PLANEACIÓN DE LA EJECUCIÓN DEL PROYECTO DE CIBERSEGURIDAD PARA LA EMPRESA LAGOBO DISTRIBUCIONES S. A. S.

ALEXANDER FRANCO MURCIA

Trabajo de grado para optar al título de magíster en Gerencia de Proyectos

Asesor

José Mauricio Tobar Guinand

UNIVERSIDAD EAFIT

ESCUELA DE ADMINISTRACIÓN

MAESTRÍA EN GERENCIA DE PROYECTOS

PEREIRA

2025

CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

Agradecimientos

Este trabajo de grado es el resultado no solo de mi esfuerzo, sino también del amor, sacrificio y apoyo incondicional de las personas que siempre han estado a mi lado. A mi esposa, quien ha sido mi pilar, brindándome su apoyo constante y comprensión. A mi hija adorada, mi mayor tesoro, por su amor y motivación, que me impulsan a seguir adelante.

A mis padres, cuyo sacrificio, esfuerzo y amor me han permitido llegar hasta aquí. Gracias por su incansable apoyo, por enseñarme a través de su ejemplo la importancia del trabajo arduo y la perseverancia, y por estar siempre a mi lado, brindándome su respaldo en cada etapa de este camino.

A mi hermana y mi sobrina, quienes siempre han sido una fuente constante de apoyo, amor y fortaleza. Gracias a las dos por estar siempre a mi lado, brindándome su amor y motivación.

A cada uno de ustedes, mi más profundo agradecimiento. Este logro es un reflejo de todo lo que me han dado y de la confianza que siempre han depositado en mí. Este trabajo es tan suyo como mío.

RESUMEN

Este trabajo de grado se enfoca en la planeación de la ejecución de un proyecto de ciberseguridad en Lagobo Distribuciones S. A. S., siguiendo el marco de planificación de la Guía PMBOK. Se estructuran las fases del proyecto de manera secuencial, con ello, se busca fortalecer la resiliencia de la empresa ante amenazas cibernéticas, cumplir con normativas vigentes como la NTC 27001 y promover una cultura organizacional consciente en ciberseguridad. A través de una metodología estructurada, se realizarán fases de diagnóstico, diseño, implementación y mejora continua. La estructuración del presupuesto garantiza una asignación eficiente de recursos. La propuesta se enfoca en la creciente relevancia de la ciberseguridad en contextos corporativos, asegurando la protección de datos y activos críticos.

Palabras clave: ciberseguridad, ISO 27001, planificación, resiliencia.

ABSTRACT

This thesis focuses on planning the execution of a cybersecurity project at Lagobo Distribuciones S. A. S., following the planning framework of the PMBOK Guide. The project phases are structured sequentially, seeking to strengthen the company's resilience to cyber threats, comply with current regulations such as NTC 27001, and promote a cybersecurity-conscious organizational culture. A structured methodology will be used to conduct diagnostic, design, implementation, and continuous improvement phases. Budget structuring ensures efficient resource allocation. The proposal focuses on the growing relevance of cybersecurity in corporate contexts, ensuring the protection of critical data and assets.

Keywords: cybersecurity, ISO 27001, planning, resilience.

1. INTRODUCCIÓN

El presente trabajo de grado introduce un proyecto integral de ciberseguridad para Lagobo Distribuciones S. A. S. El propósito es consolidar la capacidad de la empresa para enfrentar desafíos provenientes de amenazas cibernéticas, cumplir con normativas y cultivar una cultura organizacional consciente en seguridad informática. La justificación radica en la creciente importancia de la ciberseguridad en el ámbito empresarial para proteger activos y datos sensibles. La metodología abarca diagnóstico, diseño, implementación y mejora continua. Este documento se organiza en varias secciones: primero, se presenta el contexto y la justificación del proyecto; luego, se exponen los objetivos generales y específicos, seguidos de un marco teórico que sustenta las soluciones propuestas. Posteriormente, se detalla la metodología empleada, abarcando los procesos de planificación, integración y gestión de riesgos. Finalmente, se ofrecen conclusiones y recomendaciones para asegurar la efectividad y evolución constante de las medidas de ciberseguridad implementadas, proporcionando una guía clara y detallada para la ejecución del proyecto.

2. MARCO DE REFERENCIA Y CONTEXTO ORGANIZACIONAL

2.1 Información general de la compañía

2.1.1 Antecedentes

Lagobo Distribuciones S. A. S. se fundó con el propósito de satisfacer la creciente demanda de productos tecnológicos, electrodomésticos y muebles en el mercado colombiano. Desde su creación, la empresa ha evolucionado y expandido su operación para convertirse en un actor relevante en la industria de distribución y comercialización de bienes de consumo duradero a nivel nacional.

2.1.2 Fundación y primeros años

La empresa comenzó sus operaciones en 1992 en la ciudad de Pereira, enfocándose inicialmente en la comercialización de electrodomésticos y muebles. En sus primeros años, Lagobo Distribuciones se destacó por ofrecer productos de calidad a precios competitivos, lo que le permitió ganar una sólida base de clientes. A medida que crecía la demanda, la empresa expandió su portafolio de productos, incluyendo equipos de cómputo y tecnología, alineándose con las tendencias del mercado y las necesidades de los consumidores.

2.1.3 Expansión a nivel nacional

Con el éxito de sus operaciones locales, Lagobo Distribuciones S. A. S. implementó una estrategia de crecimiento que incluyó la apertura de nuevos almacenes en diferentes ciudades del país. Hoy en día, la empresa cuenta con 27 almacenes a nivel nacional, lo que le permite tener una amplia cobertura geográfica y satisfacer las necesidades de clientes en distintas regiones de Colombia.

La expansión ha sido impulsada por la visión de la empresa de llevar soluciones tecnológicas y productos de consumo a una mayor cantidad de personas, manteniendo siempre un enfoque en la calidad del servicio al cliente. Cada nuevo almacén ha sido un punto clave para consolidar la presencia de la marca y ampliar su participación en el mercado.

2.1.4 Evolución tecnológica y digitalización

A lo largo de los años, Lagobo Distribuciones ha adoptado nuevas tecnologías para optimizar sus procesos operativos y mejorar la experiencia del cliente. En los últimos años, la empresa ha invertido en la implementación de su sistema ERP Siesa Enterprise, que ha permitido una mejor gestión de sus operaciones comerciales, contables y financieras. Asimismo, el uso de un CRM ha sido fundamental para mejorar la relación con los clientes y aumentar la eficiencia de las operaciones de ventas.

Además, la empresa ha desarrollado su presencia digital, ofreciendo a los clientes la posibilidad de realizar compras en línea a través de su plataforma de comercio electrónico, lo que ha aumentado las ventas y ampliado la base de clientes más allá de los canales tradicionales.

2.1.5 Consolidación y futuro

Hoy, Lagobo Distribuciones S. A. S. es reconocida como una empresa líder en el sector de la comercialización de electrodomésticos, muebles y equipos de cómputo en Colombia. Su capacidad para adaptarse a las tendencias del mercado, invertir en tecnología y mantener altos estándares de servicio al cliente le ha permitido consolidarse en el mercado nacional.

A futuro, la empresa tiene como objetivo seguir expandiendo su red de almacenes, fortalecer su presencia en el comercio electrónico y continuar innovando en la oferta de productos y servicios. La implementación de proyectos de ciberseguridad y la adopción de tecnologías emergentes son pilares clave en la estrategia de crecimiento sostenible de la organización.

2.1.6 Descripción

Lagobo Distribuciones S. A. S. es una empresa constituida legalmente mediante escritura pública nro. 1450 de la Notaría Cuarta de Pereira, y transformada de LTDA a S.A. mediante escritura pública nro. 2818 de julio 16 de 2002.

2.1.7 Denominación social

- Nombre de la empresa: Lagobo Distribuciones S. A. S.
- Tipo de empresa: Sociedad por Acciones Simplificada (S. A. S.).
- Fecha de constitución: 22 de julio de 1991.
- Número de Identificación Tributaria (NIT): 800135342-6.

2.1.8 Objeto social

El objeto principal de Lagobo Distribuciones S. A. S. es la comercialización de electrodomésticos, muebles y computadores en general. Esto incluye la compra, venta, distribución y comercialización de dichos productos a nivel nacional, tanto al por mayor como al detal. La empresa busca satisfacer las necesidades del mercado en cuanto a productos tecnológicos y de consumo para el hogar, ofreciendo soluciones que combinen calidad, funcionalidad y precio competitivo.

Este objeto social le permite a Lagobo Distribuciones S. A. S. participar activamente en la industria de bienes de consumo duraderos y tecnología, manteniendo una amplia gama de productos que van desde electrodomésticos básicos para el hogar hasta equipos informáticos de última tecnología.

2.1.9 Capital social

Lagobo Distribuciones S. A. S. se constituyó con un capital social de $8.000.000.000 Este capital está dividido en 800.000 acciones ordinarias, con un valor nominal de $10.000 cada una.

El capital social está destinado a soportar las operaciones iniciales de la compañía, así como a servir de base para futuros aumentos de capital en caso de ampliación de la actividad comercial. Las acciones son de libre negociación entre los socios, conforme a los estatutos sociales de la empresa

2.1.10 Representante legal

El representante legal de Lagobo Distribuciones S. A. S. es el Sr. José Alejandro Gómez Álvarez. Como representante legal, tiene la facultad de actuar en nombre de la empresa, firmar contratos, tomar decisiones operativas y estratégicas, y representar los intereses de la compañía ante autoridades gubernamentales y terceros.

El representante legal está facultado para ejercer todas las acciones necesarias en el desarrollo del objeto social de la empresa, de conformidad con lo dispuesto en los estatutos y la normatividad vigente, bajo las regulaciones de la Ley 1258 de 2008 (República de Colombia, 2008), para las Sociedades por Acciones Simplificadas (S. A. S.).

2.1.11 Registro mercantil

Lagobo Distribuciones S. A. S. está inscrita en la Cámara de Comercio de Pereira bajo el número de Matrícula Mercantil 6416404 otorgado el Julio 22 de 1991, con un activo total de $102.652.577.266, grupo NIIF II.

2.1.12 Sede y domicilio

La sede principal de Lagobo Distribuciones S. A. S. se encuentra ubicada en la carrera 8 nro. 20-53 en la ciudad de Pereira, Risaralda. Este es el domicilio legal donde la empresa lleva a cabo sus operaciones administrativas y comerciales. Desde esta ubicación, la compañía gestiona su operación comercial, centrada en la distribución y venta de electrodomésticos, muebles y equipos de cómputo en general. El domicilio principal de la empresa es también el lugar desde el cual se canalizan las decisiones estratégicas y donde se encuentra su equipo directivo y administrativo.

2.1.13 Normatividad aplicable

- Lagobo Distribuciones S. A. S. opera bajo la normatividad vigente en Colombia, regulada principalmente por las siguientes leyes y disposiciones:
- Ley 1258 de 2008 – Sociedades por Acciones Simplificadas (S. A. S.): esta ley regula la constitución, operación y disolución de las Sociedades por Acciones

Simplificadas en Colombia. Lagobo Distribuciones S. A. S. se constituyó conforme a esta ley, la cual ofrece flexibilidad en la administración y permite una estructura societaria más ágil. Entre los aspectos clave de esta ley se encuentran:

- La posibilidad de constituir la sociedad con un solo accionista.
- La facilidad para establecer el capital social sin la necesidad de desembolsarlo totalmente al momento de la constitución.
- La simplificación en los trámites de administración y gestión interna de la sociedad.
- Código de Comercio Colombiano (Decreto 410 de 1971) (República de Colombia, 1971): este código regula las actividades comerciales en Colombia, incluyendo la constitución y operación de empresas. Lagobo Distribuciones S. A. S., en tanto que sociedad dedicada a la comercialización de electrodomésticos, muebles y equipos de cómputo, se encuentra sujeta a las disposiciones generales del Código de Comercio en lo referente a sus relaciones comerciales, contratos y derechos de los consumidores.
- Ley 222 de 1995 – Régimen de Sociedades Comerciales (República de Colombia, 1995): aunque la Ley 1258 es la norma específica para las S. A. S., la Ley 222 también aplica en lo relacionado con aspectos de insolvencia, reorganización empresarial y disolución de sociedades.
- Normas tributarias: la empresa debe cumplir con las obligaciones fiscales impuestas por la DIAN (Dirección de Impuestos y Aduanas Nacionales). Esto incluye la declaración y pago de impuestos como el IVA (Impuesto al Valor Agregado), el impuesto de renta y complementarios, así como las retenciones en la fuente aplicables según la actividad comercial de la compañía.
- Normatividad en protección de datos personales (Ley 1581 de 2012): dado que la empresa realiza operaciones comerciales y maneja datos de clientes, está sujeta a las disposiciones de la Ley 1581 de 2012 (República de Colombia, 2012), que establece normas sobre la protección de datos personales. Lagobo Distribuciones

S. A. S. debe implementar políticas y medidas de seguridad que garanticen la confidencialidad y el correcto manejo de la información personal que recopila.

- Normas laborales: la empresa debe cumplir con las disposiciones laborales colombianas establecidas en el Código Sustantivo del Trabajo, en lo relacionado con la contratación de personal, salarios, seguridad social y protección a los derechos de los trabajadores.
- Lagobo Distribuciones S. A. S. se constituyó por tiempo indefinido, según lo estipulado en los estatutos sociales. Esto significa que la sociedad continuará existiendo mientras los accionistas así lo deseen y no se presente ninguna causa de disolución anticipada conforme a lo establecido en la Ley 1258 de 2008 o en los estatutos internos de la compañía.
- La empresa podrá ser disuelta de manera anticipada en caso de que ocurra alguna de las causales establecidas en la ley, como la imposibilidad de cumplir su objeto social, la pérdida del capital social o por decisión de los accionistas en asamblea general.

2.1.14 Quiénes somos

Lagobo nació en el año de 1969 en Pereira con su cadena de almacenes dedicados a la venta de electrodomésticos y muebles para el hogar bajo la marca Almacenes Oportunidades®.

Gracias a su trayectoria y experiencia, hoy en día es una de las empresas líderes en el sector de electrodomésticos y tecnología en Colombia, que ofrece líneas de crédito de consumo, libranza y empresarial.

En 1972 nace la unidad de negocio dedicada a las ventas al por mayor con cubrimiento nacional, convirtiéndose rápidamente en uno de los mayoristas más grandes de Colombia.

Desde 2010, Lagobo Distribuciones S.A., con su marca Oportunidades.com.co, empieza a comercializar a través de su tienda virtual, electrodomésticos, tecnología, sonido, colchones, electrohogar, refrigeración, lavado y secado, entre otras líneas de

hogar de las mejores marcas del mercado, ofreciendo excelente calidad a muy buenos precios.

En más de 50 años de trayectoria, hemos logrado posicionarnos como líderes del sector en Colombia. Estamos en más de 30 ciudades del país con más de 50 puntos de atención al público y cientos de clientes que han vivido la experiencia de adquirir sus productos con nosotros.

2.1.15 Misión

Satisfacer las necesidades de nuestros clientes a través de la comercialización y distribución de soluciones para el hogar en electrodomésticos, gasodomésticos, muebles, tecnologías y servicios financieros, mediante experiencias positivas por medio de un excelente servicio, calidad e innovación en nuestros productos, mejorando continuamente los procesos e integrando políticas de sostenibilidad ambiental, apoyados por un talento humano capacitado y motivado.

2.1.16 Visión

Continuar siendo en el 2025 una empresa reconocida en la comercialización y distribución de electrodomésticos, gasodomésticos, muebles, tecnologías y servicios financieros, fortalecida como líder a nivel nacional que se caracterice por la excelencia del servicio, la óptima calidad e innovación de los productos que ofrecemos a nuestros clientes, fomentando constantemente políticas medioambientales que contribuyan al desarrollo sostenible y bienestar de todos nuestros colaboradores. Adicional, la compañía busca mejorar constantemente su portafolio de servicios financieros, así como su canal de proyectos y nuevos negocios, también consolidar su actividad comercial ampliando su cobertura a nivel nacional

2.1.17 Política de calidad

Lagobo Distribuciones S. A. S. está enfocada en satisfacer las necesidades y expectativas de sus clientes, mediante la comercialización y distribución de su portafolio de bienes y servicios, procurando el cumplimiento de las especificaciones de todos sus productos en funcionalidad, diseño y calidad; así como los requisitos legales aplicables,

a través de un equipo de talento humano competente que orienta a sus aliados a tomar la mejor decisión. Todas las actividades, resultados y metas están basados y controlados por el Sistema de Gestión de Calidad que promueve constantemente la mejora continua.

2.1.18 Política de servicio al cliente

Estamos comprometidos a brindar una atención al cliente de manera personalizada, escuchamos activamente las necesidades de los consumidores y brindamos soluciones adaptadas a cada situación. Nuestro personal recibe formación continua sobre habilidades de comunicación, resolución de problemas y conocimiento de productos, garantizando así una atención eficaz a las expectativas de nuestros clientes.

