará con la infraestructura de correo electrónico existente de la empresa. El Especialista en Ciberseguridad y el Analista de Infraestructura TI colaboran para desarrollar un diseño que garantice un flujo de correo seguro y eficiente, minimizando el impacto en la operación diaria del negocio.

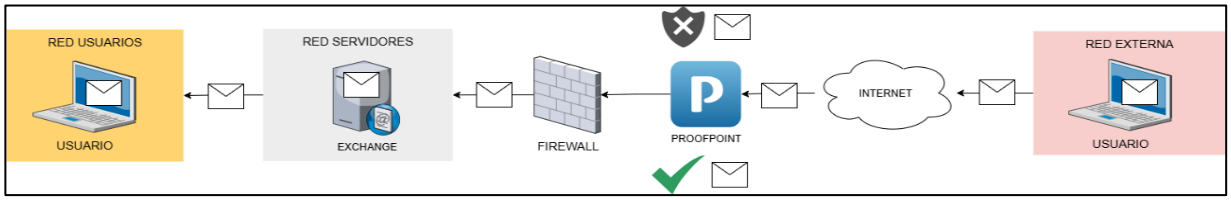
  Los entregables claves de esta tarea son:

  - **Diagrama de flujo de correo futuro:** Un diagrama detallado que ilustra cómo se redirigirá el tráfico de correo electrónico (entrante y saliente) para ser analizado por la nueva plataforma de seguridad antes de ser entregado a los destinatarios.

Flujo de Correo Entrante:

- El correo electrónico enviado a un empleado de ContruPro es dirigido primero a los servidores de Proofpoint, ya que el Registro MX del dominio apuntará a ellos.
- Proofpoint aplica su motor de análisis avanzado para detectar phishing, malware, suplantación de identidad y otras amenazas. Además, realiza las verificaciones de SPF, DKIM y DMARC.
- Solo los correos considerados seguros son reenviados a través de Internet hacia la dirección IP del firewall de ContruPro.
- El firewall recibe el correo limpio y lo entrega al servidor Microsoft Exchange, que finalmente lo deposita en el buzón del usuario.

Figura 10: Flujo de correo entrante

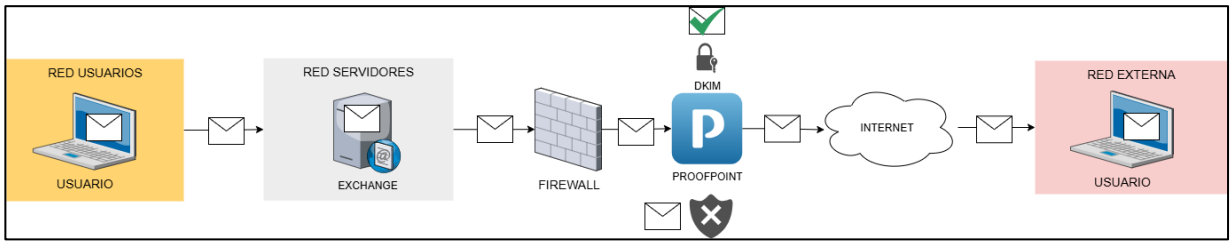


Fuente: Elaboración propia con datos obtenidos de ContruPro.

Flujo de Correo Saliente:

- El correo enviado por un empleado es procesado por el servidor Exchange.
- El servidor Exchange se configura para enrutar todo el correo saliente hacia los servidores de Proofpoint (usando un conector de envío).
- Proofpoint recibe el correo, lo firma con DKIM para autenticarlo, lo analiza en busca de contenido malicioso o fuga de datos, y lo envía a su destinatario final en Internet. Esto mejora significativamente la reputación de envío del dominio.

Figura 11: Flujo de correo saliente



Fuente: Elaboración propia con datos obtenidos de ContruPro.

- **Plan de acción para la integración:** Un documento paso a paso que describe las configuraciones técnicas necesarias para la puesta en marcha. Este plan está diseñado para ejecutarse de manera controlada y, preferiblemente, en horarios de bajo impacto para no interrumpir la continuidad del negocio.

  Plan de integración:

  Este plan desglosa el proceso de integración en tres fases principales: Preparación, Implementación Técnica - Activación y Monitoreo.

  Fase 1: Preparación y Configuración Inicial.

  El objetivo de esta fase es configurar todas las plataformas y preparar el entorno sin afectar el flujo de correo actual.

  Paso 1: Configuración del Portal de Proofpoint

  - Verificación de Dominio: Acceder al portal de administración de Proofpoint y añadir el dominio contrupro.cl. Se completará el proceso de verificación de propiedad del dominio, generalmente mediante la adición de un registro TXT específico en el DNS público.
  - Sincronización de Usuarios: Configurar la herramienta de sincronización de Active Directory (si está disponible) o importar un archivo CSV con todos los usuarios de correo electrónico. El objetivo es que Proofpoint tenga una lista completa de los buzones válidos para prevenir ataques de recolección de directorios.

- Definición de Políticas Base: Crear las políticas iniciales de seguridad. Esto incluye:
  - Configurar los niveles de agresividad del filtro anti-spam y anti-malware.
  - Activar las reglas de protección contra suplantación de identidad y ataques de phishing.
  - Configurar las notificaciones de cuarentena para los usuarios.

Paso 2: Preparación del Entorno On-Premise.

- Creación de Reglas de Firewall: Crear una nueva regla en el firewall de ContruPro que permita el tráfico SMTP (puerto 25) exclusivamente desde los rangos de direcciones IP públicas de Proofpoint.
- Configuración del Conector de Salida en Exchange: En el Centro de Administración de Exchange, configurar un nuevo "Conector de Envío". Este conector se configurará para enrutar todo el correo saliente a través de un smart host, que será la dirección proporcionada por Proofpoint.

Fase 2: Implementación Técnica y Pruebas

En esta fase se realizan pruebas controladas para asegurar que la configuración es correcta.

Paso 3: Pruebas de Flujo Saliente

- Verificación de Envío: Enviar correos de prueba a cuentas externas (Gmail, Outlook, etc.) y verificar los encabezados de los correos recibidos para confirmar que fueron enrutados a través de Proofpoint y que la firma DKIM está siendo aplicada correctamente.

- Monitoreo de Registros: Revisar los registros de correo saliente en el portal de Proofpoint para asegurar que el flujo es normal y no hay correos legítimos siendo bloqueados.

Paso 4: Pruebas de Flujo Entrante.

- Envío de Correos de Prueba**:** Enviar correos de prueba (limpios y con malware/phishing de prueba) a una dirección en el host de prueba y verificar que Proofpoint los procesa correctamente, bloqueando las amenazas y entregando los correos seguros.

Fase 3: Activación, Monitoreo y Cierre

Esta es la fase final, donde se redirige todo el flujo de correo entrante.

Paso 5: Ventana de Cambio.

- Reducción de TTL del DNS: Unas 24 horas antes del cambio, reducir el TTL (Time To Live) del registro MX actual a un valor bajo (ej. 300 segundos o 5 minutos). Esto asegurará que el cambio de DNS se propague rápidamente.
- Cambio del Registro MX: En el portal del registrador de DNS, modificar el registro MX del dominio contrupro.cl para que apunte a las direcciones proporcionadas por Proofpoint.

Paso 6: Monitoreo Post-Implementación

- Verificación Intensiva: Durante las primeras 24 horas, el equipo técnico debe monitorear activamente la consola de Proofpoint y los registros del servidor Exchange para detectar cualquier anomalía en el flujo de correo.
- Soporte a Usuarios: Estar preparado para atender consultas de usuarios sobre correos en cuarentena o cualquier otro comportamiento inesperado.

- Plan de Rollback: En caso de un fallo crítico, el plan de contingencia consiste en revertir el cambio del registro MX a su valor original y desactivar la nueva regla de firewall.

- **Tarea 3.2: Diseñar la arquitectura técnica y el plan de integración**

  Bajo la responsabilidad del Especialista en Ciberseguridad, esta tarea se enfoca en traducir los riesgos identificados en el análisis de la situación actual en reglas y políticas de seguridad concretas. El objetivo es configurar la plataforma para que sea capaz de detectar y neutralizar las amenazas más críticas para la organización, como el phishing, la suplantación de identidad y el malware. Se definen y documentan reglas específicas, umbrales de sensibilidad y acciones automáticas (ej. cuarentena, bloqueo, notificación) que la plataforma ejecutará al identificar una amenaza, asegurando una protección adaptada al perfil de riesgo de la empresa

- **Tarea 3.3: Diseñar el contenido y materiales del programa de concientización.**

  El Consultor de Concientización lidera el diseño de todos los recursos educativos que formarán parte del programa de formación para empleados. El fin es crear un programa de alto impacto, relevante y fácil de asimilar que fortalezca el factor humano como una capa de defensa. Para maximizar su efectividad, se utilizarán ejemplos de incidentes reales que hayan sido bloqueados por la plataforma de seguridad, haciendo los riesgos más tangibles para el personal.

  Los materiales por desarrollar incluyen:

  - Módulos de capacitación interactivos: cursos en línea breves, de 15 a 20 minutos, que forman la base de la educación formal. Su propósito es enseñar sobre riesgos clave como el phishing y la suplantación de identidad, utilizando ejemplos de ataques reales

bloqueados por la plataforma para ilustrar las tácticas de los ciberdelincuentes.

- Guías rápidas e infografías con consejos prácticos: archivos en formato PDF de una sola página con un formato limpio y profesional. La guía será muy visual, con iconos y poco texto, estructurada como una lista de verificación o un flujograma simple. Está pensada para que el usuario la imprima y la pegue en su espacio de trabajo o la guarde en su escritorio como un archivo de acceso directo para una consulta inmediata.
- Videos educativos breves: video corto (2-3 minutos) en alta definición (MP4). Podrá reproducirlo directamente en su navegador. La experiencia será similar a ver un video de YouTube, con animaciones dinámicas o una grabación de pantalla clara que muestra un proceso paso a paso. Los videos incluirán una narración clara y subtítulos para facilitar su comprensión, permitiendo al usuario consumirlo con o sin audio.

- **Tarea 3.4: Diseñar el contenido y materiales del programa de concientización.**

  El Analista de Calidad (QA) es el responsable de elaborar un documento de pruebas exhaustivo que permita validar la solución antes de su despliegue en el entorno productivo. Este plan es fundamental para asegurar que la plataforma funciona según lo esperado, protege eficazmente a la empresa y no introduce problemas operativos.