2.2 Análisis estratégico de Lagobo Distribuciones S. A. S.

2.2.1 Análisis FODA

Fortalezas

- Presencia nacional: Lagobo Distribuciones S. A. S. cuenta con 27 almacenes a nivel nacional, lo que le permite una cobertura extensa y una cercanía con el consumidor final en diferentes regiones del país.
- Variedad de productos: la empresa ofrece una amplia gama de productos que incluye electrodomésticos, muebles y equipos de cómputo, lo que diversifica sus ingresos y la hace atractiva para diferentes segmentos de clientes.
- Uso de sistemas de gestión: la implementación de un ERP como Siesa Enterprise y un CRM robusto le permite gestionar eficientemente sus operaciones y relaciones con los clientes, lo que brinda ventajas operativas en términos de control, eficiencia y calidad del servicio.
- Cultura organizacional: la empresa promueve una cultura de servicio al cliente, lo que se traduce en altos niveles de satisfacción del cliente y fidelización.
- Personal capacitado: la estructura de personal, con aproximadamente siete empleados por almacén, garantiza un equilibrio adecuado entre la atención al cliente y la eficiencia operativa.

Oportunidades

- Crecimiento del comercio electrónico: el aumento de la compra en línea ofrece una excelente oportunidad para que Lagobo Distribuciones refuerce su canal de ventas digitales y amplíe su base de clientes, más allá de las limitaciones geográficas.
- Adopción de nuevas tecnologías: la implementación de tecnologías emergentes, como la inteligencia artificial y la automatización, puede optimizar aún más los procesos de gestión y logística y, de esta manera, reducir costos y mejorar la precisión.
- Expansión a nuevas regiones: existen oportunidades de expansión a regiones no cubiertas en Colombia, lo que permitiría a la empresa aumentar su participación en el mercado nacional.
- Alianzas estratégicas: colaborar con otros distribuidores o fabricantes podría reducir costos y aumentar la variedad de productos ofrecidos.

Debilidades

- Dependencia de canales tradicionales: aunque la empresa tiene una buena presencia física, su canal de ventas digitales aún no está plenamente desarrollado en comparación con competidores que se enfocan más en el comercio electrónico.
- Falta de internacionalización: a pesar de su éxito a nivel nacional, la empresa no ha explorado oportunidades internacionales, lo que limita su crecimiento en mercados globales.
- Riesgos en la cadena de suministro: cualquier interrupción en la cadena de suministro puede afectar la disponibilidad de productos, especialmente en un entorno postpandemia y de crisis logística global.
- Alta competencia: el mercado de la distribución de electrodomésticos y productos tecnológicos es altamente competitivo, con grandes jugadores nacionales e internacionales que pueden ejercer presión sobre los precios.

Amenazas

- Ciberseguridad: el creciente riesgo de ataques cibernéticos puede amenazar las operaciones de la empresa, especialmente a medida que aumenta su presencia digital. La falta de medidas robustas de ciberseguridad puede comprometer datos sensibles y operaciones comerciales.
- Cambios en la regulación: modificaciones en la legislación, como impuestos a las importaciones o nuevas normativas laborales, pueden aumentar los costos operativos.
- Inflación y fluctuaciones cambiarias: las fluctuaciones económicas, como la inflación y los cambios en el valor del peso colombiano frente a otras monedas, pueden afectar los costos de importación de los productos.
- Competencia de grandes plataformas de comercio electrónico: empresas globales y plataformas como Amazon o MercadoLibre continúan expandiéndose en Colombia, lo que puede ejercer una presión adicional sobre los márgenes de ganancia de la empresa.

Análisis interno: factores clave

Capacidades operativas

La empresa tiene una estructura operativa sólida con sistemas de gestión bien implementados. Sin embargo, existen áreas que necesitan optimización, como la gestión de inventarios en tiempo real y la expansión del comercio electrónico.

Recursos humanos

Los empleados en cada almacén están bien capacitados y desempeñan funciones clave en la atención al cliente. El equipo de gestión, liderado por directores de almacén, garantiza la eficiencia operativa a nivel local, mientras que el personal administrativo gestiona las operaciones generales desde la sede principal.

Cultura organizacional

La cultura de servicio al cliente es uno de los puntos fuertes de la empresa, lo que ha generado un alto nivel de lealtad por parte de los clientes. Sin embargo, la cultura

puede adaptarse aún más hacia la innovación y la agilidad en respuesta a los cambios tecnológicos y las tendencias del mercado.

2.2.2 Análisis externo: factores de entorno

Entorno económico

La economía colombiana enfrenta retos importantes debido a la inflación y la incertidumbre en los mercados globales. Estos factores afectan la capacidad de compra de los consumidores y pueden influir en las ventas de productos de consumo duradero, como electrodomésticos y tecnología.

Entorno tecnológico

El entorno tecnológico está evolucionando rápidamente, con nuevas tendencias que van desde la inteligencia artificial hasta la automatización de procesos. Lagobo Distribuciones S. A. S. debe mantenerse a la vanguardia en el uso de estas tecnologías para seguir siendo competitiva.

Entorno competitivo

El sector de distribución de productos tecnológicos y electrodomésticos es altamente competitivo. Empresas nacionales e internacionales están constantemente innovando en la oferta de productos y en las estrategias de venta, tanto físicas como en línea.

2.2.3 Estrategias recomendadas

Con base en el análisis FODA y los factores internos y externos, Lagobo Distribuciones S. A. S. podría considerar las siguientes estrategias:

- Fortalecer el comercio electrónico mediante una mayor inversión en plataformas digitales y marketing online.
- Optimizar la cadena de suministro para reducir costos y mejorar la disponibilidad de productos.
- Desarrollar un plan de ciberseguridad sólido para mitigar los riesgos asociados con su creciente presencia digital.

- Expandir la presencia nacional con más almacenes en zonas no cubiertas y explorar posibles alianzas estratégicas para aumentar la competitividad.

2.2.4 Políticas de Lagobo distribuciones S. A. S.

Política de calidad y servicio al cliente

Lagobo Distribuciones S. A. S. se compromete a ofrecer productos de alta calidad en las áreas de electrodomésticos, muebles y equipos de cómputo, garantizando que cumplan con las expectativas de los clientes. La empresa mantiene altos estándares de servicio al cliente, asegurando una atención personalizada y eficiente, tanto en las tiendas físicas como en los canales de venta *online*.

Objetivo: asegurar la satisfacción del cliente mediante productos y servicios de calidad.

Aplicación: todos los empleados en contacto con el cliente, tanto en ventas como en servicio postventa, deben adherirse a esta política, asegurando una atención amable, informada y rápida.

Política de recursos humanos

La empresa valora el desarrollo de su talento humano y promueve un ambiente de trabajo positivo, basado en el respeto, la colaboración y el crecimiento profesional. Lagobo Distribuciones S. A. S. se compromete a ofrecer capacitación continua a sus empleados y fomentar su bienestar mediante programas de motivación y políticas de seguridad laboral.

Objetivo: mantener un equipo motivado y capacitado para cumplir los objetivos de la empresa.

Aplicación: a todos los niveles de la organización, con especial enfoque en el personal de ventas y gerentes de almacén.

Política de innovación tecnológica

Lagobo Distribuciones S. A. S. promueve el uso de tecnologías avanzadas para mejorar la eficiencia operativa y la experiencia del cliente. Esto incluye la inversión en

sistemas de gestión como el ERP Siesa Enterprise y el CRM, así como en plataformas de comercio electrónico para incrementar las ventas digitales.

Objetivo: mejorar los procesos internos y la relación con los clientes mediante la adopción de tecnologías innovadoras.

Aplicación: departamento de tecnología, ventas y operaciones, con miras a optimizar la experiencia del cliente y aumentar la eficiencia operativa.

Política de ciberseguridad

En el marco de su expansión digital, Lagobo Distribuciones S. A. S. se compromete a proteger la información de sus clientes y empleados mediante la implementación de políticas robustas de ciberseguridad. La empresa adoptará medidas preventivas para evitar ataques cibernéticos, robos de datos o cualquier otro incidente que comprometa la integridad de sus sistemas.

Objetivo: garantizar la seguridad de los datos y la continuidad operativa en el entorno digital.

Aplicación: a todo el personal que maneje sistemas de información, con especial enfoque en el departamento de tecnología y ventas en línea.

Política de sostenibilidad y responsabilidad social

Lagobo Distribuciones S. A. S. promueve prácticas de negocio responsables, orientadas a minimizar el impacto ambiental y a contribuir al desarrollo social de las comunidades en las que opera. La empresa se compromete a adoptar políticas de eficiencia energética, manejo adecuado de residuos y reciclaje de productos electrónicos.

Objetivo: contribuir a la sostenibilidad del entorno y promover prácticas responsables.

Aplicación: a nivel corporativo y en cada una de las sucursales, involucrando a los empleados en programas de reciclaje y reducción de consumo energético.

Política de comunicación interna

Lagobo Distribuciones S. A. S. promueve la comunicación clara, oportuna y efectiva entre todos los niveles de la organización. Esto incluye el uso de herramientas tecnológicas como el correo electrónico, sistemas de mensajería y reuniones periódicas para asegurar que todos los empleados estén informados sobre los objetivos, cambios y avances de la empresa.

Objetivo: facilitar la coordinación entre áreas y garantizar que todos los empleados estén alineados con los objetivos de la empresa.

Aplicación: a todos los departamentos, con especial énfasis en la coordinación entre la sede principal y los almacenes.

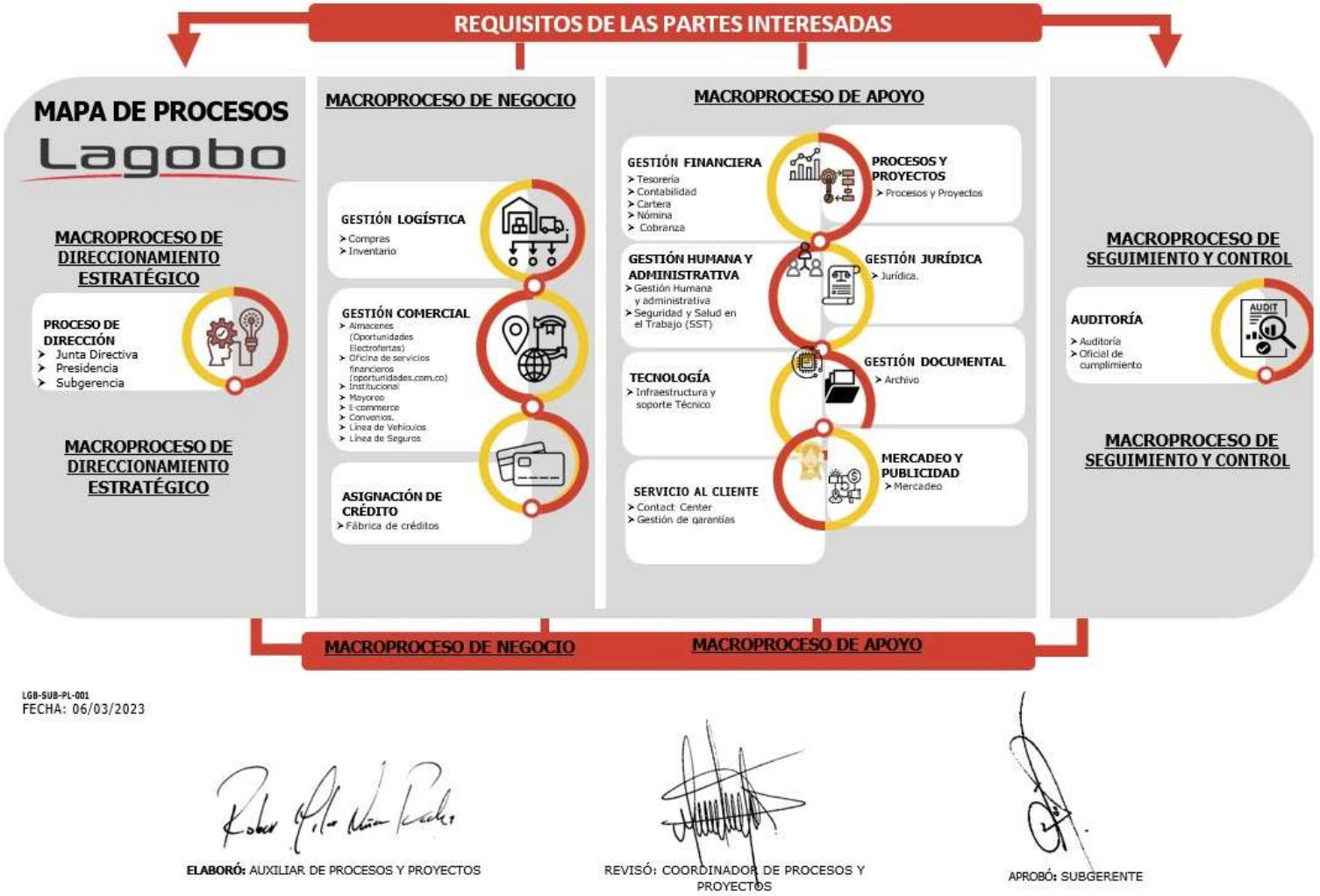
Política de cumplimiento normativo

Lagobo Distribuciones S. A. S. garantiza que todas sus operaciones se realizan de acuerdo con las normativas locales e internacionales vigentes, incluyendo aspectos fiscales, laborales y de protección al consumidor. La empresa también se adhiere estrictamente a la Ley 1581 de 2012, sobre protección de datos personales.

Objetivo: asegurar el cumplimiento legal en todas las actividades comerciales y operativas de la empresa.

Aplicación: a todos los departamentos, con un enfoque especial en las áreas de finanzas, recursos humanos y tecnología.

Figura 1. *Mapa de procesos Lagobo Distribuciones S. A. S.*



3. FUNCIONAMIENTO DE LAGOBO DISTRIBUCIONES S. A. S.

Lagobo Distribuciones S. A. S. es una empresa dedicada a la comercialización de electrodomésticos, muebles y equipos de cómputo. Su funcionamiento está basado en una estructura organizacional claramente definida, con áreas operativas y estratégicas que trabajan en conjunto para cumplir con su objeto social y satisfacer las necesidades de sus clientes.

3.1. Estructura organizacional

La empresa cuenta con una estructura jerárquica funcional, que incluye las siguientes áreas clave:

Gerencia general: encabezada por el representante legal. Esta área es responsable de la toma de decisiones estratégicas, la supervisión de las operaciones y la representación de la empresa ante las entidades reguladoras y socios comerciales.

Departamento comercial: responsable de la gestión de ventas, atención al cliente y expansión del mercado. Este departamento asegura la captación de nuevos clientes y la fidelización de los existentes mediante el manejo de promociones, políticas de precios y estrategias de ventas.

Departamento de logística y operaciones: esta área gestiona la cadena de suministro, control de inventarios, almacenamiento y distribución de productos a las sucursales o directamente a los clientes. Se encarga de coordinar las entregas a tiempo y de garantizar la disponibilidad de los productos en *stock*.

Departamento de tecnología y soporte T. I.: es el encargado de asegurar el buen funcionamiento de los sistemas informáticos y de comunicaciones de la empresa, así como de la ciberseguridad de los datos y transacciones. Además, gestiona el soporte técnico a los puntos de venta (POS) y la infraestructura digital de la compañía.

Departamento financiero y contable: administra las finanzas de la empresa, incluyendo la contabilidad, gestión de tesorería, manejo de créditos y cobros, y la presentación de informes financieros y declaraciones tributarias.

Recursos humanos: encargado de la gestión del talento humano, selección de personal, formación, bienestar laboral y cumplimiento de las normativas laborales.

3.2 Procesos operativos

Los procesos clave para el funcionamiento diario de la empresa son:

Gestión de compras y suministros: la empresa mantiene relaciones con proveedores nacionales e internacionales para garantizar el suministro constante de productos. La negociación de precios y condiciones es fundamental para asegurar la competitividad en el mercado.

Control de inventarios: se realiza un monitoreo constante del inventario mediante sistemas de gestión automatizados, lo que permite una administración eficiente y evita la falta de *stock* o el sobreabastecimiento.

Distribución: los productos son distribuidos a las diferentes sucursales o directamente a los clientes, garantizando tiempos de entrega acordes con los estándares del mercado.

Ventas y atención al cliente: la interacción con los clientes es gestionada a través de los canales de venta físicos (tiendas y sucursales) y digitales (plataforma de comercio electrónico). El servicio al cliente es una prioridad, se ofrece soporte pre y postventa para asegurar la satisfacción de los compradores.

3.3 Sistemas de información y tecnología

Lagobo Distribuciones S. A. S. ha implementado sistemas de información robustos que permiten la gestión eficiente de todas sus áreas. Estos incluyen:

ERP Siesa Enterprise: que facilita la administración de los módulos comerciales, financieros y de tesorería, así como la gestión de usuarios.

CRM (Customer Relationship Management): herramienta integrada que permite gestionar la relación con los clientes, facilitando la toma de decisiones comerciales basadas en datos.

Infraestructura de red y seguridad informática: la empresa ha implementado medidas de ciberseguridad para proteger los datos de clientes y la operación interna, lo que garantiza transacciones seguras y la protección ante amenazas digitales.

3.4 Relación con proveedores y clientes

La empresa mantiene relaciones estrechas con sus proveedores, asegurando acuerdos comerciales que le permiten ofrecer productos de calidad a precios competitivos. Asimismo, Lagobo Distribuciones S. A. S. trabaja en la construcción de relaciones duraderas con sus clientes, proporcionando atención personalizada y soluciones adaptadas a sus necesidades.

3.5 Cumplimiento normativo y responsabilidad corporativa

Lagobo Distribuciones S. A. S. opera bajo las normativas locales e internacionales aplicables a su sector, cumpliendo con las leyes comerciales, fiscales y laborales. Además, ha adoptado políticas de responsabilidad social corporativa, contribuyendo al desarrollo de las comunidades donde opera y buscando prácticas sostenibles que minimicen su impacto ambiental.

3.6 Estrategia organizacional de Lagobo Distribuciones S. A. S.

3.6.1 Expansión de mercado

Objetivo: ampliar la participación de la empresa en el mercado nacional y eventualmente explorar oportunidades internacionales.

Diversificación de productos: ampliar el portafolio de productos, añadiendo nuevas líneas tecnológicas o de electrodomésticos avanzados para diferentes segmentos de mercado (gama alta, media y baja), lo cual permitirá cubrir un rango más amplio de clientes.

Penetración en nuevos territorios: expandir la red de distribución a otras ciudades y regiones del país, abriendo sucursales o asociándose con distribuidores locales.

Estrategias de fidelización: implementar programas de fidelización para retener a los clientes, ofreciendo beneficios exclusivos como descuentos por lealtad, garantías extendidas, o promociones especiales.

3.6.2 Optimización operativa

Objetivo: mejorar la eficiencia en las operaciones para reducir costos y maximizar la rentabilidad.

Automatización de procesos: integrar herramientas tecnológicas que permitan automatizar procesos clave, como la gestión de inventarios, facturación y atención al cliente, lo que optimiza el flujo de trabajo y minimiza los errores operativos.

Gestión eficiente de la cadena de suministro: trabajar en alianzas estratégicas con proveedores para garantizar la disponibilidad continua de productos y reducir los tiempos de entrega, asegurando también mejores condiciones de negociación.

Control y reducción de costos: implementar programas de reducción de costos en áreas clave para optimizar el uso de recursos y lograr mayor eficiencia energética y operativa.

3.6.3 Transformación digital

Objetivo: adaptar a Lagobo Distribuciones S. A. S. al entorno digital para mejorar la experiencia del cliente y aumentar su competitividad.

Plataformas de comercio electrónico: crear o fortalecer un canal de ventas *online*, que permita a los clientes comprar productos de manera fácil y rápida, con opciones de entrega a domicilio y facilidades de pago en línea.

Marketing digital y *branding*: desarrollar campañas de *marketing* digital para aumentar la visibilidad de la marca en redes sociales, motores de búsqueda y plataformas de publicidad digital, adaptando las estrategias a las tendencias del consumidor.

Ciberseguridad: implementar políticas de ciberseguridad robustas para proteger los datos de la empresa y sus clientes, que garanticen un entorno seguro, tanto para las transacciones comerciales como para la gestión interna.

3.6.4 Fortalecimiento del talento humano

Objetivo: asegurar un equipo de trabajo altamente capacitado que impulse el crecimiento de la empresa.

Capacitación continua: ofrecer programas de formación continua a los empleados en áreas clave como ventas, atención al cliente, y manejo de nuevas tecnologías.

Política de bienestar laboral: promover un ambiente de trabajo saludable y motivador, que aumente la productividad y retención de talento.

3.6.5 Estrategia a largo plazo

Innovación constante: mantener un enfoque constante en la innovación de productos y servicios, evaluando las tendencias del mercado tecnológico y adaptándose rápidamente a las nuevas demandas de los consumidores.

Sostenibilidad: incorporar prácticas sostenibles y responsables que contribuyan a la eficiencia energética, la reducción del impacto ambiental y el desarrollo social.

3.7 Tamaño de la organización

Lagobo Distribuciones S. A. S. es una empresa de tamaño mediano, con una sólida presencia en el mercado colombiano. Actualmente, la compañía opera 27 almacenes a nivel nacional, estratégicamente distribuidos en diversas ciudades y regiones del país. Cada almacén está equipado para ofrecer una amplia gama de productos en las categorías de electrodomésticos, muebles y equipos de cómputo.

En términos de personal, cada almacén cuenta aproximadamente con siete empleados, conformados por:

- Cajeras: encargadas de gestionar los pagos y facturaciones.

- Director de almacén: responsable de la operación general, gestión de personal y cumplimiento de metas comerciales.
- Asesores comerciales: dedicados a la atención al cliente, venta de productos y asesoramiento sobre las soluciones más adecuadas a las necesidades del comprador.

Este equipo multidisciplinario asegura que cada almacén funcione de manera eficiente, brindando una experiencia de compra fluida y satisfactoria para los clientes. El personal se encuentra capacitado para manejar tanto las operaciones diarias del punto de venta, como para ofrecer soporte técnico básico y comercial.

Con esta estructura operativa, Lagobo Distribuciones S. A. S. garantiza una cobertura nacional robusta, lo cual hace que sus productos y servicios lleguen a diferentes mercados locales, asegurando siempre la calidad y eficiencia en cada uno de sus puntos de atención.

3.8 Portafolio de proyectos de Lagobo Distribuciones S. A. S.

a. Proyecto de expansión de almacenes

Descripción: este proyecto está enfocado en la apertura de nuevos almacenes en regiones estratégicas del país. La empresa ha identificado áreas de crecimiento potencial, como ciudades intermedias y zonas periféricas de grandes ciudades, donde existe demanda insatisfecha de productos electrónicos, muebles y electrodomésticos.

Objetivo: la meta es abrir cinco nuevos almacenes en los próximos dos años, con una inversión estratégica en infraestructura y personal capacitado. Este proyecto también incluye la selección de ubicaciones, contratación de personal y campañas de *marketing* local.

Beneficios esperados:

- Incremento en las ventas al aumentar la cobertura de mercado.
- Mayor visibilidad de marca en zonas de crecimiento.

- Fortalecimiento de la relación con los clientes, al estar más cerca de ellos geográficamente.
- Desarrollo de nuevas oportunidades de negocio en áreas que anteriormente no estaban cubiertas.

b. Proyecto de transformación digital y comercio electrónico

Descripción: en respuesta a la creciente tendencia de las compras en línea, Lagobo Distribuciones S. A. S. está trabajando en la optimización de su plataforma de comercio electrónico. El proyecto incluye la mejora de la experiencia de usuario en la página web, la integración de nuevas opciones de pago y el fortalecimiento de la logística para envíos más rápidos y eficientes.

Objetivo: aumentar las ventas digitales en un 20% en los próximos 12 meses, mediante la renovación de la plataforma de *e-commerce*, campañas de marketing digital y alianzas estratégicas con proveedores logísticos.

Beneficios esperados:

- Mejora en la experiencia de compra para los clientes, facilitando la navegación en el sitio y el proceso de pago.
- Expansión del mercado objetivo al atraer a clientes que prefieren realizar compras en línea.
- Optimización del proceso logístico para asegurar que los tiempos de entrega sean competitivos en el mercado.
- Mayor fidelización a través de una plataforma que ofrezca una experiencia personalizada y rápida.

c. Proyecto de implementación de ciberseguridad

Descripción: este proyecto surge de la creciente dependencia de la empresa en sus sistemas digitales, incluyendo su ERP, CRM y plataforma de comercio electrónico. El objetivo es proteger los datos sensibles y garantizar la continuidad operativa frente a posibles ciberataques. Incluye la instalación de soluciones de seguridad avanzada (*firewalls*, sistemas de detección de intrusos, cifrado de datos) y la capacitación continua de empleados.

Objetivo: implementar un sistema integral de ciberseguridad que proteja los activos digitales de la empresa y asegure el cumplimiento de normativas de protección de datos como la Ley 1581 de 2012.

Fases del proyecto:

Evaluación de riesgos: un análisis profundo de las vulnerabilidades en la infraestructura tecnológica.

Diseño de soluciones: identificación y adquisición de herramientas de seguridad cibernética (*firewalls*, VPN, cifrado de datos).

Implementación tecnológica: instalación y configuración de herramientas de seguridad, monitoreo en tiempo real y respuesta a incidentes.

Capacitación: formación de empleados y directivos en mejores prácticas de ciberseguridad.

Monitoreo y mejora continua: implementación de sistemas de seguimiento y actualización constante de las soluciones.

Beneficios esperados:

- Protección ante ciberataques y amenazas de seguridad.
- Cumplimiento normativo en cuanto a la gestión de datos personales y confidenciales.
- Mejora en la confianza de clientes y proveedores al garantizar que sus datos estén seguros.
- Prevención de interrupciones operativas causadas por incidentes de seguridad.

d. Proyecto de optimización de la cadena de suministro

Descripción: este proyecto está centrado en mejorar la gestión de inventarios y los procesos logísticos para reducir costos y optimizar la eficiencia operativa. Lagobo Distribuciones S. A. S. busca implementar un sistema de monitoreo de inventarios en tiempo real y fortalecer las relaciones con proveedores para garantizar entregas más rápidas y eficientes.

Objetivo: implementar un sistema automatizado de inventarios que permita un control más preciso de los productos y evitar desabastecimientos o sobreabastecimiento.

Beneficios esperados:

- Reducción de costos operativos al optimizar el almacenamiento y los procesos de distribución.
- Mejora en la disponibilidad de productos, asegurando que los artículos más demandados estén siempre en *stock*.
- Mejores condiciones con proveedores, gracias a la optimización de tiempos de entrega y pedidos más precisos.
- Mejora en la eficiencia operativa en toda la cadena de suministro.

e. Proyecto de implementación de ERP y CRM avanzados

Descripción: este proyecto busca actualizar y mejorar los sistemas de ERP Siesa Enterprise y CRM, lo que permitirá integrar mejor los procesos financieros, logísticos y de gestión de clientes en una sola plataforma. La implementación de módulos adicionales hará posible el análisis de datos en tiempo real y la automatización de procesos comerciales.

Objetivo: actualizar y expandir los sistemas de ERP y CRM para mejorar la eficiencia operativa, optimizar el manejo de inventarios, y proporcionar una experiencia más personalizada al cliente.

Beneficios esperados:

- Mejora en la toma de decisiones gracias a la disponibilidad de datos en tiempo real.
- Aumento en la eficiencia operativa, lo que se traduce en reducción de la duplicidad de tareas y la mejora de la colaboración entre departamentos.
- Personalización de la experiencia del cliente a través de un CRM mejorado, que permita una interacción más cercana y adaptada a las necesidades individuales de los clientes.

f. Proyecto de responsabilidad social y sostenibilidad

Descripción: este proyecto busca hacer que la empresa sea más sostenible, mediante la implementación de programas de reciclaje de electrodomésticos, eficiencia energética y participación en iniciativas comunitarias. El enfoque es reducir el impacto ambiental de la operación y crear un modelo de negocio más responsable.

Objetivo: desarrollar e implementar prácticas de sostenibilidad en todos los almacenes y centros de operación, con el fin de minimizar el impacto ambiental y fomentar un comportamiento corporativo responsable.

Beneficios esperados:

- Reducción del consumo energético y de recursos en los almacenes y oficinas.
- Reciclaje de productos electrónicos para minimizar los desechos electrónicos.
- Mejora en la imagen corporativa, mostrando a la empresa como un líder responsable en su industria.
- Contribución a la comunidad a través de iniciativas sociales y ambientales.

g. Proyecto de mejora del servicio al cliente

Descripción: este proyecto está enfocado en mejorar la calidad del servicio al cliente, tanto en los puntos de venta físicos como en los canales digitales. Incluye la implementación de nuevas herramientas de gestión de *feedback* y la capacitación continua de los empleados para ofrecer una experiencia de compra superior.

Objetivo: mejorar la satisfacción del cliente mediante una atención personalizada y rápida, tanto en las tiendas como en el canal de ventas en línea, y reducir el número de reclamaciones.

Beneficios esperados:

- Mayor fidelización del cliente, con un servicio más rápido y personalizado.
- Mejor percepción de la marca al ofrecer un servicio superior al de los competidores.
- Reducción en el número de reclamaciones gracias a una atención más eficiente y la resolución oportuna de problemas.
- Capacitación constante del personal, lo que incrementa su capacidad para manejar situaciones de servicio complejas.

3.9 Factores ambientales de Lagobo Distribuciones S. A. S.

Los factores ambientales de una empresa son aquellos elementos que influyen en su funcionamiento, cultura y gestión de proyectos. En el caso de Lagobo Distribuciones S. A. S., estos factores son clave para el éxito de sus operaciones y la implementación de proyectos, como el de ciberseguridad en el que estás trabajando.

3.9.1 Cultura organizacional

La cultura de Lagobo Distribuciones S. A. S. se caracteriza por su enfoque en la excelencia en el servicio al cliente y la innovación en la comercialización de productos tecnológicos y electrodomésticos. La empresa promueve una cultura de trabajo colaborativo, con una orientación hacia la resolución de problemas y el crecimiento continuo de su personal y su operación.

A nivel interno, existe un enfoque en la comunicación abierta y la toma de decisiones descentralizada, especialmente en los directores de almacenes, quienes tienen autonomía en la gestión operativa de sus puntos de venta. Además, la empresa fomenta un ambiente de responsabilidad social y sostenibilidad, asegurando prácticas éticas en sus relaciones con proveedores y clientes.

3.9.2 Recursos humanos

Los recursos humanos en Lagobo Distribuciones S. A. S. son un pilar fundamental para el éxito de la empresa. Con aproximadamente siete empleados por almacén, distribuidos entre cajeras, un director de almacén y asesores comerciales, la empresa tiene un equipo altamente comprometido con el servicio al cliente y la operación eficiente de sus tiendas.

Se implementan programas de capacitación continua para mejorar las competencias técnicas y comerciales de su personal, asegurando que estén actualizados en las últimas tendencias del mercado y en las mejores prácticas de atención al cliente. Asimismo, el departamento de Recursos Humanos se encarga de fomentar un ambiente laboral saludable, orientado a la motivación y retención de talento, con el propósito de promover el bienestar y la seguridad de sus empleados.

3.9.3 Normatividad

Como mencionamos anteriormente, Lagobo Distribuciones S. A. S. opera bajo las normativas nacionales e internacionales que rigen el comercio de bienes y la operación de Sociedades por Acciones Simplificadas (S. A. S.) en Colombia. La empresa está sujeta a la Ley 1258 de 2008, el Código de Comercio Colombiano, las normas tributarias de la DIAN, y la legislación laboral vigente.

Adicionalmente, debido a su manejo de datos personales, la empresa debe cumplir con la Ley 1581 de 2012, que regula la protección de datos personales en Colombia. Este marco normativo es crucial para garantizar el cumplimiento legal en todas las áreas operativas y de gestión de la empresa, incluidas las relacionadas con la ciberseguridad y la protección de información.

3.9.4 Sistemas de información de proyectos

La empresa utiliza el sistema ERP Siesa Enterprise, el cual integra los módulos comerciales, de contabilidad, tesorería y administración de usuarios, lo que facilita la gestión integral de los procesos operativos y financieros de la compañía. Este sistema

permite a la empresa manejar proyectos complejos, como la implementación de nuevas sucursales, control de inventarios y proyectos de mejora continua.

Además, el CRM de Siesa ayuda a gestionar la relación con los clientes y llevar un seguimiento detallado de las interacciones y transacciones realizadas, proporcionando una visión clara del comportamiento del cliente. Este sistema es un componente clave para la ejecución eficiente de proyectos relacionados con el área comercial y la expansión de mercado.

3.9.5 Canales de comunicación

La comunicación dentro de Lagobo Distribuciones S. A. S. se gestiona a través de canales formales e informales, que permiten una interacción eficiente entre los diferentes niveles de la organización. A nivel interno, la empresa utiliza:

Correo electrónico corporativo: para la comunicación formal entre almacenes, la sede principal y las áreas administrativas.

Reuniones periódicas: en los almacenes y a nivel gerencial, para coordinar estrategias y revisar el cumplimiento de metas comerciales.

Sistemas de mensajería interna: herramientas como aplicaciones de mensajería instantánea para la comunicación rápida entre empleados y gerentes.

A nivel externo, Lagobo Distribuciones S. A. S. mantiene comunicación continua con sus clientes a través de redes sociales, plataformas de comercio electrónico y un *call center*, lo que permite gestionar consultas, pedidos y servicios de manera eficiente.

4. PLANTEAMIENTO DEL PROBLEMA

En la era digital actual, la ciberseguridad se ha convertido en un elemento crítico para la estabilidad y sostenibilidad de organizaciones en todo el mundo. Con el aumento exponencial de la conectividad y la dependencia de la tecnología, las amenazas cibernéticas han evolucionado, presentando desafíos significativos para la seguridad de la información y la infraestructura tecnológica.