  El plan de pruebas debe incluir un conjunto detallado de casos de prueba que cubran, como mínimo, los siguientes escenarios:

  - **Validación de detección de amenazas:** Simulación de recepción de correos con phishing, malware y características de suplantación de identidad para verificar que son bloqueados correctamente.

- **Identificación de falsos positivos:** Envío de correos electrónicos legítimos de diversa índole (con archivos adjuntos, enlaces, etc.) para asegurar que no sean clasificados incorrectamente como amenaza.
- **Verificación del flujo normal de correo:** Confirmación de que el proceso de envío y recepción de correos legítimos no sufre retrasos ni impedimentos

- **Tarea 3.5: Diseñar el plan de pruebas de calidad (QA).**

  Reconociendo que la implementación de nuevas tecnologías y procesos puede generar resistencia, esta tarea se centra en preparar a la organización para el cambio. El jefe de Proyecto y el Consultor de Concientización colaboran para diseñar una estrategia de comunicación que facilite una adopción exitosa por parte de todos los empleados. El plan busca informar de manera clara y oportuna, gestionar las expectativas y minimizar la incertidumbre. Las acciones incluyen la preparación de comunicados oficiales, la definición de una agenda de socialización y la creación de recursos de apoyo para los usuarios finales.

4.2.2.4 Fase 4: “Configuración y Pruebas en Entorno Controlado”

Tarea 4.1: Habilitar y configurar el entorno de pruebas

La primera acción de esta fase es la creación de un ambiente técnico aislado que replique fielmente las condiciones del sistema de correo electrónico de producción de la empresa. Esta tarea, bajo la responsabilidad del Analista de Infraestructura TI, es crucial para poder realizar pruebas exhaustivas sin afectar la operatividad del negocio. Este entorno controlado servirá como el campo de pruebas para la instalación, configuración y validación de la nueva plataforma de seguridad.

Tarea 4.2: Instalar y configurar la plataforma de seguridad en el entorno de pruebas

Con el entorno de pruebas ya habilitado, el Especialista en Ciberseguridad procede con el despliegue inicial de la solución de seguridad. En esta etapa se instala el software y se aplican las políticas de protección (anti-phishing, anti-malware, etc.) que fueron documentadas en la fase de diseño. El objetivo es configurar la plataforma en el ambiente de pruebas de la misma manera en que se planea hacerlo en producción, para que los resultados de las pruebas sean representativos.

Tarea 4.3: Ejecutar el plan de pruebas de calidad (QA)

El Analista de Calidad (QA) lidera la ejecución del plan de pruebas que fue diseñado en la fase anterior. Se ejecutan de manera sistemática todos los casos de prueba definidos para validar el correcto funcionamiento de la plataforma. Las pruebas se centran en verificar que la solución detecta y bloquea eficazmente las amenazas simuladas y, de igual importancia, que no interfiere con el flujo de correos legítimos, evitando la generación de falsos positivos.

Tarea 4.4: Documentar y resolver las incidencias detectadas

Esta tarea se ejecuta en paralelo con la ejecución de las pruebas. Cualquier defecto, error o comportamiento inesperado que se identifique durante el proceso de QA es registrado y documentado formalmente por el Analista de Calidad. Una vez documentada, la incidencia es asignada al Especialista en Ciberseguridad, quien se encarga de analizarla y aplicar las correcciones necesarias en la configuración de la plataforma. Este ciclo de detección y corrección se repite hasta que la solución alcance el nivel de estabilidad y calidad requerido.

Tarea 4.5: Obtener la aprobación formal de QA

Esta es la última tarea de la fase de pruebas y actúa como un punto de control de calidad antes de proceder al despliegue final. Una vez que todas las pruebas han sido ejecutadas satisfactoriamente y las incidencias críticas han sido resueltas, el Analista de Calidad emite un informe formal con los resultados obtenidos. Con base en este informe, se otorga la aprobación formal, certificando que la solución es estable, segura y está lista para ser implementada en el ambiente productivo de la empresa

4.2.2.5 Fase 5: "Despliegue en Producción y Lanzamiento"

Tarea 5.1: Comunicar oficialmente el inicio del despliegue

Antes de realizar cualquier cambio técnico en el entorno productivo, el Jefe de Proyecto es responsable de enviar una comunicación oficial a toda la organización. El objetivo de este comunicado es informar a todos los usuarios sobre la fecha y hora de la ventana de implementación para que estén al tanto de la intervención. Esta acción, enmarcada en el plan de gestión del cambio, es fundamental para manejar las expectativas y minimizar la incertidumbre entre los empleados.

Tarea 5.2: Ejecutar el despliegue técnico en producción

Esta es la tarea central de la fase, donde el Especialista en Ciberseguridad y el Analista de Infraestructura TI llevan a cabo la puesta en marcha de la solución. La ejecución consiste en realizar las configuraciones técnicas necesarias, como el cambio de los registros MX del DNS, para que todo el flujo de correo de la empresa sea procesado por la nueva plataforma de seguridad. Conforme al plan, esta actividad debe ser ejecutada en un horario de bajo impacto operativo para no afectar las actividades comerciales de la empresa.

Tarea 5.3: Realizar monitoreo post-implementación

Una vez completado el despliegue técnico, se inicia un período de supervisión activa. Durante los primeros días de funcionamiento, el Especialista en Ciberseguridad y el Analista de Infraestructura TI monitorean de cerca la plataforma para detectar y resolver de forma inmediata cualquier anomalía que pudiera presentarse. Este seguimiento intensivo es clave para asegurar la continuidad operativa y validar el correcto funcionamiento de la solución en un entorno real.

Tarea 5.4: Lanzar el programa de concientización a toda la empresa

De manera paralela a las actividades técnicas, el Consultor de Concientización ejecuta el lanzamiento del programa de formación. Esta tarea implica enviar una comunicación de bienvenida a todos los empleados, otorgarles acceso a los primeros módulos de capacitación y presentar formalmente los objetivos de la iniciativa. Este hito marca el comienzo del fortalecimiento del factor humano como pilar de la estrategia de ciberseguridad.

Tarea 5.5: Ejecutar la primera campaña de phishing simulado

Para finalizar la fase de implementación, el Consultor de Concientización lanza una primera campaña de phishing controlado dirigida a todos los usuarios. El propósito de esta campaña no es sancionador ni para buscar culpables, sino que para establecer una métrica base que refleje el nivel de riesgo inicial de la organización ante este tipo de ataques. Los resultados obtenidos en esta primera simulación serán el punto de referencia contra el cual se medirá la efectividad futura de las capacitaciones y la evolución de la cultura de seguridad en la empresa.

4.2.2.6 Aplicación del Marco NIST en la etapa Hacer

Durante la etapa Hacer del ciclo PDCA, la implementación de la solución se llevó a cabo bajo los lineamientos del Marco NIST de Ciberseguridad (CSF), de manera que cada acción ejecutada se alineara con las cinco funciones esenciales: **Identificar, Proteger, Detectar, Responder y Recuperar**. Esta integración permitió transformar la planificación estratégica en controles técnicos y organizacionales concretos, asegurando que la propuesta no solo se limitara al despliegue de la plataforma Proofpoint y del programa de concientización, sino que se adoptara una visión integral de ciberseguridad.

- **Identificar:** Se ejecutó el levantamiento de activos críticos asociados al correo electrónico, tales como buzones corporativos, registros DNS y flujos de comunicación comercial. Esta identificación permitió mapear riesgos como suplantación de identidad, fraude financiero y fuga de información, lo que fundamentó la configuración inicial de políticas en la plataforma de seguridad.
- **Proteger:** Se implementaron controles técnicos basados en Proofpoint, incluyendo políticas anti-phishing, verificación SPF/DKIM/DMARC y protección contra malware. A nivel organizacional, se desplegó el programa de concientización, con módulos de capacitación y campañas de phishing simulado, como medida de protección frente al error humano.
- **Detectar:** Se habilitó el monitoreo en tiempo real de eventos de correo electrónico y la generación de alertas automáticas ante intentos de suplantación o recepción de adjuntos maliciosos. Este componente fue complementado con la telemetría obtenida de las campañas de simulación, que permitió detectar debilidades conductuales en los usuarios.
- **Responder:** Se establecieron procedimientos iniciales de gestión de incidentes, apoyados en la función de cuarentena automática de la plataforma y en el flujo de reporte por parte de usuarios capacitados. De esta forma, la respuesta no dependió únicamente de controles técnicos,

sino también de la activación del **usuario como sensor** frente a amenazas no filtradas.

- **Recuperar:** Aunque la fase de recuperación completa excede el alcance del proyecto, en la etapa Hacer se consideraron medidas de continuidad básica, como la retención de correos en la nube de Proofpoint, la validación de respaldos y la documentación de incidentes detectados, generando las primeras lecciones aprendidas que alimentarán los próximos ciclos.

En conclusión, la aplicación del NIST CSF en la etapa Hacer garantizó que la ejecución no se redujera a un despliegue tecnológico aislado, sino que se consolidara como un modelo de defensa integral. La solución implementada quedó alineada con estándares internacionales, reduciendo la exposición de ContruPro a riesgos críticos y sentando las bases para una cultura de seguridad sostenible.

4.2.3 Check (Verificar)

En esta etapa del ciclo PDCA se evalúa si las acciones implementadas en el proyecto han cumplido con los objetivos definidos inicialmente, considerando tanto la mejora técnica (filtrado de correo) como los aspectos de concientización del personal. Esta verificación se realiza mediante herramientas de medición objetivas como KPIs, listas de chequeo, comparación de métricas pre y post implementación, y revisión documental. Para fortalecer la trazabilidad de los indicadores, además de definir fuente, frecuencia y responsables, se establece un baseline inicial y metas progresivas a alcanzar en intervalos de tiempo definidos. El propósito es identificar desviaciones, validar los logros y establecer una base para la mejora continua (fase “Act”).