El crecimiento constante de ataques cibernéticos, desde intrusiones maliciosas hasta el *ransomware* y el robo de datos, ha afectado a empresas, Gobiernos y usuarios individuales (Arias, 2021). Organizaciones de todos los tamaños se enfrentan a la realidad de que la ciberdelincuencia es una amenaza omnipresente y en constante evolución, con consecuencias que van más allá de las pérdidas económicas para incluir la pérdida de confianza, la interrupción de operaciones críticas y el compromiso de la privacidad. Las regulaciones y estándares de ciberseguridad se han vuelto más estrictos en un esfuerzo por mitigar los riesgos. Sin embargo, la implementación efectiva de medidas de seguridad sigue siendo un desafío debido a la complejidad de las infraestructuras tecnológicas, la falta de conciencia generalizada sobre las mejores prácticas de seguridad y la rápida evolución de las tácticas utilizadas por los actores maliciosos.

Lagobo se estableció en 1969 en Pereira, con su red de tiendas especializadas en la comercialización de electrodomésticos y mobiliario para el hogar, bajo la marca Almacenes Oportunidades®. En 1972 se fundó la unidad de negocio orientada a las ventas al por mayor con cobertura a nivel nacional, consolidándose rápidamente como uno de los principales mayoristas en Colombia. Con más de 50 años de experiencia, Lagobo se ha destacado como líder en el sector en Colombia. Está presente en 27 ciudades del país, cuenta con más de 40 puntos de atención al público y ha brindado a numerosos clientes la oportunidad de adquirir productos mediante líneas de crédito de consumo, libranza y empresarial (Lagobo Distribuciones, 2024).

Estar en tantas ciudades del país introduce complejidades logísticas y operativas únicas. La uniformidad en la implementación de medidas de seguridad cibernética se ve

desafiada por la diversidad de ubicaciones, cada una con riesgos específicos. Así mismo, la creciente dependencia de sistemas digitales para la gestión de inventario y operaciones expone a Lagobo a riesgos significativos, por lo que gestión de datos sensibles aumenta la vulnerabilidad ante amenazas cibernéticas. Adicionalmente, la complejidad de la cadena de suministro implica múltiples puntos de exposición a riesgos cibernéticos.

La tendencia hacia compras en línea y la necesidad de una experiencia del cliente más fluida exponen a la empresa a amenazas del comercio electrónico, aumentando la necesidad de medidas de seguridad robustas. La rápida obsolescencia tecnológica, inherente a productos tecnológicos, plantea desafíos en seguridad y adaptabilidad. Si bien la innovación es esencial, la adopción de nuevas tecnologías sin una evaluación de seguridad adecuada deja a la empresa vulnerable a debilidades emergentes. La competencia intensa implica la necesidad de diferenciación constante, y los incidentes de seguridad podrían afectar la reputación, comprometiendo la confianza del cliente.

La planificación estratégica, especialmente siguiendo el estándar ISO 27001, se presenta como esencial para abordar estos desafíos (International Organization for Standardization [ISO] e International Electrotechnical Commission [IEC], 2013). La implementación de buenas prácticas garantiza la protección adecuada de datos sensibles; esto mitiga el riesgo de filtraciones y pérdida de confidencialidad.

Este proceso de planificación facilita un análisis exhaustivo de los riesgos, ofreciendo un marco sólido para identificar, evaluar y manejar los riesgos de seguridad. La implementación de buenas prácticas permite a Lagobo adaptarse de manera efectiva a los entornos tecnológicos cambiantes y a las amenazas cibernéticas en evolución. ISO 27001 (2013) proporciona un marco sólido para el cumplimiento normativo en seguridad de la información, y evita sanciones legales y pérdida de licencias comerciales.

La planificación integral fortalece la resiliencia ante posibles incidentes cibernéticos, estableciendo prácticas sólidas de respuesta a incidentes y planes de continuidad operativa. La implementación de buenas prácticas y la certificación ISO 27001 construyen confianza a través de medidas proactivas para salvaguardar la información del cliente. Prever y planificar proporciona la base para establecer una cultura de

seguridad cibernética en toda la organización, abordando la concientización, capacitación y participación de los empleados. Una planificación sólida permite la asignación eficiente de recursos y así garantiza que las inversiones en seguridad cibernética sean efectivas y alineadas con los objetivos estratégicos de Lagobo.

En el contexto dinámico y digitalizado en el que opera Lagobo Distribuciones S. A. S., surge la necesidad apremiante de abordar los desafíos inherentes a la seguridad informática, de ahí que la pregunta problematizadora es ¿cómo identificar las acciones para la planeación de la ejecución del proyecto de ciberseguridad en Lagobo Distribuciones S. A. S.?

5. JUSTIFICACIÓN

La necesidad imperante de implementar un proyecto de ciberseguridad en Lagobo Distribuciones S. A. S. se basa en la identificación de notables brechas en la infraestructura de seguridad. La empresa reconoce la constante evolución de las amenazas cibernéticas y la sofisticación de los métodos de ataque, generando una urgencia apremiante para abordar estas vulnerabilidades. La ausencia de una estrategia integral nos expone a riesgos financieros y de reputación significativos.

La iniciativa refleja el enérgico compromiso de la empresa en mejorar proactivamente su posición en ciberseguridad, considerándola no solo como una obligación, sino como una inversión estratégica para preservar la continuidad del negocio y preservar la confianza de los clientes y aliados comerciales. Este proyecto se posiciona como un paso decisivo hacia la adaptación y el fortalecimiento continuo en el siempre cambiante panorama de la ciberseguridad empresarial.

6. OBJETIVOS

6.1 Objetivo general

Diseñar la planeación de la ejecución del proyecto de ciberseguridad en la empresa Lagobo Distribuciones S. A. S.

6.2 Objetivos específicos

- Realizar un diagnóstico inicial de la infraestructura tecnológica de la empresa para identificar vulnerabilidades y riesgos en materia de ciberseguridad.
- Definir los requerimientos y lineamientos de seguridad necesarios para proteger los sistemas críticos de la empresa, de acuerdo con las normativas vigentes y las mejores prácticas del sector.
- Diseñar un plan de implementación de las soluciones de ciberseguridad, especificando las herramientas tecnológicas, recursos humanos y financieros necesarios para su ejecución
- Establecer un programa de capacitación y sensibilización para el personal de la empresa en temas de ciberseguridad.
- Implementar un sistema de monitoreo y actualización continua para garantizar la efectividad y evolución de las medidas de ciberseguridad implementadas.
- Definir indicadores clave de rendimiento (Key Performance Indicator [KPI]) para evaluar el impacto y la efectividad del plan de ciberseguridad a lo largo del tiempo.

7. DISEÑO METODOLÓGICO

El tipo de estudio que se utilizará para el proyecto de ciberseguridad en Lagobo Distribuciones S. A. S. es de carácter descriptivo-explicativo, ya que tiene como objetivo analizar la situación actual de ciberseguridad en la empresa, describir las vulnerabilidades y riesgos presentes, y explicar cómo la implementación de un plan de ciberseguridad mitigará esos riesgos.

Descriptivo: se busca describir el estado actual de la infraestructura tecnológica, las prácticas de seguridad existentes y el entorno de riesgo dentro de la organización. Esto implica el análisis de la infraestructura informática, los procedimientos de seguridad y la evaluación de incidentes previos.

Explicativo: el estudio también explicará cómo la implementación de soluciones de ciberseguridad y la adopción de mejores prácticas podrán reducir o eliminar las amenazas detectadas. Además, se analizará el impacto esperado en la operación de la empresa.

El proyecto utilizará tanto fuentes primarias como fuentes secundarias para la recolección de datos. Entre las primeras se encuentran las entrevistas semiestructuradas con los empleados clave, directivos y personal del área de TI, quienes proporcionarán información sobre las políticas de seguridad actuales, los incidentes de ciberseguridad pasados y las expectativas sobre el nuevo plan; cuestionarios distribuidos entre los empleados de distintas áreas para obtener su percepción sobre los riesgos de ciberseguridad y su familiaridad con las prácticas seguras de manejo de información: auditorías de seguridad: evaluaciones directas de la infraestructura tecnológica de la empresa para identificar vulnerabilidades a través de pruebas de penetración (*pentesting*), análisis de vulnerabilidades y simulaciones de ciberataques y la observación directa: análisis *in situ* de los procesos de seguridad y el comportamiento del personal frente a las políticas de seguridad actuales.

En cuanto a las fuentes secundarias están la documentación interna de la empresa: políticas de seguridad actuales, registros de incidentes de ciberseguridad,

manuales operativos y de infraestructura tecnológica; los estudios y reportes sectoriales: análisis de ciberseguridad en empresas de distribución y comercio, que permitan comparar la situación de Lagobo Distribuciones S. A. S. con estándares de la industria.: las normativas y estándares de seguridad: Ley 1581 de 2012 sobre protección de datos en Colombia, la ISO/IEC 27001 de gestión de la seguridad de la información, y guías de ciberseguridad aplicadas a empresas comerciales y la literatura académica y técnica sobre ciberseguridad, gestión de riesgos y modelos de planificación de la seguridad informática, que proporcionará un marco teórico y comparativo para las recomendaciones del proyecto.

El procedimiento para llevar a cabo la investigación se desarrollará en fases que están alineadas con las prácticas de planificación del PMBOK V7, y que aseguran un análisis exhaustivo y la correcta implementación del plan de ciberseguridad. A continuación, se describen las fases y los pasos específicos:

Fase 1. Identificación y diagnóstico inicial

Paso 1: recolección de la información preliminar mediante entrevistas con el personal de TI y otros interesados clave. Esto incluye la identificación de vulnerabilidades existentes en la infraestructura tecnológica.

Paso 2: auditoría de seguridad inicial de los sistemas de la empresa, utilizando herramientas como análisis de vulnerabilidades y pruebas de penetración para identificar debilidades en la red y sistemas críticos.

Paso 3: análisis de incidentes pasados de ciberseguridad, revisando los registros históricos y los informes de seguridad generados por la empresa.

Fase 2. Diseño del plan de ciberseguridad

Paso 4: análisis de las fuentes secundarias para definir las políticas de ciberseguridad que deben implementarse. Se realizará una revisión comparativa de estándares como la ISO/IEC 27001 y la Ley 1581 de 2012.

Paso 5: desarrollo de un plan detallado que incluya la selección de herramientas tecnológicas (*firewalls*, sistemas de detección de intrusos, encriptación de datos) y los protocolos de seguridad específicos que se implementarán.

Fase 3. Planificación de la implementación

Paso 6: planificación de recursos, tanto humanos como financieros, necesarios para ejecutar el proyecto de ciberseguridad. Se creará un cronograma para la implementación de soluciones de seguridad.

Paso 7: elaboración de un presupuesto y cronograma detallado que especifique los tiempos de implementación de las soluciones y la capacitación del personal.

Fase 4. Capacitación y sensibilización del personal

Paso 8: creación y distribución de material de capacitación para empleados de todos los niveles. Esto incluirá buenas prácticas para la gestión segura de datos y el uso correcto de las nuevas herramientas de ciberseguridad.

Paso 9: ejecución de talleres y sesiones de formación, con evaluaciones posteriores para medir el nivel de comprensión de los conceptos de seguridad.

Fase 5. Monitoreo y control

Paso 10: implementación de un sistema de monitoreo continuo que supervise los eventos de seguridad en tiempo real. Herramientas como sistemas de detección de intrusos (IDS) y *software* de gestión de eventos de seguridad (SIEM) se utilizarán para identificar amenazas.

Paso 11: auditorías periódicas para revisar la efectividad de las medidas de seguridad implementadas y la evolución de la situación de ciberseguridad en la empresa.

Fase 6. Evaluación de impacto

Paso 12: evaluación de la efectividad del plan de ciberseguridad implementado, utilizando indicadores clave de rendimiento (KPI). Se medirá la reducción de vulnerabilidades, el número de incidentes prevenidos y el impacto económico de las mejoras implementadas.

8. MARCO TEÓRICO

8.1 Proyecto, programa y portafolio

Un proyecto es un esfuerzo temporal diseñado para generar un resultado único, ya sea un producto, servicio o resultado específico (Project Management Institute [PMI], 2021). La temporalidad del proyecto implica que tiene un inicio y un fin claramente definidos, lo que lo diferencia de las operaciones continuas de una organización. En el contexto de Lagobo Distribuciones S. A. S., el proyecto se refiere a la implementación de un plan de ciberseguridad destinado a proteger los datos sensibles y los sistemas críticos de la empresa.

Por su parte, un programa es una agrupación de proyectos relacionados que se gestionan de manera coordinada para lograr beneficios que no podrían alcanzarse si se gestionaran de forma independiente (Project Management Institute [PMI], 2021). En este sentido, aunque el proyecto de ciberseguridad es único, podría formar parte de un programa más amplio de transformación digital dentro de la empresa, enfocado en mejorar la infraestructura tecnológica.

Finalmente, el portafolio abarca todos los proyectos y programas de una organización, gestionados en conjunto para alinear los resultados con los objetivos estratégicos (Project Management Institute [PMI], 2021). El proyecto de ciberseguridad en Lagobo Distribuciones S. A. S. forma parte de un portafolio más amplio, que podría incluir iniciativas relacionadas con mejoras en tecnología, operaciones y seguridad de la información.

8.2 Dirección de proyectos

La dirección de proyectos es la aplicación sistemática de conocimientos, herramientas, habilidades y técnicas para planificar y ejecutar proyectos de manera eficiente (PMI, 2021). Este enfoque implica la gestión de diversas etapas del proyecto, como la planificación, ejecución, monitoreo, control y cierre. En el contexto del proyecto de ciberseguridad de Lagobo Distribuciones S. A. S., la dirección de proyectos es crucial para asegurar que todas las fases, desde la identificación de riesgos hasta la

implementación de soluciones de seguridad, se lleven a cabo de manera organizada y dentro de los parámetros establecidos de tiempo, costo y calidad.

8.3 Estándares para la dirección de proyectos

Los estándares en la gestión de proyectos proporcionan un marco metodológico que ayuda a los equipos de trabajo a organizar y ejecutar proyectos de manera efectiva. Estos estándares aseguran que los proyectos se gestionen utilizando buenas prácticas reconocidas globalmente. El PMBOK (Project Management Body of Knowledge), desarrollado por el Project Management Institute (PMI, 2021), es uno de los estándares más utilizados. A través del PMBOK, las organizaciones pueden seguir un enfoque basado en procesos que garantiza el cumplimiento de los objetivos del proyecto de manera estructurada y eficiente.

8.4 Estándar del Project Management Institute (PMI)

El Project Management Institute (PMI) es una organización internacional que proporciona estándares y certificaciones para la gestión de proyectos. El PMI es conocido por su guía PMBOK, que ofrece un marco completo para la gestión de proyectos, basado en cinco grupos de procesos y diez áreas de conocimiento clave. Estos procesos cubren todas las fases del ciclo de vida de un proyecto, desde su inicio hasta su cierre. El PMI establece un enfoque estructurado que es seguido por profesionales de todo el mundo para asegurar la correcta ejecución y control de los proyectos, como en el caso de la implementación del plan de ciberseguridad en Lagobo Distribuciones S. A. S.

8.4.1 Grupos de procesos

Iniciación

La fase de iniciación marca el comienzo del proyecto, donde se define su viabilidad y se autorizan formalmente los objetivos generales (PMI, 2021). Para el proyecto de ciberseguridad en Lagobo Distribuciones S. A. S., esta fase incluye la identificación de la necesidad de reforzar la seguridad de los sistemas de la empresa y la determinación de

los objetivos iniciales del proyecto, que pueden incluir la protección de datos sensibles y la mitigación de riesgos de ciberataques.

Planeación

La fase de planeación es fundamental para el éxito del proyecto, ya que implica la elaboración de una hoja de ruta detallada que especifica cómo se alcanzarán los objetivos del proyecto (PMI, 2021). En el proyecto de ciberseguridad, esta etapa incluye la planificación de todas las actividades de seguridad, como la adquisición de herramientas tecnológicas, la capacitación del personal y el cronograma para la implementación de las medidas de protección.

Ejecución

La fase de ejecución implica poner en marcha el plan establecido, realizando las tareas planificadas para cumplir con los objetivos del proyecto (PMI, 2021). En el caso del proyecto de ciberseguridad, la ejecución implica la implementación de las soluciones tecnológicas, como sistemas de *firewall*, detección de intrusos y encriptación de datos, así como la capacitación del personal de la empresa en buenas prácticas de ciberseguridad.

Seguimiento y control

La fase de seguimiento y control garantiza que el proyecto avance conforme al plan y que los resultados sean los esperados (PMI, 2021). En esta fase, se supervisa el rendimiento del proyecto, se evalúan los riesgos y se aplican medidas correctivas cuando sea necesario. En el contexto del proyecto de ciberseguridad, el seguimiento y control implica monitorear el desempeño de las soluciones implementadas y realizar ajustes para mejorar la protección contra posibles amenazas.

Cierre

El cierre es la fase final del proyecto, donde se concluyen todas las actividades y se realiza la entrega de los resultados (PMI, 2021). En este caso, se completará la implementación de las soluciones de ciberseguridad, se verificarán los resultados

mediante auditorías de seguridad y se documentarán las lecciones aprendidas para futuros proyectos.

8.4.2 Áreas de conocimiento

Integración

La gestión de la integración se refiere a coordinar todos los elementos del proyecto de manera efectiva (PMI, 2021). En el caso del proyecto de ciberseguridad, esto incluye integrar las soluciones tecnológicas con los procesos internos de la empresa y asegurar que todas las partes del proyecto estén alineadas para lograr un resultado coherente.

Alcance

La gestión del alcance implica definir y controlar lo que está incluido en el proyecto (PMI, 2021). Para el proyecto de ciberseguridad en Lagobo Distribuciones S. A. S., el alcance incluirá la implementación de medidas de seguridad en los sistemas críticos y la protección de los datos sensibles de clientes y empleados.

Tiempo

La gestión del tiempo se enfoca en asegurar que las actividades del proyecto se completen dentro del plazo establecido (PMI, 2021). Esto implica la creación de un cronograma detallado que incluya todas las fases de implementación de las soluciones de ciberseguridad.

Costo

La gestión de costos asegura que el proyecto se mantenga dentro del presupuesto asignado (PMI, 2021). Para el proyecto de ciberseguridad, esto incluye la estimación y control de los costos asociados con la adquisición de tecnología, la capacitación del personal y los servicios de consultoría.

Calidad

La gestión de la calidad se enfoca en asegurar que las soluciones implementadas cumplan con los estándares y normativas vigentes (PMI, 2021). En el contexto del proyecto de ciberseguridad, las medidas de seguridad deben alinearse con estándares

internacionales, como ISO/IEC 27001, y con la legislación local, como La Ley 1581 sobre protección de datos (República de Colombia, 2012).

Recursos

La gestión de recursos implica la planificación y asignación adecuada de los recursos humanos y materiales necesarios para el proyecto (PMI, 2021). Esto incluye el equipo de TI, los especialistas en ciberseguridad y los consultores externos que participarán en la implementación del plan de seguridad.

Comunicaciones

La gestión de comunicaciones asegura que la información fluya adecuadamente entre todos los interesados del proyecto (PMI, 2021). Durante la ejecución del proyecto de ciberseguridad, se establecerán canales de comunicación eficaces para informar a la alta dirección, el personal técnico y otros interesados sobre los avances y decisiones clave.

Riesgos

La gestión de riesgos es esencial para identificar y mitigar las amenazas que puedan afectar el proyecto (PMI, 2021). En este caso, los riesgos pueden incluir fallas tecnológicas, ataques cibernéticos o retrasos en la implementación de las medidas de seguridad.

Adquisiciones

La gestión de adquisiciones incluye la compra de bienes y servicios necesarios para el proyecto (PMI, 2021). Esto puede incluir la adquisición de herramientas de seguridad, como *software* de *firewall*, sistemas de detección de intrusos y servicios de consultoría en ciberseguridad.

Interesados

La gestión de los interesados se refiere a identificar a todas las personas afectadas por el proyecto y gestionar sus expectativas de manera efectiva (PMI, 2021). En el proyecto de ciberseguridad, los interesados clave son la alta dirección, el equipo de TI, los empleados y los proveedores de soluciones tecnológicas.

8.4.3 Matriz de grupos de procesos (GP) vs. Áreas de conocimiento (AC)

La matriz de grupos de procesos (GP) vs. Áreas de conocimiento (AC) funciona como una herramienta esencial para coordinar los elementos clave de un proyecto de manera efectiva (PMI, 2021). Este recurso permite conectar de forma clara cada grupo de procesos (iniciación, planeación, ejecución, seguimiento y control, y cierre) con sus respectivas áreas de conocimiento (como integración, alcance, tiempo, costo, calidad, recursos, comunicaciones, riesgos, adquisiciones e interesados). De esta manera, se logra una visión integral y detallada que facilita no solo una planificación estructurada, sino también una gestión más eficiente en cada fase, asegurando que todos los aspectos del proyecto estén alineados y trabajando en conjunto para cumplir con los objetivos establecidos.

Tabla 1. *Matriz grupos de procesos (GP) vs. Áreas de conocimiento (AC)*

Área de conocimiento (AC)	Planificación: actividades clave (GP)
Integración	Desarrollar el plan de gestión del proyecto de ciberseguridad, que incluye unificación de políticas, normas y metodologías a utilizar.
	Definir la secuencia de integración entre soluciones como *firewall*s, IDS y MFA, garantizando su compatibilidad y efectividad.
Alcance	Realizar la declaración detallada del alcance, incluyendo todas las fases de implementación de soluciones (*firewall*s, IDS, MFA).
	Crear la EDT (Estructura de desglose de trabajo) para segmentar cada componente de ciberseguridad.
	Definir el cronograma detallado para cada fase de implementación de soluciones de ciberseguridad.

Área de conocimiento (AC)	Planificación: actividades clave (GP)
Cronograma	Estimar la duración de actividades, asignando recursos a tareas clave como configuración de *firewall*s e instalación de IDS.
Costo	Estimar el presupuesto detallado para licencias, infraestructura adicional y capacitación.
	Considerar costos adicionales para posibles cambios en herramientas debido a nuevas amenazas (flexibilidad de presupuesto).
Calidad	Definir los estándares de calidad y KPI para el desempeño de cada solución (ej., tiempo de respuesta de IDS, efectividad de MFA).
	Establecer criterios para la revisión continua y auditorías del sistema de ciberseguridad.
Recursos	Planificar la disponibilidad de especialistas en TI y consultores de ciberseguridad para cada fase.
	Asignar recursos específicos para la gestión del cambio, especialmente en fases de integración.
Comunicaciones	Definir el plan de comunicaciones internas para informar al personal sobre políticas y actualizaciones.
	Establecer reportes periódicos para la gerencia sobre el progreso y resultados de las implementaciones.
Riesgos	Identificar riesgos clave como posibles vulnerabilidades durante la integración de sistemas o cambios tecnológicos urgentes.
	Desarrollar planes de respuesta ante riesgos cibernéticos y cambios inesperados en el panorama de amenazas.
	Planificar la adquisición de licencias de *software* y hardware.

Área de conocimiento (AC)	Planificación: actividades clave (GP)
Adquisiciones	Coordinar contratos con proveedores de soluciones específicas como sistemas de autenticación multifactor (MFA).
Interesados	Identificar a los interesados clave, incluyendo la gerencia y empleados que interactúan con los sistemas. Definir el plan de involucramiento de los interesados en cada fase, asegurando su apoyo y comprensión del proyecto de ciberseguridad.

Tabla 2. *Procesos de dirección de proyectos según PMBOK*

	GRUPOS DE PROCESOS				
ÁREAS DE CONOCIMIENTO	**Grupo de procesos de Iniciación**	**Grupo de procesos de Planificación**	**Grupo de procesos de Ejecución**	**Grupo de procesos de Monitoreo y control**	**Grupo de procesos de Cierre**
1. Gestión de la integración del proyecto	1.1 Desarrollar el acta de constitución del proyecto	1.2 Desarrollar el plan para la dirección del proyecto	1.3 Dirigir y gestionar el trabajo del proyecto	1.4 Monitorizar y controlar el trabajo del proyecto 1.5 Realizar el control integrado de cambios	1.6 Cerrar el proyecto o fase
2. Gestión del alcance		2.1 Planificar la gestión del alcance 2.2 Recopilar requisitos 2.3 Definir el alcance 2.4 Crear EDT/WBS		2.5 Validar el alcance 2.6 Controlar el alcance	

	GRUPOS DE PROCESOS				
ÁREAS DE CONOCIMIENTO	**Grupo de procesos de Iniciación**	**Grupo de procesos de Planificación**	**Grupo de procesos de Ejecución**	**Grupo de procesos de Monitoreo y control**	**Grupo de procesos de Cierre**
3. Gestión del cronograma		3.1 Planificar la gestión del cronograma 3.2 Definir las actividades 3.3 Secuenciar las actividades 3.4 Estimar la duración de las actividades 3.5 Desarrollar el cronograma		3.6 Controlar el cronograma	
4. Gestión de los costos del proyecto		4.1 Planificar la Gestión de los Costos 4.2 Estimar los costos 4.3 Determinar el Presupuesto		4.4 Controlar los costos	
5. Gestión de la calidad del proyecto		5.1 Planificar la gestión de la calidad	5.2 Gestionar la calidad	5.3 Controlar la calidad	

	GRUPOS DE PROCESOS				
ÁREAS DE CONOCIMIENTO	**Grupo de procesos de Iniciación**	**Grupo de procesos de Planificación**	**Grupo de procesos de Ejecución**	**Grupo de procesos de Monitoreo y control**	**Grupo de procesos de Cierre**
6. Gestión de los recursos del proyecto		6.1 Planificar la gestión de recursos 6.2 Estimar los recursos de las actividades	6.3 Adquirir recursos 6.4 Desarrollar el equipo 6.5 Dirigir al equipo		
7. Gestión de las comunicaciones del proyecto		7.1 Planificar la gestión de las comunicaciones	7.2 Gestionar las comunicaciones	7.3 Monitorear las comunicaciones	
8. Gestión de los riesgos del proyecto		8.1 Planificar la gestión de los riesgos 8.2 Identificar los riesgos 8.3 Realizar el análisis cualitativo de riesgos		8.7 Monitorear los riesgos	

	GRUPOS DE PROCESOS				
ÁREAS DE CONOCIMIENTO	**Grupo de procesos de Iniciación**	**Grupo de procesos de Planificación**	**Grupo de procesos de Ejecución**	**Grupo de procesos de Monitoreo y control**	**Grupo de procesos de Cierre**
		8.4 Realizar el análisis cuantitativo de riesgos 8.5 Planificar la respuesta a los riesgos			
9. Gestión de las adquisicio-nes del proyecto		9.1 Planificar la gestión de las adquisiciones	9.2 Efectuar las adquisiciones	9.3 Controlar las adquisiciones	9.4 Cerrar las adquisiciones
10. Gestión de los interesados	10.1 Identificar a los interesados (*stakeholders*)	10.2 Planificar el involucramiento de los interesados	10.3 Gestionar la participación de los Interesados	10.4 Monitorear el involucramiento de los interesados	

8.5 Ciberseguridad

La ciberseguridad abarca un conjunto de estrategias, herramientas y metodologías diseñadas para salvaguardar la integridad, confidencialidad y disponibilidad de los sistemas de información y los datos frente a riesgos y ataques digitales (Ortega Candel, 2021). Para Lagobo Distribuciones S. A. S., la ciberseguridad es esencial para proteger los datos de sus clientes y empleados, así como para garantizar la continuidad operativa de sus sistemas tecnológicos. El proyecto de ciberseguridad incluye la implementación de medidas como firewalls, sistemas de detección de intrusos, encriptación de datos y capacitación del personal, con el objetivo de prevenir ataques y proteger los activos digitales de la empresa.

Adware: es un software que muestra pautas publicitarias en equipos de cómputo y dispositivos móviles, generalmente sin consentimiento. Puede afectar la privacidad al recopilar datos de navegación para personalizar la publicidad.

Algoritmo: secuencia de pasos definidos que un sistema sigue para ejecutar una tarea, como cifrar datos o analizar amenazas (Kumar, 2024).

Apache: servidor web de código abierto que requiere medidas de seguridad constantes debido a su exposición a ciberataques (Cooper, & Powell, 2020)

API: conjunto de reglas que permiten la comunicación entre aplicaciones, siendo un punto vulnerable si no se protege adecuadamente (Red Hat, s. f.).

Ataque de fuerza bruta: método que prueba combinaciones de contraseñas hasta encontrar la correcta, mitigable con autenticación multifactor (Fortinet, s. f. a).

Auditoría: proceso estructurado y sistemático que permite evaluar el nivel de seguridad en sistemas informáticos, identificando vulnerabilidades y asegurando el cumplimiento de normativas establecidas (Tarlogic, s. f. a).

Babuk: *ransomware* que cifra archivos y exige pago para su recuperación; afecta infraestructuras críticas (SentinelOne, s. f.).

Backdoor: acceso oculto a un sistema que permite el control no autorizado, usado por atacantes y malware (Alberts, 2021).

Backup: copia de seguridad de datos para prevenir pérdidas en caso de ataques o fallos (Ortiz, 2021).

Big Data: análisis de grandes volúmenes de información para detectar patrones y prevenir amenazas (Gandomi, & Haider, 2015).

Blockchain: registro distribuido que protege la integridad de transacciones y datos frente a manipulaciones (Casino et al., 2019).

BlueTrust: técnica que explota vulnerabilidades en conexiones bluetooth para obtener acceso no autorizado (Lee, & Park, 2018).

Bot: programa automatizado que ejecuta tareas repetitivas, a veces con fines maliciosos como spam o ataques DDoS (Cloudflare, s. f.).

Botnet: conjunto de dispositivos comprometidos y controlados de manera remota por un atacante. Se usa para realizar acciones maliciosas como el envío masivo de correos no deseados o ataques coordinados contra sistemas en línea (Alberts, 2021).

Braktooth: conjunto de fallos en chips bluetooth que permiten a los atacantes tomar el control de los dispositivos (Malwarebytes, 2021).

Burp Suite: herramienta de pruebas de seguridad para detectar vulnerabilidades en aplicaciones web (Fletcher, 2020).

C2 (Command and Control): infraestructura usada por ciberdelincuentes para gestionar sistemas comprometidos de forma remota (Alberts, 2021).

Catfishing: suplantación de identidad en línea con el fin de engañar y obtener información personal (Chen, & Li, 2020).

Controlador de dominio: servidor que administra accesos en una red y es un objetivo clave para atacantes (NinjaOne. s. f.).

Cracker: persona que vulnera sistemas con fines destructivos o de robo de información (Chen, & Li, 2020).

Cryptojacking: uso no autorizado de recursos de un dispositivo para minar criptomonedas (Feldman, 2021).

CVE: base de datos que identifica y clasifica vulnerabilidades de software y hardware (IBM, s. f. a).

DCSync: método que permite a los atacantes replicar el tráfico de autenticación para robar credenciales (SentinelOne, s. f).

DDoS: ataque que satura un servidor con tráfico excesivo para dejarlo inoperativo (Tarlogic Security, s. f. a).

DHCP: protocolo que asigna direcciones IP automáticamente; es vulnerable si se configura incorrectamente (Alberts, 2021).

DNS: sistema que traduce nombres de dominio en direcciones IP y puede ser explotado mediante ataques de envenenamiento de caché.

DRM: tecnología que protege derechos digitales y restringe el acceso no autorizado a contenido (Chen, & Li, 2020).

EDR: solución de seguridad que detecta y responde a amenazas en dispositivos finales (Ortega Candel, 2021).

Emotet: malware que se propaga a través de correos electrónicos y facilita otros ataques (Alberts, 2021).

Firmware: software interno de dispositivos electrónicos, susceptible a ataques si no se actualiza (AVG, s. f.).

FSTM: técnica que monitorea cambios en archivos para detectar accesos no autorizados (Tarlogic Security, s. f. a).

Fuzzing: prueba de software que inyecta datos aleatorios para descubrir vulnerabilidades (GitLab, s. f.).

Golang: lenguaje de programación seguro y eficiente, usado en aplicaciones de ciberseguridad (Leung, 2021).

Gusano informático: malware que se propaga automáticamente en redes sin intervención humana (Tarlogic, s. f. a).

Hacker: persona con conocimientos avanzados en informática que puede usar sus habilidades para fines éticos o maliciosos.

Hash NTLM: método de autenticación de Windows vulnerable a ataques, si no se protege adecuadamente (CrowdStrike, s. f.).

Hashcat: herramienta para descifrar contraseñas mediante ataques de fuerza bruta o diccionario (Chen, & Li, 2020).

Honeypotting: técnica que usa sistemas trampa para atraer y analizar ciberdelincuentes (Alberts, 2021).

Ingeniería social: método de manipulación psicológica para obtener información confidencial mediante engaños (Tarlogic, s. f. a).

Instancia Amazon EC2: servidor virtual de AWS que permite ejecutar aplicaciones con escalabilidad y seguridad configurable.

Inyección SQL: ataque que introduce código malicioso en bases de datos para acceder o modificar información (Chen, & Li, 2020).

IoT (Internet de las cosas): conexión de dispositivos a internet para automatización. Tiene riesgos de seguridad por vulnerabilidades (Feldman, 2021).

Kerberoasting: ataque que extrae credenciales en entornos Kerberos descifrando tickets de autenticación (IBM, s. f. b).

Kerberos: protocolo de autenticación basado en tickets para validar identidades en redes.

Kernel: núcleo del sistema operativo que gestiona hardware y procesos (Geeknetic, s. f.).

Keylogger: programa malicioso que registra las pulsaciones del teclado para robar información (Chen, & Li, 2020).

Klist: herramienta de línea de comandos para administrar tickets Kerberos en Windows (MIT, s. f.).

KRBTGT: cuenta de Kerberos responsable de emitir tickets de autenticación en una red (Quest, s. f.).

Latencia: retardo en la transmisión de datos en redes, que afecta el rendimiento y la seguridad (Tarlogic, s. f. a).

LDAP: protocolo para gestionar directorios de usuarios en redes empresariales (Chen, & Li, 2020).

Log4j: biblioteca de registro en Java con una vulnerabilidad crítica; descubierta en 2021 (Apache Software Foundation, s. f.).

Log4Shell: fallo de seguridad en Log4j que permite la ejecución remota de código (IBM, (s. f. c).