Aspectos Verificados:

Evaluación de la solución técnica implementada (filtro de correo electrónico)

- Reducción de correos de phishing recibidos
- Bloqueo de mensajes con adjuntos maliciosos o enlaces sospechosos
- Disminución de correos spam detectados en bandeja de entrada
- Estabilidad del sistema y ausencia de interferencia en correos legítimos (falsos positivos)
- Registro de eventos o logs de detección y bloqueo

Evaluación del programa de concientización

- Participación del personal en las actividades de capacitación
- Resultados de las evaluaciones de conocimiento antes y después de la capacitación
- Número de incidentes reportados por los usuarios
- Cambio en el comportamiento del usuario (simulaciones o campañas de phishing ético)
- Retroalimentación de los participantes (encuestas o entrevistas)

Cumplimiento técnico y administrativo

- Cronograma original vs. ejecución real.
- Alcances definidos vs. soluciones entregadas.
- Presupuesto estimado vs. recursos utilizados.
- Cumplimiento de entregables técnicos y administrativos.

Análisis de brechas y oportunidades de mejora

- Aspectos que no se cumplieron totalmente o que requieren ajustes.
- Áreas que pueden ser fortalecidas en futuras etapas (por ejemplo, ampliar la concientización a otras amenazas).
- Lecciones aprendidas que servirán como base para la fase siguiente del ciclo (Act – Mejorar).

Cada uno de estos puntos fue evaluado utilizando KPIs con fórmulas objetivas y criterios de aceptación definidos, permitiendo determinar cuantitativamente el éxito del proyecto y las áreas con oportunidad de mejora. Esta verificación

sistemática respalda la toma de decisiones para la siguiente fase del ciclo: Act (Mejorar).

4.2.3.1 Evaluación de la solución técnica implementada (filtro de correo electrónico)

Este apartado analiza el impacto del filtro de correo electrónico en la seguridad de la organización. Se evalúa su efectividad en bloquear amenazas, reducir correo no deseado y mantener la operación estable, sin afectar la entrega de mensajes válidos. Cada indicador considera criterios cuantificables para validar la eficacia de la solución.

A. Reducción de correos de phishing recibidos

El filtro debe reducir significativamente la llegada de correos de phishing, minimizando la exposición a fraudes y robo de credenciales.

KPI: Tasa de reducción de correos phishing recibidos

$$\text{Reducción phishing (\%)} = \left(\frac{P_{\text{inicial}} - P_{\text{final}}}{P_{\text{inicial}}} \right) \times 100$$

- P_{inicial}: correos phishing detectados antes de implementar el filtro
- P_{final}: correos phishing recibidos luego de la implementación

Criterio de aceptación: ≥ 70%

Baseline inicial: No existe reducción, el 100% de intentos llegan a la bandeja del usuario antes del proyecto.

Meta progresiva: ≥70% en 6 meses; ≥80% en 12 meses.

Se considera aceptable porque implica una baja considerable del riesgo con una expectativa realista.

Justificación:

El umbral se fijó en 70% porque representa un equilibrio razonable entre impacto en la seguridad y viabilidad técnica.

- Valores mayores (90–95%) pueden aumentar falsos positivos y afectar la entrega de correos válidos.
- Valores menores (< 50%) no justifican la inversión ni reducen suficientemente el riesgo.

Fuente de datos**:** Consola de Proofpoint (logs de correo filtrados, reportes de amenazas).

Frecuencia: Mensual (comparación contra línea base).

Responsable: Especialista en Ciberseguridad.

B. Bloqueo de mensajes con adjuntos maliciosos o enlaces sospechosos

Evalúa la capacidad del filtro para detener correos peligrosos de forma automática.

KPI: Porcentaje de bloqueos efectivos

$$\text{Bloqueo efectivo } (\%) = \left(\frac{M_{\text{bloqueados}}}{M_{\text{intentados}}} \right) \times 100$$

- $M_{\text{bloqueados}}$: cantidad de correos con adjuntos o enlaces maliciosos bloqueados
- $M_{\text{intentados}}$: total de correos con adjuntos/enlaces maliciosos detectados

Criterio de aceptación: ≥ 95%

Baseline inicial: Sin control dedicado, bloqueo ≤60% con filtros básicos de Exchange.

Meta progresiva: ≥95% en 6 meses; mantener ≥97% estable en 12 meses.

Justificación:

El umbral del 95% asegura que el sistema bloquea la gran mayoría de amenazas antes de llegar al usuario, reduciendo la exposición directa.

- Valores mayores (ej. ≥ 98%) pueden ser técnicamente poco sostenibles o aumentar el riesgo de falsos positivos.
- Valores menores (< 90%) dejarían pasar demasiadas amenazas, comprometiendo la eficacia del sistema.

Fuente de datos: Plataforma Proofpoint

Frecuencia: Diario, con un consolidado mensual.

Responsable: Especialista en Ciberseguridad, con apoyo del Analista de Infraestructura TI.

C. Disminución de correos spam en bandeja de entrada

Una reducción efectiva del spam mejora la productividad y disminuye riesgos ocultos.

KPI: Tasa de disminución de spam recibido

$$\text{Bloqueo efectivo } (\%) = \left(\frac{M_{\text{bloqueados}}}{M_{\text{intentados}}} \right) \times 100$$

- $M_{\text{bloqueados}}$: cantidad de correos con adjuntos o enlaces maliciosos bloqueados
- $M_{\text{intentados}}$: total de correos con adjuntos/enlaces maliciosos detectados

Criterio de aceptación: ≥ 80%

Baseline inicial: Alto volumen de spam con un 0% reducción efectiva.

Meta progresiva: ≥80% en 6 meses; ≥85% en 12 meses.

Justificación:

El umbral del 80% ofrece un punto óptimo entre reducción efectiva de spam y minimización de falsos positivos.

- Uno más alto (ej. ≥ 90%) podría afectar la entrega de correos legítimos por sobre filtrado.
- Uno menor (< 70%) no produciría mejoras tangibles en la experiencia del usuario ni justificaría la solución implementada.

Fuente de datos: Consola de Proofpoint (reportes de spam entregado vs. bloqueado).

Frecuencia: Mensual.

Responsable: Analista de Infraestructura TI.

D. Estabilidad del sistema y falsos positivos

Un sistema eficaz debe bloquear amenazas sin afectar la entrega normal de correos válidos.

KPI: Tasa de falsos positivos

$$\text{Falsos positivos } (\%) = \left(\frac{C_{\text{legítimos bloqueados}}}{C_{\text{legítimos totales}}} \right) \times 100$$

- $C_{\text{legítimos bloqueados}}$: cantidad de correos válidos bloqueados por error
- $C_{\text{legítimos totales}}$: total de correos legítimos enviados al dominio

Criterio de aceptación: ≤ 2%

Un umbral comúnmente aceptado para no impactar operaciones.

Baseline inicial: Sin medición formal, pero tendencia a errores por ausencia de filtros.

Meta progresiva: ≤2% en 6 meses; ≤1% en 12 meses.

Justificación:
El 2% es un estándar aceptado en entornos corporativos, ya que asegura alta precisión sin generar fricciones operativas.

- Tasas menores al 2% mantienen la fluidez del trabajo sin requerir constantes revisiones del área TI.

- Valores más altos (> 5%) podrían interrumpir procesos clave por bloqueos erróneos de correos legítimos, afectando la productividad.

Fuente de datos: Consola Proofpoint junto a los tickets de soporte internos levantados por usuarios.

Frecuencia: Semanal, con un consolidado mensual.

Responsable: Analista de Calidad (QA).

E. Registro de eventos o logs de detección y bloqueo

Tener trazabilidad completa es clave para auditoría y análisis forense.

KPI: Porcentaje de eventos registrados

$$\text{Trazabilidad } (\%) = \left(\frac{E_{\text{logueados}}}{E_{\text{totales}}} \right) \times 100$$

- $E_{\text{logueados}}$: eventos detectados con registro disponible
- E_{totales}: total estimado de eventos detectados por el sistema

Criterio de aceptación: ≥ 95%

Permite mantener una trazabilidad confiable.

Baseline inicial: Sin registro centralizado.

Meta progresiva: ≥95% en 6 meses; ≥98% en 12 meses.

Justificación:
El registro de al menos el 95% de eventos garantiza trazabilidad casi total, suficiente para auditorías, investigación de incidentes y retroalimentación del sistema.

- Estándares de ciberseguridad recomiendan una cobertura cercana al 100% para mantener control efectivo.
- Un umbral inferior podría dejar brechas críticas sin registrar, afectando la capacidad de respuesta o corrección.

Fuente de datos: Consola Proofpoint.

Frecuencia: Diario con un consolidado mensual.

Responsable: Especialista en Ciberseguridad.

4.2.3.2 Evaluación del programa de concientización

Esta sección analiza el impacto del programa de capacitación sobre el comportamiento de los usuarios frente a amenazas por correo electrónico. Se consideran participación, mejora de conocimientos, capacidad de respuesta, comportamiento ante simulaciones y percepción general del contenido.

A. Participación del personal en las actividades de capacitación

Una alta participación demuestra el alcance real del programa y permite que su efecto sea transversal en la organización.

KPI: Tasa de participación

$$\text{Participación } (\%) = \left(\frac{N_{\text{asistentes}}}{N_{\text{invitados}}} \right) \times 100$$

- $N_{\text{asistentes}}$: número de empleados que participaron en las sesiones
- $N_{\text{invitados}}$: total de colaboradores convocados

Criterio de aceptación: ≥ 80%

Este valor asegura que la mayoría del personal fue impactada, permitiendo generar un cambio organizacional.

Baseline inicial: 0% debido a que no existe programa formal.

Meta progresiva: ≥80% de empleados capacitados en 6 meses; ≥90% en 12 meses

Justificación:
El umbral del 80% garantiza que una mayoría representativa del personal haya sido impactada por el programa.

- Este nivel de participación permite un cambio cultural organizacional sostenido.
- Umbrales menores (< 60%) reflejarían difusión parcial, limitando el alcance del aprendizaje.

Fuente de datos: Herramienta de concientización Proofpoint SAT.

Frecuencia: Trimestral.

Responsable: Consultor de Concientización.

B. Resultados de evaluaciones antes y después de la capacitación.

Se mide el aumento del conocimiento sobre buenas prácticas de seguridad y detección de amenazas.