LoRa Protocol: tecnología inalámbrica para IoT, eficiente pero con desafíos de seguridad (Feldman, 2021).

Malware: software malicioso diseñado para infiltrarse y dañar sistemas (Alberts, 2021).

MASA: evaluación de seguridad de aplicaciones móviles contra amenazas cibernéticas (Abstracta, 2023).

MDR: servicio de detección y respuesta ante amenazas en tiempo real (Microsoft, s. f.).

Mimikatz: herramienta que extrae credenciales de sistemas Windows (Parrot Security, s. f.).

OWASP: proyecto que mejora la seguridad en aplicaciones web, conocido por su OWASP Top 10 (Alberts, 2021).

Phishing: fraude que usa engaños para obtener credenciales o información sensible (Chen, & Li, 2020).

PHP: lenguaje de programación web; si no se implementa correctamente representa riesgos (GeeksforGeeks, s. f.).

RaaS: modelo en el que los ciberdelincuentes alquilan *ransomware* a cambio de ganancias (IBM, s. f. d).

Ransomcloud: *ransomware* dirigido a datos almacenados en la nube (Tarlogic Security, s. f. a).

Ransomware: malware que cifra archivos y exige un pago por su recuperación (Trend Micro, s. f.)

Rootkit: programa que oculta la presencia de atacantes en un sistema (Kaspersky, s. f.).

SaaS: software accesible en la nube sin necesidad de instalación local (Feldman, 2021).

Sandbox: entorno aislado para analizar archivos sospechosos sin comprometer el sistema (Chen, & Li, 2020).

Secuestro de cuenta: acceso no autorizado a una cuenta mediante phishing u otros ataques (Tarlogic Security, s. f. a).

Selenium Grid: herramienta para pruebas automatizadas en múltiples navegadores y sistemas (Selenium, s. f.).

Shimming: técnica que inyecta código malicioso en aplicaciones sin modificar su código fuente original, utilizada para escalar privilegios (Tarlogic, s. f. b).

Skimmers de tarjetas de pago: dispositivos físicos ocultos en cajeros o terminales, que roban datos de tarjetas sin que el usuario lo note (Tarlogic, s. f. a).

Sniffer: herramienta que intercepta y analiza tráfico de red, utilizada tanto para diagnóstico como para el robo de información (Chen, & Li, 2020).

SPAM: envío masivo e indiscriminado de mensajes no solicitados, generalmente con fines publicitarios o fraudulentos, que pueden incluir enlaces maliciosos o intentos de suplantación de identidad (Feldman, 2021).

Spear Phishing: variante de phishing que usa información personalizada para engañar a individuos o empresas específicas (Chen, & Li, 2020).

Spyware: malware diseñado para espiar a los usuarios, recopilando credenciales, historial de navegación y otros datos sensibles (Alberts, 2021).

TIBER (Threat Intelligence-Based Ethical Red Teaming): marco utilizado en el sector financiero para evaluar la resiliencia ante ataques cibernéticos mediante simulaciones controladas (European Central Bank, s. f.).

TLS (Transport Layer Security): protocolo de seguridad que cifra la comunicación en red para evitar la interceptación o modificación de datos (Entrust, s. f.).

Troyano: malware disfrazado de software legítimo que permite el acceso no autorizado a un sistema y puede robar información o instalar otros programas maliciosos (Tarlogic, s. f. a).

Vector de ataque: método utilizado por atacantes para explotar vulnerabilidades y comprometer un sistema, como phishing o inyección SQL (Alberts, 2021).

Virus heurístico: técnica de detección antivirus que identifica comportamientos sospechosos en archivos para detectar malware sin necesidad de firmas conocidas (Chen, & Li, 2020).

WAF (Web Application Firewall): firewall que protege aplicaciones web filtrando y monitoreando el tráfico HTTP para bloquear ataques como inyección SQL (Feldman, 2021).

Watering Hole: técnica de ataque en la que un ciberdelincuente compromete un sitio web frecuentado por un grupo específico de usuarios, insertando código malicioso para infectar sus dispositivos y obtener acceso a sus sistemas (Chen, & Li, 2020).

XAMPP: paquete de software de código abierto que facilita el desarrollo web, incluyendo Apache, MySQL, PHP y Perl (Leung, 2021).

XDR (Extended Detection and Response): solución de seguridad que unifica la detección y respuesta ante amenazas en endpoints, redes y servidores (Fortinet, s. f., b).

ZeroShell: distribución Linux especializada en servicios de red y seguridad como firewalls, VPNs y autenticación (LinuxMind, 2024).

Zombie: dispositivo infectado por malware y controlado por un atacante, generalmente como parte de una botnet para ataques coordinados (Chen, & Li, 2020).

8.6 Inteligencia artificial

La inteligencia artificial (IA) es una disciplina dentro de la informática que se centra en el desarrollo de sistemas capaces de llevar a cabo tareas que, en condiciones normales, requieren habilidades cognitivas humanas. Entre estas tareas se incluyen el procesamiento del lenguaje, la identificación de patrones, la toma de decisiones y el aprendizaje basado en la experiencia previa. Para su implementación, la IA integra algoritmos avanzados, modelos computacionales y la gestión de grandes volúmenes de datos, permitiendo la evolución constante de los sistemas sin la necesidad de una intervención humana continua (Russell, & Norvig, 2021).

Dentro de la IA, se pueden distinguir dos enfoques principales: la IA débil y la IA fuerte. La IA débil está diseñada para realizar tareas específicas, como la recomendación de contenido o la detección de anomalías en sistemas informáticos. Por otro lado, la IA fuerte busca replicar la inteligencia humana en su totalidad, aunque su desarrollo aún se encuentra en una etapa temprana. A pesar de ello, los avances en IA débil han transformado diversos sectores, incluyendo el ámbito de la ciberseguridad.

8.6.1 IA en ciberseguridad

En el contexto de la seguridad informática, la inteligencia artificial ha revolucionado las estrategias de defensa, permitiendo a las organizaciones adelantarse a posibles amenazas y responder con mayor rapidez a incidentes. Su capacidad para analizar volúmenes masivos de datos en tiempo real la convierte en una herramienta fundamental para detectar comportamientos sospechosos, predecir posibles ataques y automatizar procesos de respuesta ante incidentes. Esta evolución es particularmente relevante en una era donde los ataques cibernéticos han aumentado tanto en frecuencia como en sofisticación (Goodfellow et al., 2016).

8.6.2 Análisis y detección de amenazas

Uno de los usos más destacados de la IA en seguridad informática es su capacidad para examinar grandes cantidades de información y detectar actividades anómalas. Los métodos tradicionales de detección de intrusos dependen de bases de

datos con firmas predefinidas de malware, lo que resulta insuficiente frente a amenazas desconocidas o de reciente aparición, como los ataques de día cero (Sarker, 2021).

En contraste, la IA emplea modelos de aprendizaje automático que analizan el tráfico de red y los comportamientos de los usuarios, identificando patrones inusuales que podrían ser indicios de un ataque. A medida que los sistemas procesan más información, su capacidad de detección mejora, permitiendo una identificación más precisa de amenazas emergentes (Russell, & Norvig, 2021).

8.6.3 Prevención y mitigación automática de amenazas

Además de detectar riesgos, la IA puede actuar automáticamente para evitar la propagación de ataques. Un ejemplo de esto es el uso de plataformas de respuesta ante incidentes que integran múltiples capas de seguridad y analizan información proveniente de distintas fuentes, como redes, servidores y dispositivos finales (Sarker, 2021).

Cuando un sistema basado en IA detecta un comportamiento sospechoso, como intentos de acceso no autorizados o tráfico inusual en la red, puede bloquear automáticamente la amenaza o aislarla antes de que cause un daño significativo. En ataques de *ransomware*, por ejemplo, la IA es capaz de identificar patrones característicos de cifrado malicioso y detener el proceso antes de que afecte a múltiples sistemas (Russell, & Norvig, 2021).

8.6.4 Detección y prevención del phishing

El phishing es una de las técnicas más utilizadas por los ciberdelincuentes para obtener información confidencial. Los métodos tradicionales de detección, basados en listas negras y patrones predefinidos, pueden ser eludidos con facilidad mediante la creación de nuevas variantes de ataques (Goodfellow et al., 2016).

La IA ha permitido mejorar la detección de intentos de phishing a través del procesamiento avanzado del lenguaje natural. Mediante esta tecnología, los sistemas pueden analizar correos electrónicos y mensajes en busca de indicios de engaño, como el uso de lenguaje persuasivo o la inclusión de enlaces sospechosos. Además, los

modelos pueden evolucionar con el tiempo, adaptándose a nuevas estrategias utilizadas por los atacantes (Russell, & Norvig, 2021).

8.6.5 Fortalecimiento de la autenticación y gestión de identidades

Otro uso importante de la IA en seguridad informática es en la autenticación y administración de identidades digitales. Los métodos tradicionales de autenticación, como el uso de contraseñas, presentan vulnerabilidades ante ataques de fuerza bruta o suplantación de identidad (Goodfellow et al., 2016).

El empleo de IA en este ámbito permite la implementación de medidas más seguras, como el reconocimiento biométrico y la autenticación multifactor. Además, los sistemas pueden analizar el comportamiento habitual de los usuarios y detectar cualquier actividad anómala, exigiendo pasos adicionales de verificación cuando sea necesario.

8.6.6 Predicción y defensa proactiva

Uno de los avances más prometedores en ciberseguridad es la capacidad de la IA para prever amenazas futuras. A partir del análisis de incidentes pasados, los modelos predictivos pueden identificar patrones y tendencias que ayuden a anticipar posibles ataques (Sarker, 2021).

Por ejemplo, mediante el estudio de ataques de *ransomware* en diferentes regiones, la IA puede predecir posibles focos de infección y recomendar medidas de prevención antes de que ocurra un incidente. Este enfoque permite que las organizaciones adopten estrategias preventivas, en lugar de reaccionar únicamente cuando ya se ha producido un ataque (Goodfellow et al., 2016).

8.6.7 Desafíos en la interpretación de datos e IA

A pesar de las ventajas que ofrece la IA en ciberseguridad, uno de los principales desafíos es la gestión de la gran cantidad de información que generan estos sistemas. Los datos relacionados con posibles amenazas pueden ser abrumadores y, en muchos casos, los analistas de seguridad deben priorizar aquellos eventos que representan un riesgo real (Russell, & Norvig, 2021).

Para abordar este desafío, los modelos de IA se han diseñado para clasificar y evaluar la criticidad de los eventos detectados, permitiendo a los especialistas enfocarse en los incidentes más relevantes. De esta manera, se optimizan los tiempos de respuesta y se reduce la carga de trabajo en los equipos de seguridad.

8.6.8 El uso de IA por parte de los ciberdelincuentes

A medida que la inteligencia artificial se convierte en una herramienta clave para la ciberdefensa, también existe el riesgo de que los atacantes la utilicen para desarrollar estrategias más sofisticadas. Los ciberdelincuentes pueden emplear IA para evadir sistemas de detección, generar malware adaptativo y personalizar ataques dirigidos con mayor efectividad.

Esta realidad plantea un nuevo reto en el ámbito de la ciberseguridad, ya que se requiere un desarrollo continuo de nuevas estrategias y tecnologías que permitan mantenerse un paso adelante frente a las amenazas emergentes. La competencia entre los sistemas defensivos y ofensivos basados en IA se ha convertido en un campo de batalla clave en la seguridad digital.

9. GRUPO DE PROCESOS DE INICIO

Acta de constitución del proyecto

Proyecto: Planificación de la ejecución del proyecto de ciberseguridad para Lagobo Distribuciones S. A. S.

Gerente: Alexander Franco Murcia
Preparado por: Departamento de Tecnología y Ciberseguridad
Revisado por: Departamento de Seguridad Informática
Aprobado por: Germán Gustavo López Galvis

Revisión

Correlativo: 01

Descripción - Realizada por: Departamento de Tecnología

Fecha: 10/11/2024

Breve descripción del producto o servicio del proyecto

Este proyecto tiene como objetivo diseñar y planificar la ejecución de un sistema de ciberseguridad integral en Lagobo Distribuciones S. A. S. La propuesta incluye el diagnóstico de la infraestructura actual, la definición de requerimientos de seguridad, el diseño de un plan de implementación de herramientas y tecnologías de protección, y la capacitación del personal para asegurar el cumplimiento de normativas y mejores prácticas en ciberseguridad. La implementación de esta planificación mejorará la resiliencia de la organización frente a amenazas cibernéticas y garantizará la protección de sus activos digitales y datos sensibles.

Los principales entregables incluyen:

1. Diagnóstico de la infraestructura de TI y evaluación de riesgos.
2. Diseño del plan de implementación de ciberseguridad con tecnologías específicas como *firewall*s, IDS/IPS, y autenticación multifactor.
3. Programa de capacitación para el personal en políticas de ciberseguridad.

4. Sistema de monitoreo y definición de indicadores clave (KPI) para la evaluación continua de la efectividad de las soluciones de seguridad implementadas.

Tabla 3. *Alineamiento del proyecto*

Objetivos estratégicos de la organización	Propósito del proyecto
Proteger los datos y sistemas críticos de la empresa y cumplir con normativas de seguridad.	Incrementar la seguridad cibernética de Lagobo Distribuciones S. A. S. mediante una planificación exhaustiva y alineada a las mejores prácticas.
Fortalecer la cultura de ciberseguridad en toda la organización.	Capacitar al personal para identificar y prevenir amenazas cibernéticas.
Desarrollar un sistema de monitoreo constante que permita una actualización continua de las medidas de seguridad.	Asegurar la sostenibilidad y evolución del sistema de ciberseguridad en el tiempo.

9.1 Alcance, tiempo, costo y calidad

- Alcance: el proyecto de planificación incluirá el diagnóstico, la definición de requerimientos, el diseño del plan de implementación de ciberseguridad y la capacitación del personal.
- Tiempo: el plazo estimado para completar la planificación es de seis meses.
    - Fecha de inicio: 15/01/2025
    - Fecha de término: 15/06/2025
- Costo: el presupuesto estimado para esta fase de planificación es de $200 mil dólares.

- Calidad: el proyecto debe cumplir con los estándares internacionales de seguridad, como ISO/IEC 27001, y asegurar la eficiencia en la protección de datos y sistemas.

Tabla 4. *Interesados*

Interesado	Requisitos	Criterio de Aceptación
Gerente General	Aprobar el plan de implementación de ciberseguridad y asegurar la inversión en recursos.	El plan debe estar completo, en tiempo, y dentro del presupuesto aprobado.
Departamento de TI	Implementar el diagnóstico y diseño de soluciones de ciberseguridad en todas las sucursales.	El plan de implementación debe ser compatible con la infraestructura actual y alinearse con la normativa vigente.
Personal de Lagobo	Recibir capacitación en políticas y protocolos de ciberseguridad.	Completar la capacitación y evaluar el conocimiento en ciberseguridad mediante pruebas de desempeño.
Consultores Externos	Realizar el diagnóstico de infraestructura y asesorar en el diseño de soluciones seguras.	Entrega de informes de evaluación, recomendaciones y un plan aprobado por el equipo de ciberseguridad.

Tabla 5. *Extensión y alcance del proyecto*

Etapas del proyecto	Principales entregables
Diagnóstico inicial	Evaluación de la infraestructura tecnológica y detección de vulnerabilidades.
Definición de requerimientos	Identificación de las soluciones de ciberseguridad necesarias, alineadas con las normativas y buenas prácticas.
Diseño del plan de implementación	Plan detallado con las herramientas de seguridad específicas, incluyendo IDS, *firewall*s, MFA y cifrado.
Capacitación del personal	Programa de capacitación en ciberseguridad para los empleados de todas las sucursales.
Monitoreo y KPI	Sistema de monitoreo continuo y KPI para medir la efectividad del plan de seguridad implementado.

Tabla 6. *Roles en el proyecto*

Rol en el proyecto	Nombre y cargo
Patrocinador	Gerente General de Lagobo Distribuciones S. A. S.
Director	Alexander Franco, Gerente de Tecnología
Auditor de seguridad	Consultor externo en ciberseguridad
Responsable de capacitación	Gerente de Recursos Humanos y Formación
Supervisor de monitoreo y KPI	Especialista en Seguridad Informática

Tabla 7. *Riesgos*

Tipo de riesgo	Descripción	Impacto en objetivos
Riesgo positivo	Aceleración en la adopción de políticas de ciberseguridad por parte del personal.	Mayor eficiencia en la implementación de las políticas de seguridad.
Riesgo negativo	Evolución de amenazas cibernéticas durante el proceso de diseño e implementación del plan.	Ajustes de costos y tiempos para adaptar las medidas de seguridad.
Riesgo negativo	Falta de adopción o resistencia del personal al cambio en procesos de seguridad.	Posible retraso en la capacitación y cumplimiento de políticas.
Riesgo negativo	Incremento de costos por la necesidad de nuevas herramientas o licencias adicionales.	Ampliación del presupuesto y posible extensión del cronograma.