KPI: Mejora de conocimiento

$$\text{Mejora } (\%) = \left(\frac{P_{\text{post}} - P_{\text{pre}}}{100 - P_{\text{pre}}} \right) \times 100$$

- P_{pre}: puntaje promedio pre capacitación
- P_{post}: puntaje promedio post capacitación

Criterio de aceptación: ≥ 60%
Este umbral refleja una mejora sustancial en la comprensión de los riesgos asociados al correo electrónico.

Baseline inicial: Promedio de respuestas correctas <40% en evaluaciones iniciales.

Meta progresiva: ≥60% de mejora en 6 meses; ≥75% en 12 meses.

Justificación:
Un aumento igual o mayor al 60% indica que el personal no solo participó, sino que comprendió e incorporó nuevos conocimientos.

- Este umbral se basa en experiencias de programas similares, donde un incremento inferior tiende a ser marginal.

- Superar esta meta valida tanto la metodología como la relevancia del contenido.
- Además, permite proyectar mejoras prácticas en el manejo del correo seguro.

Fuente de datos: Plataforma de concientización.

Frecuencia: Trimestral.

Responsable: Consultor de Concientización.

C. Número de incidentes reportados por los usuarios

El aumento de reportes demuestra que el personal reconoce riesgos y actúa proactivamente.

KPI: Tasa de reportes de incidentes

$$\text{Reportes } (\%) = \left(\frac{I_{\text{reportados}}}{I_{\text{total detectados}}} \right) \times 100$$

- $I_{\text{reportados}}$: incidentes reportados por usuarios
- $I_{\text{total detectados}}$: total estimado de correos sospechosos que llegaron a usuarios

Criterio de aceptación: ≥ 20%

Este nivel indica que se está desarrollando una cultura de seguridad participativa.

Baseline inicial: no existen reportes previos registrados.

Meta progresiva: ≥20% en 6 meses; ≥30% en 12 meses.

Justificación:
Un mínimo del 20% representa que una parte relevante del personal está alerta y aplica lo aprendido.

- Este umbral es razonable en entornos donde la cultura de reporte aún se está desarrollando.
- Aumentar los reportes refleja madurez organizacional y empoderamiento del usuario frente a amenazas.

- El incremento sostenido en reportes indica vigilancia activa y compromiso con la seguridad.

Fuente de datos: Botón de reporte en cliente de correos junto al buzón de incidentes.

Frecuencia: Semanal, con un consolidado mensual.

Responsable: Especialista en Ciberseguridad (análisis) junto al Consultor de Concientización (seguimiento).

D. Cambio en el comportamiento del usuario (simulaciones de phishing).

Se mide cuántos usuarios fueron víctimas de campañas de phishing ético antes y después de la capacitación.

KPI: Tasa de mejora en simulaciones de phishing

$$\text{Reducción de clics (\%)} = \left(\frac{C_{\text{antes}} - C_{\text{después}}}{C_{\text{antes}}} \right) \times 100$$

- C_{antes}: usuarios que hicieron clic en phishing antes de la capacitación
- $C_{\text{después}}$: usuarios que cayeron después de la capacitación

Criterio de aceptación: ≥ 50% de reducción

Este valor refleja una transformación práctica en el comportamiento ante amenazas reales.

Baseline inicial: ≥60% de clics en pruebas iniciales.

Meta progresiva: Reducción ≥50% en 6 meses; ≥70% en 12 meses.

Justificación:
Reducir a la mitad los clics en correos falsos demuestra un cambio conductual tangible.

- Este umbral está alineado con buenas prácticas internacionales (ej. SANS Institute).

- Menor exposición en campañas éticas indica internalización de conocimientos.
- Es un indicador directo de que el aprendizaje fue aplicado en escenarios realistas.

Fuente de datos: Resultados de campañas de phishing simulado Proofpoint SAT.

Frecuencia: Trimestral.

Responsable: Consultor de Concientización.

E. Retroalimentación de los participantes

La percepción del personal sobre la utilidad del contenido permite validar el valor percibido y detectar oportunidades de mejora.

KPI: Nivel de satisfacción promedio

$$\text{Satisfacción promedio} = \frac{\sum R_i}{N}$$

- R_i: puntuación de satisfacción de cada participante (escala 1 a 5 o 1 a 10)
- N: total de encuestas respondidas

Criterio de aceptación: ≥ 4.0 (escala de 1 a 5)

Este valor asegura que la mayoría encontró la capacitación útil, clara y relevante.

Baseline inicial: Sin métricas de a que no se mide actualmente.

Meta progresiva: ≥4 en 6 meses; ≥4,5 en 12 meses.

Justificación:
Una media de 4.0 asegura que la mayoría valoró la formación positivamente.

- Este nivel de satisfacción fomenta futuras participaciones y refuerza la percepción de utilidad.
- Valores más bajos podrían indicar falta de claridad, lenguaje técnico excesivo o baja aplicabilidad.

- Una experiencia bien evaluada es clave para sostener el ciclo de concientización continua.

Fuente de datos: Encuestas internas posteriores a cada capacitación.

Frecuencia: Trimestral.

Responsable: Consultor de Concientización.

4.2.3.3 Revisión documental y cumplimiento del plan

En este apartado se contrasta lo planificado inicialmente con lo efectivamente ejecutado, tanto en términos técnicos como administrativos. Se comparan hitos temporales (cronograma), alcances proyectados con respecto a las funcionalidades entregadas, y el presupuesto estimado frente a los recursos reales utilizados. También se revisa el cumplimiento de los entregables acordados, tanto técnicos (configuraciones, documentación, informes) como administrativos. Esta revisión es clave para evaluar la capacidad de gestión del proyecto, el uso eficiente de recursos y el nivel de organización del equipo ejecutor. Además, permite detectar posibles desviaciones que pudieran impactar en futuras implementaciones similares.

Se revisa el cumplimiento de las actividades propuestas en la planificación inicial del proyecto, contrastando:

A. Cronograma original vs. ejecución real.

El seguimiento del cronograma permite medir la eficiencia de la gestión del tiempo durante la ejecución del proyecto. Esta comparación busca identificar desviaciones entre los plazos planificados y los tiempos reales de ejecución, con el fin de evaluar la planificación y la ejecución operativa.

KPI: Porcentaje de cumplimiento de la carta Gantt

Fórmula:

$$\text{Cumplimiento del cronograma } (\%) = \left(\frac{T_{\text{planificado}}}{T_{\text{real}}} \right) \times 100$$

- $T_{\text{planificado}}$: tiempo total estimado en el cronograma original
- T_{real}: tiempo total real de ejecución del proyecto

Criterio de aceptación: entre 90% y 110%

Justificación:

Se acepta un cumplimiento entre 90% y 110% como margen razonable, considerando que pueden surgir contingencias menores sin comprometer el éxito general. Este rango permite evaluar tanto atrasos como adelantos con una perspectiva realista de gestión de proyectos.

Fuente de datos: Cronograma maestro del proyecto.

Frecuencia: Mensual.

Responsable: Jefe de Proyecto.

B. Alcances definidos vs. soluciones entregadas.

Es esencial verificar si el producto final cumple con todos los objetivos definidos inicialmente. Este indicador permite evaluar si se entregaron todas las funcionalidades y mejoras previstas en el alcance del proyecto, sin omisiones ni entregas parciales.

KPI: Porcentaje de cumplimiento del alcance

Fórmula:

$$\text{Cumplimiento del alcance } (\%) = \left(\frac{E_{\text{entregado}}}{E_{\text{planificado}}} \right) \times 100$$

- $E_{\text{entregado}}$: número de entregables o funcionalidades completadas
- $E_{\text{planificado}}$: entregables definidos en el acta de inicio del proyecto

Criterio de aceptación: Aceptable: ≥ 95%

Justificación:
Se considera ≥ 95% como cumplimiento aceptable, dado que siempre puede haber pequeñas adaptaciones o limitaciones técnicas no previstas. Este valor asegura que la mayor parte del valor comprometido al inicio fue efectivamente entregada.

Fuente de datos: Documentación del proyecto planificación contrastada con los entregables.

Frecuencia: Al cierre de cada fase.

Responsable: Jefe de Proyecto junto al Analista de Calidad (QA).

C. Presupuesto estimado vs. recursos utilizados.

Este KPI evalúa el control financiero del proyecto, comparando los costos estimados con los realmente utilizados. Aunque en algunos proyectos de título no se maneja presupuesto formal, este indicador puede aplicarse para medir uso de horas-hombre, licencias, herramientas, etc.

KPI: Porcentaje de desviación presupuestaria

Fórmula:

$$\text{Desviación presupuestaria } (\%) = \left(\frac{C_{\text{real}} - C_{\text{estimado}}}{C_{\text{estimado}}} \right) \times 10($$

- C_{real}: costo o recursos efectivamente utilizados
- C_{estimado}: presupuesto o recursos planificados

Criterio de aceptación: ±10% de desviación

Justificación:
Una desviación de ±10% es estándar en gestión de proyectos. Este rango permite manejar variaciones normales sin considerarse ineficiencia o mala planificación. Superar ese valor puede indicar falta de control o cambios mal gestionados.

Fuente de datos: Registros de costos (HH, licencias, soporte).

Frecuencia: Trimestral.

Responsable: Jefe de Proyecto.

D. Cumplimiento de entregables técnicos y administrativos.

Todo proyecto debe cerrar con documentación técnica y administrativa que respalde la implementación. Este KPI mide si los entregables como manuales, informes, minutas y respaldos técnicos fueron entregados en forma y tiempo.

KPI: Porcentaje de entregables cumplidos

Fórmula:

$$\text{Cumplimiento de entregables } (\%) = \left(\frac{D_{\text{entregados}}}{D_{\text{requeridos}}} \right) \times 100$$

- $D_{\text{entregados}}$: entregables realizados y validados
- $D_{\text{requeridos}}$: entregables definidos en el plan de trabajo

Criterio de aceptación: Aceptable: ≥ 90%

Justificación:
Un nivel de ≥ 90% garantiza que casi la totalidad de la documentación y respaldos fue entregada de forma oportuna. Este umbral permite un pequeño margen de error, pero asegura cumplimiento formal del proyecto ante revisores y stakeholders.

Fuente de datos: Checklist de QA junto a la documentación técnica y administrativa.

Frecuencia: Al cierre del proyecto y de cada fase mayor.

Responsable: Analista de Calidad (QA).