Tabla 8. *Hitos principales del proyecto*

N.º	Hito principal	Fecha inicio	Fecha final	Responsable
1	Inicio del diagnóstico	15/01/2025	30/01/2025	Director del Proyecto
2	Definición de requerimientos	01/02/2025	28/02/2025	Consultores Externos
3	Diseño del plan de implementación	01/03/2025	31/05/2025	Director del Proyecto
4	Capacitación del personal	01/06/2025	30/06/2025	Gerente de Recursos Humanos
5	Establecimiento de sistema de monitoreo y KPI	01/07/2025	31/07/2025	Especialista en Seguridad Informática

Tabla 9. *Restricciones*

Restricción	Impuesta por
El proyecto debe culminarse antes del 31/07/2025	Gerente General
El presupuesto máximo disponible es de $200 millones de pesos colombianos	Gerente General
No se permitirá ampliación de plazos sin justificación adecuada	Patrocinador

Tabla 10. *Supuestos*

Supuesto	Incertidumbre
Desembolso del presupuesto según cronograma	Retraso en la compra de herramientas críticas.
Apoyo de los empleados en la capacitación	Retrasos si el personal no asiste a las sesiones.
Estabilidad de las normas de ciberseguridad	Ajuste del plan si surgen nuevas normativas.

Tabla 11. *Requerimientos de aprobación del proyecto*

Criterio de éxito	Evaluador
Entregar el proyecto de planificación en el plazo acordado	Gerente General de Lagobo Distribuciones S. A. S.
Mantener el costo dentro del presupuesto aprobado	Gerente General de Lagobo
Cumplir con los estándares de calidad y seguridad requeridos	Gerente General de Lagobo
Completar todos los entregables definidos en el plan	Gerente de Tecnología

Gerente asignado al proyecto: Alexander Franco, Gerente de Tecnología

Autoridad asignada: Germán Gustavo López Galvis, Gerente General

Aceptado por: Alexander Franco, Gerente del Proyecto

Aprobado por: Germán Gustavo López Galvis, Patrocinador

Fecha: 01/01/2025

10. GRUPO DE PROCESOS DE PLANIFICACIÓN

10.1 Plan para la dirección del proyecto de ciberseguridad

Este plan establece las pautas para la planificación del proyecto de ciberseguridad en Lagobo Distribuciones S. A. S. Su función es asegurar que todas las áreas de conocimiento involucradas en el proyecto (alcance, tiempo, costo, calidad, recursos, comunicaciones, riesgos, adquisiciones e interesados) se integren de manera coherente. Además, servirá como base para orientar y coordinar las actividades que permitirán, en etapas posteriores, implementar soluciones tecnológicas, capacitar al personal y establecer un sistema de monitoreo continuo.

10.2 Propósito y alcance

El principal propósito de este plan es ofrecer un marco claro que guíe la fase de planificación, garantizando que las decisiones que tomemos ahora faciliten la futura ejecución de las medidas de ciberseguridad. El alcance de este documento incluye:

- La definición de cómo elaboraremos y coordinaremos los planes subsidiarios (por ejemplo, el plan de gestión del alcance, del cronograma, de costos y otros).
- El establecimiento de normas sobre cómo manejaremos cambios, comunicaremos avances y gestionaremos riesgos durante la planificación.
- La determinación de criterios de calidad, estándares normativos (como ISO/IEC 27001) y estrategias para involucrar a todos los interesados.

10.3 Alineación con la estrategia de la empresa

La necesidad de una sólida ciberseguridad está alineada con la estrategia de Lagobo Distribuciones S. A. S. de proteger sus activos digitales, cumplir con las regulaciones vigentes y mantener la confianza de sus clientes. Al aplicar las mejores

prácticas en gestión de proyectos y ciberseguridad, este plan contribuye a la misión corporativa de ofrecer un entorno digital confiable y resiliente.

10.4 Estructura del plan

Este plan articula cómo abordaremos cada área de conocimiento:

- Alcance: definiremos las tareas a realizar en la planificación (como el diagnóstico de vulnerabilidades y la determinación de requerimientos) y los entregables que resulten de esta fase.
- Tiempo: desarrollaremos un cronograma con hitos para asegurar que el diagnóstico, la definición del plan de implementación y la creación del programa de capacitación se completen a tiempo.
- Costo: estimaremos los recursos financieros necesarios para las actividades de planificación, cuidando no superar el presupuesto asignado.
- Calidad: estableceremos estándares de calidad y criterios de éxito que garanticen que las soluciones diseñadas cumplan con normativas y recomendaciones internacionales.
- Recursos: identificaremos el personal y las herramientas necesarias en esta etapa; esto incluye consultores externos en ciberseguridad y miembros clave del equipo de TI.
- Comunicaciones: definiremos los canales y la frecuencia de las comunicaciones entre el equipo, la dirección de la empresa y los consultores, asegurando una información fluida y transparente.
- Riesgos: analizaremos riesgos potenciales desde cambios normativos hasta nuevas amenazas y estableceremos planes de respuesta apropiados.

- Adquisiciones: aunque la planificación no implica compras directas, determinaremos pautas para futuras adquisiciones de licencias, *software* y otros recursos.
- Interesados: planificaremos cómo involucrar a la alta dirección, al personal y a los consultores de manera que comprendan, apoyen y se alineen con los objetivos del proyecto.

10.5 Roles y responsabilidades

- Director del proyecto (Alexander Franco): coordina la integración de todos los planes subsidiarios y supervisa su coherencia.
- Consultores externos: aportan experiencia técnica para el análisis de riesgos y la selección de soluciones.
- Equipo de TI y RR. HH.: colaboran en la definición de requerimientos técnicos y el programa de formación para el personal.
- Gerente general (patrocinador): valida las directrices, provee recursos y respalda las decisiones clave.

10.6 Gestión de cambios

Reconocemos que la ciberseguridad es un ámbito dinámico. Por ello, cualquier cambio en la planificación (por ejemplo, la incorporación de una nueva herramienta de filtrado anti*phishing*) se evaluará en términos de impacto en el tiempo, el alcance, los costos y la calidad, asegurando que nada se altere sin la debida aprobación y sin mantener la coherencia global del proyecto.

10.7 Monitoreo, control y actualización

A medida que avance la planificación, revisaremos periódicamente este plan. Si surgen nuevas amenazas o necesidades, actualizaremos las directrices y notificaremos a los interesados clave, de modo que todos estén informados y preparados para ajustar el rumbo.

10.8 Aprobación del plan

Una vez revisado y entendido por los interesados clave, este plan requerirá la aprobación del Gerente General, lo cual confirmará el compromiso institucional con las estrategias y métodos aquí propuestos. Esta aprobación marcará el inicio formal de la fase de planificación detallada del proyecto de ciberseguridad.

10.9 Recopilación de requisitos para el proyecto de ciberseguridad

La fase de recopilación de requisitos es fundamental para establecer una base sólida en el diseño del proyecto de ciberseguridad de Lagobo Distribuciones S. A. S. Este proceso busca identificar todas las necesidades, expectativas y limitaciones para garantizar que la planificación cumpla con los objetivos estratégicos de la organización y permita implementar soluciones que respondan a los riesgos actuales y futuros.

10.9.1 Fuentes de información para los requisitos

Los requisitos se recopilaron de diversas áreas clave de la empresa y actores involucrados, asegurando que todas las perspectivas relevantes se consideren:

Alta Dirección

Gerente general: solicitó garantizar el cumplimiento de normativas internacionales como ISO/IEC 27001, reducir los incidentes cibernéticos en al menos un 80 % durante el primer año y reforzar la confianza de los clientes en la seguridad de la información que maneja la empresa.

Director del proyecto: indicó la necesidad de un sistema escalable que permita integrar nuevas herramientas en el futuro, además de establecer indicadores clave que midan la efectividad del proyecto, como tiempos de respuesta ante incidentes y reducción de intentos de acceso no autorizados.

Departamento de TI

Administrador de infraestructura: planteó la importancia de implementar herramientas avanzadas de monitoreo y detección, como sistemas IDS/IPS, y garantizar su compatibilidad con la infraestructura tecnológica actual.

Administrador de redes: resaltó la necesidad de segmentar la red corporativa para limitar accesos por departamento y reducir el impacto de posibles intrusiones. También propuso la instalación de *firewall*s actualizables que bloqueen amenazas externas y detecten actividades anómalas.

Otros

Consultores externos: sugirieron realizar una evaluación exhaustiva de las vulnerabilidades existentes y priorizar la protección de sistemas críticos en la sede principal, extendiéndola luego a las sucursales. También recomendaron incorporar autenticación multifactorial (MFA) y cifrado de datos para mayor seguridad.

Recursos humanos: propusieron diseñar un programa de formación práctico y accesible para todos los empleados, enfocado en concientizar sobre ciberseguridad y entrenar en la detección de amenazas como *phishing*.

Empleados: a través de encuestas y entrevistas, se identificó la necesidad de contar con herramientas fáciles de usar que no interfieran con las tareas diarias, además de guías claras sobre buenas prácticas, como el uso de contraseñas seguras y la prevención de riesgos comunes.

10.9.2 Métodos de recopilación de requisitos

Se emplearon diversas técnicas para obtener información relevante de manera estructurada y comprensiva:

- Entrevistas: reuniones individuales con la Gerencia General, el Director del Proyecto y responsables de TI para entender sus prioridades.
- Encuestas: aplicadas a los empleados para evaluar su percepción de las amenazas y su conocimiento actual sobre ciberseguridad.
- Observación directa: análisis de flujos de trabajo para detectar vulnerabilidades en el manejo diario de información.
- Revisión documental: análisis de políticas internas, normativas internacionales y auditorías anteriores.

- Talleres: sesiones colaborativas con equipos de TI y Recursos Humanos para priorizar necesidades.

10.9.3 Tipos de requisitos identificados

Funcionales

- Implementar IDS/IPS para monitorear el tráfico de red en tiempo real.
- Instalar autenticación multifactor (MFA) para accesos críticos y remotos.
- Aplicar cifrado a la información sensible, tanto en tránsito como en reposo.

No funcionales

- Asegurar la compatibilidad de las soluciones con la infraestructura actual.
- Garantizar un sistema accesible y fácil de usar para el personal.
- Diseñar herramientas escalables que permitan crecer según las necesidades futuras.

Formativos

- Cumplir con ISO/IEC 27001 y regulaciones locales sobre protección de datos personales.
- Incluir mecanismos de auditoría regular para validar el cumplimiento normativo.

Organizativos

- Capacitar al personal en ciberseguridad y fomentar una cultura organizacional comprometida con la seguridad digital.
- Definir roles y responsabilidades claras para la gestión de incidentes.

De calidad

- Reducir en un 90 % los intentos exitosos de intrusión.
- Establecer tiempo máximo de respuesta ante incidentes críticos, no superior a 5 minutos.

- Validar la efectividad de las medidas con auditorías trimestrales.

10.9.4 Resultados

Tras la recopilación y el análisis de los datos, se elaborará un “Documento de Requisitos” que sirva como guía central para la planificación del proyecto. Este documento incluirá:

- Detalles de cada requisito identificado, clasificado por tipo y área de impacto.
- Prioridades para cada requisito según su relevancia estratégica.
- Responsables y plazos asociados a cada categoría.

La recopilación de requisitos es una etapa crucial para asegurar que el proyecto de ciberseguridad en Lagobo Distribuciones S. A. S. no solo cumpla con las expectativas de la empresa, sino que también se adapte a las necesidades reales de su operación. Al comprender las prioridades de los interesados y las características de la infraestructura actual, podemos establecer las bases para un proyecto sólido y exitoso.

10.9.5 Definir el alcance

En el proyecto de planificación de la ejecución para el proyecto de ciberseguridad en Lagobo Distribuciones S. A. S., la definición del alcance permite establecer con precisión las actividades, entregables y objetivos específicos que guiarán las acciones. Este proceso garantiza que las áreas clave a abordar estén claramente identificadas y alineadas con las prioridades estratégicas de la organización, proporcionando una base sólida para diseñar soluciones que respondan a las necesidades actuales y futuras en materia de seguridad digital.

Aclaración del alcance

El proyecto abarca las siguientes actividades principales:

- Diagnóstico de infraestructura y análisis de riesgos:
    - Evaluar la infraestructura tecnológica actual en la sede principal y las 27 sucursales.

  - Identificar las vulnerabilidades más críticas y las amenazas potenciales que podrían afectar los sistemas operativos y los datos sensibles.
  - Revisar el grado de cumplimiento con normativas internacionales como ISO/IEC 27001 y las regulaciones locales de protección de datos.

- Definición de requerimientos técnicos y de seguridad:
  - Determinar las herramientas y tecnologías necesarias, como IDS/IPS, *firewall*s, autenticación multifactor (MFA) y cifrado de datos.
  - Diseñar políticas de seguridad y protocolos de respuesta ante incidentes adaptados a las necesidades de la organización.
- Diseño del plan de implementación:
  - Crear un plan estructurado que detalle las fases de implementación, priorizando la protección de los sistemas críticos.
  - Establecer un cronograma que permita la integración escalonada de las soluciones en la sede principal y las sucursales.
- Desarrollo del programa de capacitación:
  - Diseñar un programa de formación para todos los empleados, enfocado en buenas prácticas de ciberseguridad, como la prevención de ataques de *phishing* y el uso correcto de contraseñas.
  - Producir materiales educativos interactivos y adaptados a los diferentes roles dentro de la empresa.
- Establecimiento del sistema de monitoreo y definición de KPI:
  - Diseñar un sistema que permita supervisar continuamente el estado de seguridad de los sistemas y la red.
  - Definir indicadores clave de rendimiento (KPI) que midan la efectividad de las soluciones implementadas, como tiempos de respuesta ante amenazas o reducción de incidentes.

Exclusiones del alcance

Para garantizar un enfoque claro, se excluyen de este proyecto las siguientes actividades:

- La adquisición e instalación de hardware y *software*, que se abordarán en una fase posterior.
- Tareas operativas como el soporte continuo o mantenimiento de las soluciones implementadas.
- Cambios significativos en la infraestructura tecnológica existente.

Entregables del proyecto

Los principales productos generados en esta fase de planificación son:

- Informe de diagnóstico y análisis de riesgos: documento que identifica vulnerabilidades, evalúa riesgos y propone recomendaciones iniciales.
- Especificaciones de requerimientos técnicos y políticas de seguridad: Listado detallado de las herramientas, tecnologías y políticas necesarias para proteger los sistemas y datos sensibles.
- Plan de implementación de ciberseguridad: guía detallada que describe las fases, recursos, cronograma y metodología para ejecutar las soluciones de seguridad.
- Programa de capacitación: materiales educativos y cronogramas para formar al personal en ciberseguridad, incluyendo simulaciones de amenazas y buenas prácticas.
- Sistema de monitoreo y cuadro de KPI: modelo diseñado para evaluar la efectividad de las medidas de seguridad implementadas y supervisar la infraestructura tecnológica en tiempo real.

Validación del alcance

El alcance será revisado y aprobado por:

- Director del proyecto (Alexander Franco): responsable de asegurar que el alcance cumpla con los objetivos estratégicos de la organización.
- Gerente general/patrocinador: confirmará que el alcance refleja las prioridades de la empresa y se ajusta a las expectativas de los interesados clave.
- Departamento de TI y consultores externos: verificarán la viabilidad técnica de las actividades y entregables definidos.

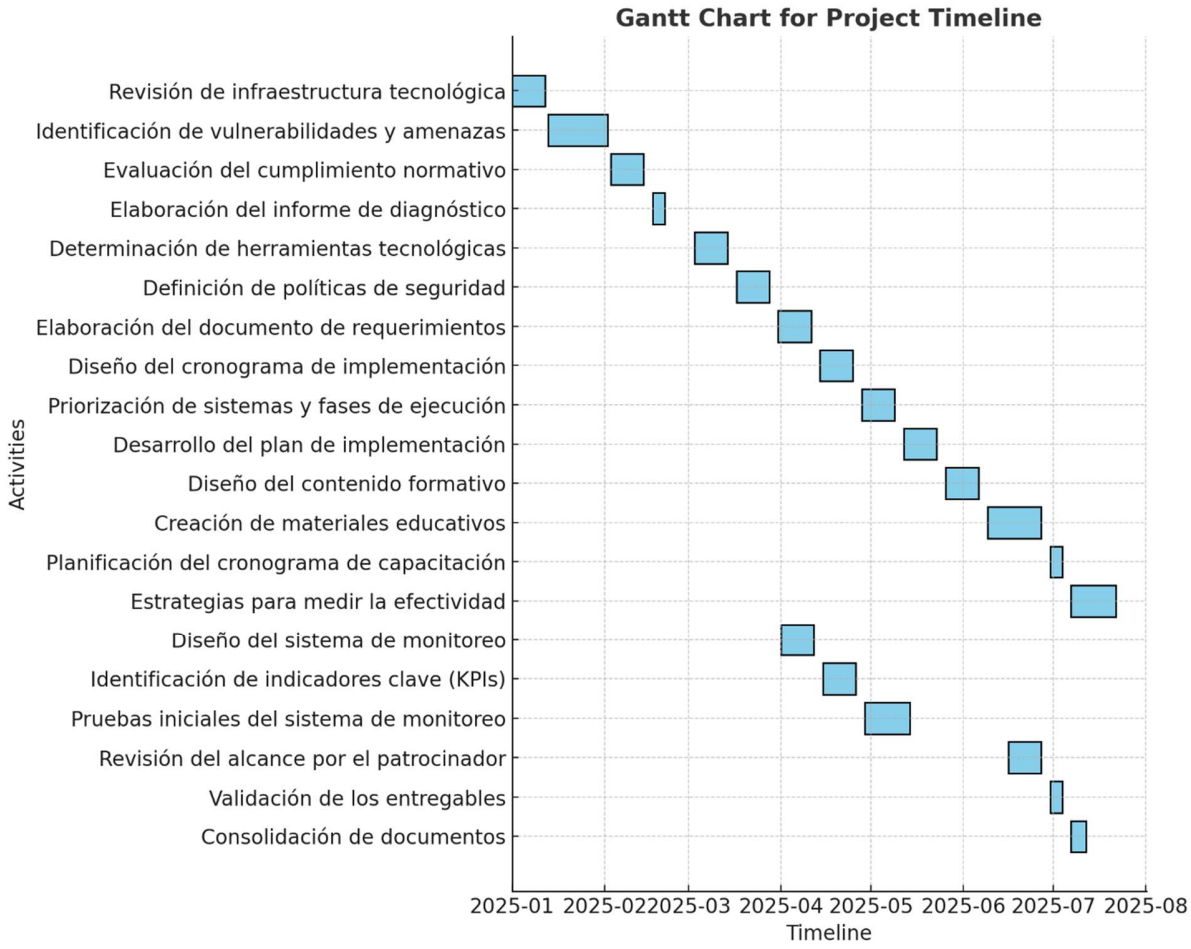
Límites del proyecto

El proyecto se limita a:

- Diagnosticar la situación actual y proponer soluciones viables.
- Diseñar estrategias y planes detallados para la implementación futura.
- Establecer programas de formación y protocolos de monitoreo.