4.2.3.4 Análisis de brechas y oportunidades de mejora

Esta sección identifica puntos del proyecto que no cumplieron completamente las expectativas, así como oportunidades de mejora en la solución técnica y en el

proceso de concientización. También se documentan aprendizajes clave que servirán para futuras fases de seguridad y mejora continua.

A. Aspectos que no se cumplieron totalmente o que requieren ajustes

Se analizan desviaciones respecto a lo planificado, con foco en entregables incompletos o modificados. Esta revisión permite detectar puntos débiles y corregirlos a tiempo en futuras implementaciones.

KPI: Porcentaje de desviaciones detectadas en entregables

$$\text{Desviaciones } (\%) = \left(\frac{E_{\text{incompletos o ajustados}}}{E_{\text{totales}}} \right) \times 100$$

- $E_{\text{incompletos o ajustados}}$: entregables que no cumplieron con los criterios iniciales
- E_{totales}: total de entregables evaluados

Criterio de aceptación: ≤ 10%

Este límite permite cierto margen de error sin comprometer la calidad global del proyecto.

Justificación:
El porcentaje está justo en el umbral aceptable. Aunque no es crítico, indica que hay espacio para mejorar los procesos de revisión y control en fases tempranas del proyecto.

Fuente de datos: Cronograma maestro (Gantt), registro de cambios (change log), checklist de QA, actas de reunión.

Frecuencia: Seguimiento semanal en ejecución; consolidado mensual y revisión al cierre de fase.

Responsable: Jefe de Proyecto y Analista de Calidad.

B. Áreas del sistema técnico que pueden ser mejoradas o ampliadas

Este indicador evalúa si hay módulos del sistema que pueden fortalecerse, ya sea por limitaciones funcionales detectadas o por necesidades futuras de escalabilidad.

KPI: Proporción de componentes identificados como mejorables

$$\text{Áreas a mejorar } (\%) = \left(\frac{A_{\text{detectadas}}}{A_{\text{evaluadas}}} \right) \times 100$$

- $A_{\text{detectadas}}$: áreas donde se propusieron mejoras concretas
- $A_{\text{evaluadas}}$: áreas clave revisadas durante el cierre del proyecto

Criterio de aceptación: ≤ 25%

Un máximo de 25% es razonable en etapas iniciales, permitiendo detectar mejoras sin comprometer la estabilidad general.

Fuente de datos: Informes de rendimiento, retrospectivas técnicas, tickets de mejora.

Frecuencia: Mensual, con revisión al cierre de fase.

Responsable: Especialista en Ciberseguridad y Analista de Infraestructura TI.

Justificación:
El resultado se mantiene dentro del rango esperado. Identificar mejoras en ciertos módulos (como el filtrado granular o los informes automatizados) permitirá robustecer el sistema en la próxima fase.

C. Ámbitos de la concientización que requieren refuerzo

El programa de formación también puede presentar áreas menos efectivas. Este KPI identifica contenidos o enfoques que no lograron el impacto deseado y deben ajustarse.

KPI: Porcentaje de temas de capacitación con baja retención o recepción

$$\text{Áreas a mejorar } (\%) = \left(\frac{A_{\text{detectadas}}}{A_{\text{evaluadas}}} \right) \times 100$$

- $A_{\text{detectadas}}$: áreas donde se propusieron mejoras concretas
- $A_{\text{evaluadas}}$: áreas clave revisadas durante el cierre del proyecto

Criterio de aceptación: ≤ 20%

Un valor ≤ 20% es aceptable, permitiendo reconocer temáticas que no fueron bien comprendidas o valoradas sin afectar la percepción global del programa.

Justificación:
El resultado cumple el criterio, pero destaca la necesidad de reformular o reforzar algunos contenidos, como el uso de firmas digitales o la gestión de adjuntos sospechosos.

Fuente de datos: Plataforma de concientización, encuestas de satisfacción, reportes de campañas de phishing simulado.

Frecuencia: Trimestral por campaña, resumen mensual de avance.

Responsable: Consultor de Concientización y Especialista en Ciberseguridad.

D. Lecciones aprendidas documentadas para mejora continua

Registrar y compartir lo aprendido es clave para que otras iniciativas aprovechen la experiencia ganada.

KPI: Porcentaje de hallazgos y lecciones documentadas formalmente

Criterio de aceptación: ≥ 90%

Un nivel alto asegura que los aprendizajes se capitalicen y queden disponibles como insumo futuro.

Justificación:
El registro fue casi completo, lo cual garantiza continuidad y coherencia en futuros ciclos de mejora. Esta práctica fortalece la cultura organizacional orientada al aprendizaje.

Fuente de datos: Repositorio de lecciones aprendidas.

Frecuencia: Tras cada incidente y cierre de fase, con revisión trimestral de completitud.

Responsable: Jefe de Proyecto y Analista de Calidad.

4.2.4 Act (Actuar)

En esta etapa se cierra formalmente el ciclo PDCA en curso, luego de la evaluación realizada en la fase "Verificar", se han identificado oportunidades de mejora que dan origen a nuevos ciclos de acción. El propósito de esta etapa es estandarizar los aciertos e implementar ajustes específicos para robustecer la solución y la cultura de seguridad de manera continua. Las cuales se detallan en las siguientes líneas de acción.

4.2.4.1 Línea de Acción: Ciclo de Implementación de Prevención de Fuga de Datos (DLP)

Esta acción se introduce para abordar de manera proactiva el riesgo de fuga de información sensible, una vulnerabilidad crítica identificada en múltiples fases del análisis, como la exposición de cotizaciones y la propiedad intelectual.

- **Objetivo y Estrategia de Mejora:**
    - **Objetivo:** Prevenir la exfiltración no autorizada de datos comerciales y técnicos confidenciales, fortaleciendo la protección de los activos de información de la empresa.
    - **Estrategia:** Implementar un piloto de DLP en modo "monitoreo" para detectar fugas de información sin interrumpir las operaciones, enfocándose inicialmente en los datos de mayor riesgo.
- **Acciones Planificadas:**
    - **Taller de Clasificación de Información:** Realizar una sesión de trabajo con los líderes de las áreas Comercial y Técnica para definir y clasificar formalmente la información crítica (ej., plantillas de

cotización, listas de precios, planos de diseño CAD, datos de clientes).

- **Configuración de Política DLP en Modo Monitoreo:** Activar el módulo de DLP en la plataforma de seguridad existente (Proofpoint) y configurar una política inicial que alerte (sin bloquear) sobre el envío de la información clasificada a dominios externos.
- **Implementación del Piloto con el Área Comercial:** Aplicar la política de monitoreo exclusivamente a los usuarios del área de "Gestión Comercial", por ser el equipo que maneja la información de precios y datos de clientes de forma constante.
- **Análisis y Ajuste de Alertas:** Revisar semanalmente las alertas generadas por el sistema DLP para identificar fugas reales y ajustar las reglas para reducir los falsos positivos.

- **Evaluación de Resultados (KPIs):**
  - **KPI 1: Precisión en la Detección de Datos Sensibles:** Medir el porcentaje de documentos sensibles enviados (en un entorno de prueba controlado) que son correctamente identificados por la política de DLP.
    - **Meta:** Lograr una precisión de detección ≥ 95%
  - **KPI 2: Tasa de Falsos Positivos en DLP:** Calcular el porcentaje de alertas generadas que corresponden a comunicaciones de negocio legítimas y permitidas.
    - **Meta:** Mantener una tasa de falsos positivos ≤ 5% durante la fase piloto.
- **Justificación:** La implementación de una capacidad de DLP es un paso evolutivo y crucial para la madurez en ciberseguridad de la empresa. Mientras que la propuesta inicial se centró en defender a la organización de amenazas externas (phishing, malware), esta acción aborda el riesgo, igualmente crítico, de la pérdida de información desde adentro hacia

afuera. El éxito de este ciclo, validado a través de sus metas de precisión en la detección y una baja tasa de falsos positivos, demostraría la viabilidad técnica y operacional de proteger activamente la propiedad intelectual (planos, diseños) y los datos comerciales sensibles (cotizaciones, precios). Esto no solo mitiga riesgos de alto impacto financiero y reputacional, sino que también justifica una futura inversión para expandir esta protección a toda la organización, completando así un enfoque de seguridad verdaderamente integral.

Fuentes: Consola DLP/Proofpoint.

Frecuencia: Semanal (ajuste y revisión de incidentes), consolidado mensual.

Responsables: Especialista en Ciberseguridad y Analista de Calidad.

4.2.4.2 Línea de Acción: Implementación de un Proceso Formalizado de Reporte de Incidentes

Esta acción se enfoca en fortalecer al usuario como la última línea de defensa, reconociendo que ninguna plataforma tecnológica es infalible. Se basa en la necesidad de que los empleados no solo detecten, sino que también reporten de manera efectiva un correo malicioso que haya logrado eludir los filtros automáticos, convirtiendo la concientización en una acción medible y eficaz.

- **Objetivo y Estrategia de Mejora:**
    - **Objetivo:** Reducir el tiempo de detección y respuesta ante un incidente de seguridad que haya superado las barreras tecnológicas, mediante la implementación de un canal de reporte claro y un procedimiento formal.
    - **Estrategia:** Combinar una herramienta técnica de fácil uso (botón de reporte en el cliente de correo) con un procedimiento de respuesta documentado y comunicado, para que el usuario sepa exactamente qué hacer y qué esperar al reportar una amenaza.

- **Acciones Planificadas:**
    - **Implementación Técnica del Botón de Reporte:** Desplegar un complemento en el cliente de correo (Microsoft Exchange) que añada un botón "Reportar Correo Malicioso". Al presionarlo, el correo será enviado automáticamente a un buzón de análisis de seguridad y eliminado de la bandeja del usuario.
    - **Desarrollo del Procedimiento de Respuesta:** Crear un flujograma simple y visual que describa el proceso post-reporte: confirmación de recepción, análisis por parte del equipo correspondiente y comunicación de los resultados al usuario que reportó.
    - **Campaña de Comunicación y Entrenamiento:** Lanzar una campaña interna para presentar la nueva herramienta y el procedimiento. Esto incluirá un video demostrativo de 2 minutos, infografías y una sección dedicada en el programa de concientización.
    - **Simulacro de Reporte de Incidentes:** Ejecutar un simulacro donde se envía un correo sospechoso (pero inofensivo) a todos los usuarios, con el objetivo de medir cuántos utilizan correctamente el nuevo botón de reporte en lugar de solo eliminarlo o ignorarlo.
- **Evaluación de Resultados (KPIs):**
    - **KPI 1: Tasa de Adopción de la Herramienta de Reporte:** Medir el porcentaje de usuarios que utilizan el nuevo botón durante el simulacro de reporte.
        - **Meta:** Lograr una tasa de adopción ≥ 70%.
    - **KPI 2: Tiempo Medio para Reportar:** Calcular el tiempo promedio que transcurre desde la entrega de un correo malicioso (en un simulacro) hasta que es reportado por el primer usuario.

        - **Meta:** Reducir el tiempo medio de reporte a menos de 60 minutos.

- **Justificación:** Esta iniciativa es la materialización del concepto de "cultura de ciberseguridad", transformando al empleado de un posible eslabón débil a un sensor de defensa activo. El proyecto identifica el "error humano" como una causa principal de brechas de seguridad. Por lo tanto, establecer un proceso de reporte formal y simple no es solo una mejora técnica, sino un cambio cultural. El cumplimiento de las metas de alta adopción de la herramienta y un bajo tiempo de reporte validaría que la inversión en concientización ha generado un retorno medible. Demostraría que la organización ha creado una capacidad de resiliencia humana, capaz de acortar drásticamente los tiempos de respuesta ante un incidente real y minimizar su impacto, lo cual es fundamental para una defensa integral y sostenible en el tiempo.

Fuentes: Telemetría del botón de reporte, mesa de ayuda (tickets), resultados de simulacros.

Frecuencia: Por campaña/simulacro trimestral, con seguimiento mensual de adopción y tiempos.

Responsables: Especialista en Ciberseguridad y Analista de Calidad.

Con la ejecución de las líneas de acción priorizadas, se cierra formalmente el ciclo PDCA vigente y se consolidan los aprendizajes de la fase Verificar, se estandarizan los aciertos, se implementan ajustes específicos sobre las brechas detectadas y se actualizan los artefactos de gobierno. Con estos cambios documentados y con recursos y plazos definidos se traspasan las iniciativas al siguiente “Plan”, asegurando la mejora continua del control de correo y de la cultura de seguridad mediante un nuevo ciclo con objetivos más precisos, indicadores trazables y revisiones periódicas.

4.2.4.3 Gestión de la resistencia al cambio

Este apartado no forma parte de los alcances definidos en el presente proyecto, sino que corresponde a una propuesta de mejora continua dirigida a la organización. La responsabilidad de su ejecución recae en la empresa en el futuro, como parte de su estrategia de sostenibilidad en seguridad. Para abordar este desafío, se sugieren estrategias de gestión del cambio organizacional orientadas a asegurar la adopción sostenida de la solución:

- Comunicación clara y temprana: se mantendrá informados a los empleados sobre los objetivos, beneficios y alcances de la plataforma de seguridad y del programa de concientización, reduciendo la incertidumbre y generando confianza.
- Capacitación continua y acompañamiento: se reforzará el aprendizaje mediante capacitaciones periódicas, guías prácticas y campañas de phishing simulado que permitan a los usuarios ejercitar nuevas conductas en un entorno controlado.
- Participación: se incentivará la retroalimentación de los trabajadores, generando instancias de consulta y mejora continua en base a sus experiencias de uso.
- Reconocimiento y refuerzo positivo: se valorará el desempeño de quienes demuestren buenas prácticas de seguridad, motivando la adherencia al cambio mediante incentivos no económicos, como reconocimientos internos.

De esta manera, la propuesta no solo introduce una mejora técnica, sino que incorpora medidas concretas para asegurar su adopción cultural y mitigar la resistencia natural al cambio, garantizando la sostenibilidad de los resultados en el tiempo.

5 Análisis Económico

Tras haber definido la propuesta de mejora y el plan de acción para su implementación, este capítulo se centra en evaluar la viabilidad y sostenibilidad económica del proyecto. Un análisis financiero riguroso es fundamental para justificar la inversión, no solo desde una perspectiva de seguridad, sino también como una decisión estratégica que aporta valor tangible a la organización. A continuación, se desglosarán los costos asociados a la implementación de la plataforma de seguridad y el programa de concientización, se realizará un análisis costo-beneficio para cuantificar el retorno de la inversión y se examinarán los beneficios, tanto económicos como intangibles, que la solución aportará a la empresa.

5.1 Costos de la propuesta

Para llevar a cabo la implementación de la solución de seguridad de correo electrónico y el programa de concientización, es indispensable realizar una estimación detallada de todos los recursos económicos necesarios. En esta sección se desglosarán los costos del proyecto, clasificándolos en distintas categorías para ofrecer una visión clara y ordenada de la inversión requerida. Este análisis abarcará desde los costos de infraestructura tecnológica y el capital humano involucrado, hasta los costos fijos y variables asociados a la operación de la nueva plataforma, sentando las bases para una evaluación financiera completa.

Los costos de todas las tablas presentadas en este punto serán calculados considerando un tipo de cambio referencial de $971,88 CLP/USD, con datos obtenidos del banco central de chile del día 08-08-2025.

5.1.1 Costos de infraestructura

La solución propuesta se implementa íntegramente bajo un modelo Software as a Service (SaaS) provisto por Proofpoint, lo que elimina la necesidad de adquirir, instalar o mantener infraestructura física propia. Toda la operación de la plataforma, incluyendo servidores, almacenamiento, balanceo de carga y

mecanismos de alta disponibilidad, es gestionada y soportada directamente por el proveedor. Esto significa que las tareas de mantención preventiva, actualizaciones de software y gestión de capacidad quedan bajo responsabilidad de Proofpoint, garantizando un servicio estable, seguro y escalable sin costos adicionales para la organización en términos de hardware, licencias de sistemas base o personal técnico especializado para su operación. Gracias a este enfoque, la empresa puede concentrar sus recursos en la adopción y uso efectivo de la plataforma, asegurando un despliegue ágil y una reducción significativa de riesgos asociados a la administración de infraestructura propia.

5.1.2 Costos de capital humano

El éxito de la implementación del proyecto depende directamente de la experiencia y dedicación del equipo de trabajo. Este costo representa la inversión en las horas profesionales del equipo multidisciplinario, cuyo tiempo se calculó sumando las duraciones de cada tarea asignada en el plan de proyecto. Dichas actividades fueron enumeradas en la sección 4.2.1 'Plan (Planificar)' y su ejecución se detalló a lo largo de las cinco fases descritas en la sección 4.2.2 'Do (hacer)'. Para valorizar este esfuerzo, y dado que el documento no especifica salarios, se utilizarán costos por hora referenciales basados en el mercado laboral chileno para perfiles TI, permitiendo así una estimación realista de la inversión total en capital humano.

5.1.2.1 Cálculo de valor hora hombre

La siguiente tabla presenta la estimación del costo real de cada profesional involucrado en el proyecto, considerando la conversión de su sueldo líquido a bruto, el costo empresa asociado y el valor hora-hombre. Estos cálculos permiten reflejar de manera transparente y fundamentada el gasto en recursos humanos.

Tabla 7: Costos de capital humano en hora hombre

Rol	Sueldo Líquido (CLP)	Sueldo Bruto Estimado (CLP)	Costo Empresa (CLP)	Valor HH (CLP)
Jefe de Proyecto	$2.200.000	$2.750.000	$3.300.000	$20.625
Especialista en Ciberseguridad	$2.000.000	$2.500.000	$3.000.000	$18.750
Analista de Infraestructura TI	$1.600.000	$2.000.000	$2.400.000	$15.000
Analista de Calidad (QA)	$1.600.000	$2.000.000	$2.400.000	$15.000
Consultor de Concientización	$2.500.000	$3.125.000	$3.750.000	$23.438

Fuente: Elaboración propia con datos obtenidos de análisis de mercado laboral

Criterios utilizados

Del sueldo líquido al bruto Se aplicó un factor de 1,25. El líquido representa aprox. un 80% del bruto, considerando descuentos legales de AFP, Salud e impuestos.

Costo empresa

Al sueldo bruto se le sumó un 20% adicional correspondiente a cotizaciones patronales y costos asociados a la relación laboral (seguro de cesantía, mutual, seguro de invalidez, etc.).

Valor hora-hombre (HH) Se calculó en base a una jornada de 160 horas mensuales (40 horas semanales).

5.1.2.2 Cálculo de horas hombre utilizadas en este proyecto

Una vez establecidos los costos asociados a cada perfil profesional, resulta necesario detallar la distribución temporal de su participación en el proyecto. Esta planificación permite vincular el costo hora-hombre previamente calculado con la carga efectiva de trabajo de cada rol.

Tabla 8: Cálculo de las horas hombre

Jefe de Proyecto			
Tarea	**Sem.**	**Días**	**HH**
Constitución y Planificación	2	10	80
Plan de Gestión del Proyecto	1	5	40
Revisión y Supervisión	1	5	40
Total Jefe de Proyecto	**4**	**20**	**160**
Especialista en Ciberseguridad			
Tarea	**Sem.**	**Días**	**HH**
Evaluación de Soluciones de Seguridad	2	10	80
Implementación de Plataforma	2	10	80
Coordinación de Integración	2	10	80
Total Especialista en Ciberseguridad	**6**	**30**	**240**
Analista de Infraestructura TI			
Tarea	**Sem.**	**Días**	**HH**
Levantamiento Infraestructura	1	5	40
Configuración Entorno Pruebas	1	5	40
Total Analista de Infraestructura TI	**2**	**10**	**80**
Analista de Calidad (QA)			
Tarea	**Sem.**	**Días**	**HH**
Planificación Pruebas	1	5	40
Ejecución Pruebas	2	10	80
Total Analista de Calidad (QA)	**3**	**15**	**120**
Consultor de Concientización			
Tarea	**Sem.**	**Días**	**HH**
Desarrollo Programa	2	10	80
Implementación Programa	1	5	40
Total Consultor de Concientización	**3**	**15**	**120**

Fuente: Elaboración propia con datos de ContruPro

5.1.2.3 Calculo costo en mano de obra del proyecto en HH

Con el valor hora-hombre previamente calculado y la planificación de horas asignadas a cada rol, es posible determinar el costo total de los recursos humanos involucrados en el proyecto. La siguiente tabla muestra el resultado de

esta relación, reflejando el gasto estimado por profesional y el monto global asociado al desarrollo del proyecto.

Tabla 9: Calculo costo total de HH en pesos.

Rol / Profesional	Valor HH (CLP)	Cantidad HH	Costo Total (CLP)
Jefe de Proyecto	$20.625	160	$3.300.000
Especialista en Ciberseguridad	$18.750	240	$4.500.000
Analista Infraestructura TI	$15.000	80	$1.200.000
Analista QA	$15.000	120	$1.800.000
Consultor Concientización	$23.438	120	$2.812.500
Total General			**$13.612.500**

Fuente: Elaboración propia con datos de ContruPro

5.1.3 Costos fijos

Los costos fijos del proyecto corresponden principalmente a la suscripción anual de la plataforma Proofpoint Cloud bajo modalidad *Software as a Service* (SaaS), que incluye tanto la protección avanzada de correo electrónico como el módulo de concientización, simulación de ataques de phishing para 500 usuarios y soporte sobre incidencias de la plataforma. Al tratarse de un servicio en la nube, no requiere implementación ni mantención de servidores físicos (*on-premise*), lo que elimina gastos en hardware y soporte interno. Según datos de distribuidores y análisis de mercado, el costo estimado para la plataforma de filtrado de correo más la protección avanzada se sitúa entre USD 24 y USD 48 por usuario/año (Underdefender, 2025; Sherweb, 2021), mientras que el módulo de *Security Awareness Training* (concientización) y simulación de phishing se encuentra entre USD 18 y USD 25 por usuario/año (Constant Edge, s.f.; CDW, s.f.). Para este análisis se adopta un valor promedio de USD 36 por usuario/año para la plataforma cloud y USD 22 por usuario/año para el módulo de concientización, lo que permite proyectar de manera realista la inversión anual necesaria.

Tabla 10: Costos fijos

N°	Nombre	Descripción	Costo usuario/año (USD)	Cantidad usuarios	Costo USD	Costo CLP
1	Proofpoint Cloud – Protección correo	Plataforma SaaS de filtrado y protección avanzada contra phishing, malware y suplantación de identidad.	36	500	18.000	$17.493.840
2	Proofpoint SAT – Concientización y simulación	Módulo de capacitación en seguridad y campañas de phishing simulado.	22	500	11.000	$10.690.680
	Total				29.000	$28.184.520

Fuente: Elaboración propia con datos obtenidos de análisis de mercado comercial

5.1.4 Costos variables

En el marco de este proyecto, el único costo variable identificado corresponde a la contratación de soporte técnico especializado bajo demanda, el cual se presenta cuando se requiere la intervención de ingenieros certificados para realizar configuraciones avanzadas, integraciones específicas o resolver incidencias críticas que exceden el alcance del soporte estándar incluido en la suscripción anual de Proofpoint.

Según referencias de mercado y estimaciones publicadas por distribuidores y proveedores de servicios profesionales, como Underdefense y Sherweb, el valor promedio de la hora de soporte técnico especializado para soluciones de seguridad en la nube de tipo SaaS oscila entre 180 y 220 USD por hora, se

considerará un valor promedio de 200 USD por hora de soporte, en un escenario de 10 horas anuales.

Tabla 11: Costos variables

N°	Nombre	Descripción	Horas (anuales)	Valor Hora USD	Valor anual USD	Valor anual CLP
1	Soporte técnico especializado bajo demanda	Intervenciones o configuraciones no cubiertas en el contrato estándar	10	200	2000	$1.943.760

Fuente: Elaboración propia con datos obtenidos de análisis de mercado comercial

5.1.5 Costo Total del proyecto

El costo total del proyecto corresponde a la suma de todos los elementos definidos en los apartados anteriores, incluyendo los costos de infraestructura, los costos fijos asociados al licenciamiento anual de la plataforma y al soporte estándar, así como los costos variables vinculados a la contratación eventual de soporte técnico especializado. Este cálculo permite obtener una estimación global de la inversión necesaria para la puesta en marcha y operación de la solución propuesta durante su primer año de funcionamiento.

La consolidación de estos costos no solo entrega una visión clara del presupuesto requerido, sino que también facilita la evaluación económica y la toma de decisiones en relación con el retorno esperado y la viabilidad financiera del proyecto.

Tabla 12: Costos total del proyecto

Item	Nombre	Costo Total CLP
5.1.1	Costos de infraestructura	$ 0
5.1.2	Costos de capital humano	$ 13.612.500
5.1.3	Costos fijos	$ 28.184.520
5.1.4	Costos variables	$ 1.943.760
	TOTAL	$ 43.740.780

Fuente: Elaboración propia con datos obtenidos de ContruPro.

Nota: valores indicados son valores netos.

5.2 Beneficios económicos

La implementación de la plataforma de seguridad y el programa de concientización no debe ser vista únicamente como un gasto operativo, sino como una inversión estratégica destinada a proteger los activos y la continuidad del negocio. Los beneficios económicos del proyecto se derivan principalmente de la mitigación de los riesgos financieros directos identificados en el análisis de la situación actual. Amenazas como la suplantación de identidad para el desvío de fondos, la recepción de comprobantes de pago falsificados y la fabricación basada en información fraudulenta representan un impacto económico tangible y cuantificable que la solución propuesta busca anular.

En esta sección, se procederá a cuantificar estos beneficios, estimando los costos evitados gracias a la implementación de los nuevos controles de seguridad. Este análisis permitirá demostrar el valor económico directo que el proyecto aporta a la empresa, estableciendo una base sólida para la evaluación del retorno de la inversión que se detallará en el siguiente apartado.

5.2.1 Beneficios económicos

El análisis costo-beneficio (ACB) es una herramienta financiera fundamental para evaluar la viabilidad de un proyecto, comparando los costos totales de la

inversión con los beneficios económicos que se espera obtener. Para este proyecto, el análisis se centra en demostrar que la inversión en la plataforma de seguridad y el programa de concientización no solo se justifica, sino que también genera un retorno positivo al prevenir pérdidas financieras significativas. La viabilidad del proyecto se determinará utilizando dos indicadores clave:

- **Relación Costo-Beneficio (CB) > 1:** Indica que los beneficios superan los costos, haciendo el proyecto financieramente favorable.
- **Ganancia Total Neta (GTN) > 0:** Muestra que el proyecto genera un valor económico neto positivo después de cubrir todos los costos de inversión.

5.2.1.1 Estimación de Beneficios Anuales

Los beneficios se cuantifican como los costos directos que la empresa evitará anualmente al mitigar los riesgos de mayor criticidad. Para este análisis, se utilizarán estimaciones de pérdida definidas por la propia empresa, las cuales se fundamentan en el conocimiento de sus costos operativos y el valor promedio de sus proyectos**.** Esta metodología permite anclar el análisis en el impacto financiero real que un incidente tendría sobre la organización, considerando el costo de materiales, mano de obra y la pérdida de ingresos asociada a un proyecto comprometido.

Tabla 13: Costos total del proyecto

Riesgo Mitigado	Estimación de Pérdida Anual (CLP)	Justificación de la Estimación
Suplantación de identidad para desviar pagos de clientes	$8.500.000	Se estima la pérdida de al menos un pago ($8.500.000 Valor unitario) de un proyecto modular de tamaño mediano al año, considerando el alto riesgo (Impacto 4, Probabilidad 4)
Falsificación de información de la empresa cliente	$6.000.000	Se estima el costo asociado al desgaste de recursos comerciales y técnicos en procesos de cotización y diseño para clientes fraudulentos.

Recepción de comprobantes de pago falsificados	$19.500.000	Se proyecta el costo de fabricación y entrega de un módulo (Valor unitario + gastos administrativos + gastos de movilización material) basado en un comprobante fraudulento, lo que representa una pérdida directa del activo y los recursos invertidos.
Total de Beneficios Anuales (Costos Evitados)		**$34.000.000**

Fuente: Elaboración propia con datos obtenidos de Contrupro

Nota: valores indicados son valores netos.

5.2.1.2 Costos Totales del Proyecto

Los costos totales del proyecto fueron definidos en el punto “5.1.5 Costo total del proyecto” entregando un monto total de $ 43.740.780 para su implementación.

5.2.1.3 Cálculo de indicadores

Se procede a calcular la relación Costo-Beneficio y la Ganancia Total Neta para el primer año de operación.

- **Relación Costo-Beneficio (CB):**

  CB= Costos Totales / Beneficios Totales= $43.740.780 / $34.000.000 = 0,78

- **Ganancia Total Neta (GTN):**

  GTN = Beneficios Totales − Costos Totales = $34.000.000 − $43.740.780 = −$9.740.780

El análisis financiero para el primer año de implementación indica que el proyecto no alcanza el punto de equilibrio, con una relación costo-beneficio de 0,78 y una ganancia neta negativa de $9.740.780. Sin embargo, esta perspectiva a corto plazo no captura el valor estratégico de la inversión. Es importante mencionar que en el cálculo de estos indicadores solo se consideró un incidente anual**,** compuesto por las tres amenazas principales identificadas en el proyecto: la suplantación de identidad para desviar pagos, la recepción de comprobantes de pago falsificados y el robo de información sensible a través de correos

fraudulentos. Aunque se ha asumido un único incidente a lo largo del año, es posible que estas amenazas se presenten en momentos diferentes, lo que podría aumentar el impacto financiero y reputacional.

Cabe resaltar que la seguridad no siempre genera retornos inmediatos, ya que su efectividad se mide principalmente por la cantidad de incidentes que previene y el impacto que tiene sobre la empresa cuando esos incidentes son evitados. Si bien los indicadores financieros pueden ser negativos a corto plazo, esto se debe a que la seguridad actúa como una medida preventiva y, en muchos casos, no se percibe un retorno directo hasta que ocurre un incidente importante. Por lo tanto, la implementación de esta solución de seguridad debe evaluarse no solo por las pérdidas recurrentes que evita, sino como una póliza de seguro esencial contra un incidente de alto impacto que podría generar un daño financiero y reputacional mucho superior al costo total del proyecto. Así, aunque los indicadores no muestren un retorno positivo inmediato, la implementación se justifica plenamente como una medida de protección fundamental para la continuidad y viabilidad del negocio a largo plazo, cuyo verdadero valor se explorará en la siguiente sección sobre beneficios no económicos.

5.3 Beneficios no económicos

Más allá del retorno financiero directo, la implementación de la plataforma de seguridad y el programa de concientización genera una serie de beneficios intangibles que son cruciales para la sostenibilidad, resiliencia y el éxito a largo plazo de la empresa. A diferencia de los costos evitados, estos beneficios no se reflejan directamente en un estado financiero, pero impactan positivamente en la reputación, la cultura interna y la continuidad del negocio.

A continuación, se detallan los principales beneficios no económicos del proyecto:

- **Fortalecimiento de la Confianza de Clientes y Socios Comerciales:** La confianza es un activo fundamental en el sector inmobiliario, que se distingue por la administración de información delicada y la realización de

operaciones de alto valor. Al implementar una solución robusta que protege activamente las comunicaciones y previene fraudes, la empresa proyecta una imagen de fiabilidad y profesionalismo. Esto fortalece las relaciones existentes y facilita la captación de nuevos clientes que valoran la seguridad.

- **Mejora de la Reputación de la Marca:** Un solo incidente de seguridad, como una fuga de datos de clientes o un fraude exitoso, puede causar daños irreparables al prestigio de la organización. La inversión en ciberseguridad actúa como un escudo protector para la reputación de la marca, posicionando a la empresa como una entidad seria y comprometida con la protección de la información de sus clientes.
- **Incremento de la Cultura de Ciberseguridad Interna:** Uno de los pilares del proyecto es el componente de concientización, diseñado explícitamente para impulsar un cambio cultural en la organización. Al capacitar de forma continua a los empleados, estos dejan de ser un posible vector de ataque para convertirse en una línea activa de defensa. Se fomenta un ambiente de trabajo donde la seguridad es una responsabilidad compartida, reduciendo la probabilidad de errores humanos.
- **Garantía de la Continuidad Operativa:** Los ciberataques no solo generan pérdidas económicas, sino que también pueden interrumpir los procesos críticos del negocio. Al neutralizar amenazas como el phishing y el malware antes de que alcancen a los usuarios, se asegura que los procesos de gestión comercial, técnica y logística no se vean afectados. Esto garantiza que la empresa pueda operar sin interrupciones, manteniendo su productividad y cumpliendo con los plazos de entrega prometidos a los clientes.
- **Protección de la Propiedad Intelectual e Información Sensible:** La empresa maneja información de alto valor cuya pérdida o filtración podría ser perjudicial, como contratos, planos de edificación y datos personales

de los clientes. La plataforma de seguridad protege estos activos digitales contra el robo o la exposición no autorizada, salvaguardando la ventaja competitiva de la empresa y evitando posibles consecuencias legales derivadas de una brecha de datos.

6 Conclusión

El desarrollo del proyecto permitió abordar de manera integral los retos de seguridad del correo electrónico en la empresa ContruPro, resultando en una propuesta robusta que resuelve las vulnerabilidades detectadas en sus sistemas de comunicación. Se realizó un diagnóstico exhaustivo de la organización, describiendo su estructura organizacional y analizando los tres macroprocesos de negocio: Gestión Comercial, Gestión Técnica y Producción, y Logística y Entrega. Este análisis reveló que el correo electrónico es una herramienta crítica para la comunicación interna y externa, lo que lo convierte en un punto de vulnerabilidad que requiere atención inmediata.

La evaluación del nivel de seguridad evidenció la falta de controles técnicos avanzados y protocolos administrativos para el manejo seguro de la información sensible. Este diagnóstico inicial fue fundamental para comprender las debilidades operativas existentes, lo que permitió sentar las bases para el desarrollo de soluciones efectivas que protegerían a la empresa ante las amenazas cibernéticas.

Además, se llevó a cabo un análisis de las amenazas cibernéticas que afectan al sector inmobiliario, basado en informes de empresas especializadas como Proofpoint, Cisco y Verizon, los cuales confirmaron que el correo electrónico es uno de los vectores de ataque más comunes, con el phishing y la suplantación de identidad como las técnicas más prevalentes. Este análisis permitió contextualizar los riesgos dentro de ContruPro, proporcionando información clave sobre las amenazas externas a las que se enfrenta la empresa.

El diagnóstico detallado de la organización reveló causas raíz relacionadas con la vulnerabilidad del correo electrónico, lo que permitió clasificar los riesgos detectados y cuantificar su probabilidad e impacto. Se concluyó que la suplantación de identidad y el uso de comprobantes falsificados representaban un riesgo alto para el negocio, lo que subrayó la necesidad urgente de implementar controles específicos para proteger la comunicación por correo electrónico.

A lo largo del proyecto, se definieron los requisitos funcionales y no funcionales de una plataforma de seguridad de correo electrónico adaptada al rubro inmobiliario. La selección de Proofpoint en su modalidad cloud (SaaS) fue una decisión acertada, ya que cumplió con todos los requisitos técnicos y permitió una integración sencilla con la infraestructura local. Esta plataforma no solo brindó protección avanzada contra amenazas, sino que también incluyó un componente de concientización, que fue clave para abordar los problemas relacionados con el factor humano.

El componente de concientización diseñado incluyó módulos interactivos, guías rápidas, infografías y videos educativos para sensibilizar al personal sobre las amenazas cibernéticas más comunes, como el phishing y la suplantación de identidad. Se utilizó incidentes reales bloqueados como parte del contenido educativo para maximizar el impacto de la capacitación. Además, se implementaron campañas de phishing simulado, las cuales permitieron medir la efectividad de las capacitaciones y establecer una métrica base del nivel de riesgo en la organización.

Por último, se realizó una estimación detallada de los costos de implementación de la plataforma de seguridad de correo electrónico, considerando tanto los costos fijos como los variables. Este análisis económico proporcionó la base necesaria para justificar la inversión en la propuesta, demostrando que los beneficios a largo plazo superan los costos iniciales. Así, el proyecto no solo respondió a una necesidad técnica, sino que también protege la continuidad operativa de la empresa, su reputación y fortalece la confianza de sus clientes.

En resumen, el proyecto cumplió con los objetivos planteados, entregando una solución integral que mejora la seguridad del correo electrónico y establece una cultura de seguridad sostenible dentro de la organización. Este trabajo subraya el papel fundamental del Ingeniero en Ciberseguridad como líder en la creación de estrategias que protejan la información crítica y fortalezcan la confianza del mercado hacia la empresa.

Webgrafia

Cameron, S. (2024, 3 septiembre). *What is real estate investment trust (REIT) fraud?* ComplyAdvantage. https://complyadvantage.com/insights/real-estate-investment-trust-fraud/

Cybersecurity Report series. (2025, 18 junio). Cisco. https://www.cisco.com/c/en/us/products/security/cybersecurity-reports.html#~newest-reports

The Human Factor 2025: Vol. 1 Social Engineering | ProofPoint US. (2025, 29 mayo). Proofpoint. https://www.proofpoint.com/us/resources/threat-reports/human-factor-social-engineering

Verizon Business. (s. f.). Verizon Business. https://www.verizon.com/business/resources/reports/2025-dbir-data-breach-investigations-report.pdf

Kontseva, L. (2025, 10 julio). Proofpoint Pricing 2025: Ultimate Guide for Security Products. UnderDefense. https://underdefense.com/industry-pricings/proofpoint-pricing

ProofPoint Security Awareness Training Pricing | Constant Edge. (s. f.). https://www.constantedge.com/products/proofpoint-security-awareness-training/pricing

Proofpoint Security Awareness-1 Year-Education Training for E-Mail Threat Protection-Subscription License-1-500 Licenses - CH-B-WENT-S-A-101 - E-mail - CDW.com. (s. f.). CDW.com. https://www.cdw.com/product/proofpoint-security-awareness-psat-1-year-enterprise-vr.2-1-500-users/7551864

Sherweb. (2021, 18 mayo). Proofpoint - Pricing & plans | Sherweb. https://www.sherweb.com/security/proofpoint/pricing

Anexos

Anexo 1: “Formato cronograma maestro”

Nombre del Proyecto: [Nombre del Proyecto]

Jefe de Proyecto: [Nombre del responsable]

Fecha de Elaboración: [DD/MM/AAAA]

Fase 1: [Nombre de la Fase de Planificación Inicial]

- **1.1 Actividad:** [Descripción de la primera actividad, ej. "Constitución del equipo del proyecto"]
    - **Responsable:** [Rol del responsable, ej. "jefe de Proyecto"]
    - **Fechas Previstas:** [Fecha de Inicio] – [Fecha de Fin]
    - **Duración Estimada:** [Número] días
    - **Entregable:** [Resultado de la actividad, ej. "Acta de constitución del proyecto"]
- **1.2 Actividad:** [Descripción de la segunda actividad, ej. "Desarrollo del Plan de Gestión"]
    - **Responsable:** [Rol del responsable]
    - **Fechas Previstas:** [Fecha de Inicio] – [Fecha de Fin]
    - **Duración Estimada:** [Número] días
    - **Entregable:** [Resultado de la actividad, ej. "Documento del Plan de Gestión del Proyecto"]

Fase 2: [Nombre de la Fase de Investigación y Diseño]

- **2.1 Actividad:** [Descripción de la actividad]
    - **Responsable:** [Rol del responsable]

    - **Fechas Previstas:** [Fecha de Inicio] – [Fecha de Fin]
    - **Duración Estimada:** [Número] días
    - **Entregable:** [Resultado de la actividad]
- **2.2 Actividad:** [Descripción de la actividad]
    - **Responsable:** [Rol del responsable]
    - **Fechas Previstas:** [Fecha de Inicio] – [Fecha de Fin]
    - **Duración Estimada:** [Número] días
    - **Entregable:** [Resultado de la actividad]

Fase N: [Nombre de la Fase de Cierre]

- **N.1 Actividad:** [Descripción de la actividad final, ej. "Elaboración del informe de cierre"]
    - **Responsable:** [Rol del responsable]
    - **Fechas Previstas:** [Fecha de Inicio] – [Fecha de Fin]
    - **Duración Estimada:** [Número] días
    - **Entregable:** [Resultado de la actividad, ej. "Informe Final y Lecciones Aprendidas"]