No incluye tareas operativas relacionadas con la implementación o mantenimiento de las medidas planificadas, ya que estas se abordarán en fases posteriores.

Figura 2. *Diagrama de Gantt requisitos*



10.10 Estructura de desglose del trabajo (EDT)

La estructura de desglose del trabajo (EDT) es un componente esencial para organizar de manera jerárquica las tareas y actividades necesarias para llevar a cabo el proyecto de planificación de la ejecución del proyecto de ciberseguridad en Lagobo Distribuciones S. A. S. Este desglose permite asignar responsabilidades, estimar recursos, definir cronogramas y facilitar el seguimiento del progreso.

El propósito principal de la EDT es descomponer el proyecto en elementos manejables, proporcionando una visión clara de todas las actividades involucradas. Esto facilita la gestión, asignación de recursos y control de las diferentes tareas, asegurando que el proyecto cumpla con sus objetivos estratégicos dentro de los plazos y presupuestos establecidos.

10.10.1 Estructura jerárquica de la EDT

La estructura de desglose del trabajo se divide en los siguientes niveles:

Nivel 0. Proyecto de planificación de la ejecución del proyecto de ciberseguridad

Este nivel representa el objetivo global del proyecto: realizar una planificación efectiva y detallada que sirva como base para la futura implementación de las soluciones de ciberseguridad.

Nivel 1. Componentes principales del proyecto

a. Diagnóstico de infraestructura y análisis de riesgos.
b. Definición de requerimientos técnicos y de seguridad.
c. Diseño del plan de implementación.
d. Desarrollo del programa de capacitación y sensibilización.
e. Establecimiento del sistema de monitoreo y definición de KPI.
f. Gestión y validación del alcance y entregables.

Nivel 2. Subcomponentes detallados

a. Diagnóstico de infraestructura y análisis de riesgos.

b. Revisión de la infraestructura tecnológica existente (sede principal y 27 sucursales).
c. Identificación de vulnerabilidades y amenazas.
d. Evaluación del cumplimiento normativo con estándares internacionales (ISO/IEC27001) y regulaciones locales.
e. Elaboración del informe de diagnóstico.
f. Definición de requerimientos técnicos y de seguridad.
g. Determinación de herramientas tecnológicas necesarias: FortiGate 40G (27 unidades), ISL Online para soporte remoto, FortiSwitch de 24 puertos (8 unidades) y FortiAP (10 unidades).
h. Definición de políticas de seguridad organizacional: fortalecimiento del directorio activo y Políticas de control de hardware y *software*.
i. Priorización de sistemas críticos y fases de ejecución: configuración de SD-WAN para almacenes, integración de VPN site-to-site seguras, identificación y asignación de recursos necesarios, y desarrollo del plan de implementación detallado.
j. Desarrollo del programa de capacitación y sensibilización: diseño del contenido formativo adaptado a diferentes roles organizacionales y creación de materiales educativos interactivos (simulaciones, videos).
k. Planificación del cronograma de capacitación para todo el personal: estrategias para medir la efectividad de la capacitación y establecimiento del Sistema de Monitoreo y Definición de KPI.
l. Diseño del sistema de monitoreo en tiempo real: UTM FortiGate 100F (2 unidades), herramientas de monitoreo (SolarWinds, PRTG), identificación de indicadores clave de rendimiento (KPI) (tiempo de respuesta ante incidentes, reducción de amenazas detectadas, pruebas iniciales del sistema de monitoreo, elaboración del modelo de seguimiento y evaluación continua).
m. Gestión y validación del alcance y entregables: revisión del alcance definido con el patrocinador, validación de los entregables generados en cada etapa del proyecto y consolidación de documentos en un repositorio centralizado e implementación de dispositivos QNAP de 30 TB para respaldo de información.

Nivel 3. Tareas específicas por subcomponente

a. Diagnóstico de infraestructura: realizar inspecciones técnicas en sistemas críticos y documentar vulnerabilidades por prioridad.
b. Requerimientos técnicos: seleccionar tecnologías basadas en estándares de la industria y alinear políticas organizacionales con las normativas aplicables.
c. Implementación: crear cronogramas específicos para la configuración de redes SD-WAN y diseñar VPN seguras para la integración con proveedores de servicios en la nube.
d. Capacitación: diseñar simulaciones de ataques cibernéticos como ejercicios prácticos y crear guías específicas para uso de herramientas como EDR y XDR.
e. Monitoreo y KPI: configurar paneles de control personalizados para la visualización de métricas clave, y probar y validar las configuraciones del sistema de monitoreo en entornos controlados.
f. Validación: asegurar la entrega de los informes de alcance y estado del proyecto en tiempo y forma, y validar la integración de dispositivos QNAP para el cumplimiento de la ISO/IEC 27001.

10.10.2 Definición de las actividades

En el proyecto de planificación para la ejecución de un plan de ciberseguridad en Lagobo Distribuciones S. A. S., definir las actividades es un paso crítico que conecta los entregables de la Estructura de Desglose del Trabajo (EDT) con las tareas específicas necesarias para lograr los objetivos del proyecto. Este proceso detalla el trabajo que se debe realizar, asegurando una comprensión clara por parte de todos los involucrados y facilitando la programación, la asignación de recursos y el control del progreso.

Propósito y beneficios

Definir las actividades proporciona un desglose exhaustivo de lo que implica cada entregable, transformando los elementos de alto nivel en pasos concretos y manejables.

Este proceso permite establecer claridad en las tareas, en tanto cada actividad se define con un nivel de detalle suficiente para que el equipo de trabajo entienda qué se

debe hacer y cómo. Además, facilita la programación: un desglose claro permite asignar tiempos precisos a cada tarea y calcular los recursos necesarios. Así mismo, ayuda a mitigar riesgos: la descomposición ayuda a identificar posibles obstáculos o dependencias entre actividades, lo que permite gestionarlos con antelación y un control y monitoreo eficiente: una lista detallada de actividades facilita el seguimiento del progreso y el cumplimiento de los objetivos establecidos.

La EDT proporciona una visión jerárquica de los entregables del proyecto. El primer paso es analizar cada componente de la EDT para identificar las actividades necesarias para completarlo. Esto asegura que todas las tareas estén directamente vinculadas a los objetivos del proyecto.

El proceso de definir actividades se organiza en varias etapas clave:

- Descomposición de entregables: cada entregable se divide en tareas específicas. Estas actividades deben ser lo suficientemente detalladas para asignarse, programadas y monitoreadas, pero no tan pequeñas que compliquen la gestión.
- Validación de actividades: se revisan las actividades definidas con el equipo de trabajo y las partes interesadas clave para garantizar que reflejen las necesidades y objetivos del proyecto. Este paso asegura que no se omitan tareas importantes y que todas las actividades estén alineadas con los entregables.
- Documentación de las actividades: las actividades definidas se documentan utilizando un formato estándar que incluye su descripción, objetivos, resultados esperados, recursos necesarios y dependencias con otras tareas.

A continuación, se presenta el desglose detallado de las actividades necesarias para cada entregable:

Diagnóstico de infraestructura y análisis de riesgos

- Recopilar información técnica sobre infraestructura tecnológica en la sede principal y sucursales.
- Realizar inspecciones y evaluaciones técnicas de sistemas críticos.
- Identificar puntos vulnerables en la infraestructura física y virtual.
- Evaluar riesgos asociados a amenazas internas y externas.
- Generar un informe detallado con hallazgos y recomendaciones priorizadas.
- Definición de requerimientos técnicos y de seguridad
- Analizar herramientas tecnológicas disponibles en el mercado.
- Determinar especificaciones técnicas para sistemas de seguridad como IDS, MFA y *firewall*s.
- Diseñar políticas internas que promuevan la protección de datos sensibles.
- Elaborar un documento de requerimientos técnicos y operativos.
- Diseño del plan de implementación
- Crear un cronograma inicial que contemple todas las fases del proyecto.
- Priorizar los sistemas críticos y definir el orden de implementación.
- Identificar recursos humanos, financieros y tecnológicos requeridos.
- Redactar un plan detallado que incluya metodología, plazos y puntos de control.
- Desarrollo del programa de capacitación y sensibilización
- Diseñar módulos formativos adaptados a distintos niveles de conocimiento.

- Crear materiales educativos interactivos, como simulaciones de ataques y guías prácticas.
- Planificar un cronograma de capacitación que garantice la participación de todos los empleados.
- Evaluar el impacto de las capacitaciones a través de encuestas y análisis de desempeño.
- Establecimiento del sistema de monitoreo y definición de KPI.
- Diseñar una arquitectura de monitoreo que permita supervisar redes y sistemas en tiempo real.
- Definir indicadores clave de rendimiento (KPI) como tiempo de respuesta a incidentes y reducción de vulnerabilidades.
- Realizar pruebas piloto para validar la funcionalidad del sistema.
- Documentar un modelo de seguimiento que permita evaluar continuamente la efectividad de las medidas implementadas.

Gestión y validación del alcance y entregables

- Revisar el alcance del proyecto con el patrocinador para asegurar su alineación con los objetivos estratégicos.
- Validar los entregables en cada etapa para garantizar que cumplan con los estándares establecidos.
- Consolidar todos los documentos en un repositorio centralizado para referencia futura.

Herramientas y técnicas utilizadas

Para definir las actividades de manera efectiva, se emplean las siguientes herramientas y técnicas:

- Descomposición jerárquica: proceso para dividir los entregables en actividades más pequeñas y manejables.

- Listas de verificación: aseguran que todas las tareas necesarias sean consideradas.
- *Software* de gestión de proyectos: herramientas como Microsoft Project para documentar, organizar y rastrear actividades.
- Reuniones de equipo: facilitan la colaboración y validación de actividades con los involucrados.

Resultados del proceso

El resultado principal de este proceso es una lista detallada de actividades que se convierte en la base para el desarrollo del cronograma y la asignación de recursos en etapas posteriores.

Descripción de cada actividad.

- Dependencias y relaciones entre tareas.
- Identificación de recursos y tiempos estimados.
- Resultados esperados de cada actividad.

10.10.3 Secuenciación de las actividades

Secuenciar las actividades es una etapa clave dentro del grupo de procesos de planificación en la gestión de proyectos. Este proceso se centra en identificar y documentar las relaciones lógicas entre las actividades previamente definidas, estableciendo el orden en el que deben ejecutarse. En el caso del proyecto de planificación de la ejecución del plan de ciberseguridad para Lagobo Distribuciones S. A. S., esta etapa asegura una progresión lógica y eficiente del trabajo, permitiendo la creación de un cronograma realista.

Propósito y beneficios

El objetivo principal de secuenciar las actividades es organizar el trabajo de forma estructurada para maximizar la eficiencia y minimizar los riesgos de retrasos. Los beneficios de este proceso incluyen:

- Claridad en las dependencias: identificar cómo las tareas están interrelacionadas para garantizar que se ejecuten en el orden correcto.
- Creación de un cronograma eficiente: establecer un flujo de trabajo lógico facilita el desarrollo de un plan de tiempo viable.
- Gestión de riesgos: detectar dependencias críticas permite anticipar posibles cuellos de botella o retrasos.
- Optimización de recursos: alinear actividades con recursos disponibles para evitar solapamientos o ineficiencias.

Proceso de secuenciación

El proceso de secuenciación de actividades para este proyecto incluye los siguientes pasos:

- Identificación de dependencias: se revisan las actividades definidas para identificar dependencias entre ellas. Estas pueden ser:
- Dependencias obligatorias: relacionadas con la naturaleza del trabajo (por ejemplo, no se puede implementar un sistema de monitoreo antes de definir los requerimientos técnicos).
- Dependencias discrecionales: decisiones estratégicas tomadas por el equipo del proyecto.
- Dependencias externas: factores fuera del control del equipo del proyecto (como la disponibilidad de proveedores).

Tipos de relaciones

Las actividades se relacionan mediante los siguientes tipos de dependencias:

- Fin a comienzo (FS): una actividad debe terminar antes de que la siguiente comience (ej., completar el diagnóstico antes de definir los requerimientos).

- Comienzo a comienzo (SS): dos actividades pueden empezar simultáneamente (ej., creación de políticas y desarrollo del plan de implementación).
- Fin a fin (FF): dos actividades deben terminar al mismo tiempo (ej., pruebas piloto y validación del sistema).
- Comienzo a fin (SF): una actividad no puede finalizar hasta que otra haya comenzado (raro en este contexto).

10.10.4 Elaboración del diagrama de secuencia

Con base en las dependencias identificadas, se crea un diagrama lógico que visualiza las relaciones entre las actividades. Este diagrama ayuda a determinar el camino crítico y las áreas donde es necesario prestar mayor atención. A continuación, se presenta la secuencia lógica para las actividades clave del proyecto:

Diagnóstico de infraestructura y análisis de riesgos

- Revisión de la infraestructura tecnológica (FS) → Identificación de vulnerabilidades y amenazas.
- Identificación de vulnerabilidades y amenazas (FS) → Evaluación del cumplimiento normativo.
- Evaluación del cumplimiento normativo (FS) → Elaboración del informe de diagnóstico.

Definición de requerimientos técnicos y de seguridad

- Informe de diagnóstico (FS) → Determinación de herramientas tecnológicas.
- Determinación de herramientas tecnológicas (FS) → Definición de políticas de seguridad.
- Definición de políticas de seguridad (FS) → Elaboración del documento de requerimientos.

Diseño del plan de implementación

- Documento de requerimientos técnicos (FS) → Diseño del cronograma de implementación.
- Cronograma de implementación (FS) → Priorización de sistemas y fases.
- Priorización de sistemas y fases (FS) → Desarrollo del plan de implementación.
- *Desarrollo del programa de capacitación*
- Plan de implementación (SS) → Diseño del contenido formativo.
- Diseño del contenido formativo (FS) → Creación de materiales educativos.
- Creación de materiales educativos (FS) → Planificación del cronograma de capacitación.

Establecimiento del sistema de monitoreo

- Priorización de sistemas y fases (SS) → Diseño del sistema de monitoreo.
- Diseño del sistema de monitoreo (FS) → Identificación de indicadores clave (KPI).
- Identificación de indicadores clave (FS) → Pruebas iniciales del sistema de monitoreo.

Gestión y validación del alcance

- Validación del informe de diagnóstico (FS) → Revisión del alcance por el patrocinador.
- Revisión del alcance (FS) → Validación de los entregables.
- Validación de los entregables (FS) → Consolidación de documentos.

Herramientas y técnicas utilizadas

- Diagramas de red del proyecto: visualizan las relaciones entre actividades y dependencias.
- *Software* de gestión de proyectos: herramientas como Microsoft Project o herramientas en línea permiten crear diagramas y cronogramas automatizados.
- Reuniones colaborativas: facilitan la identificación de dependencias y la validación de relaciones entre tareas.

Resultados del proceso

El resultado principal de este proceso es un Diagrama de Secuencia de Actividades, que incluye:

- Relaciones lógicas entre las actividades.
- Identificación del camino crítico (actividades que determinan la duración total del proyecto).
- Base para desarrollar el cronograma del proyecto.

10.11 Estimación de recursos de las actividades con valoración económica

La estimación de recursos para el proyecto de planificación del plan de ciberseguridad de Lagobo Distribuciones S. A. S. incluye un desglose detallado de los recursos necesarios, asignación de valores económicos, y una distribución optimizada de los $200.000 USD destinados para dispositivos y licenciamientos. Además, se incorporan dos dispositivos QNAP de 30 TB cada uno para respaldos y custodia de información conforme a las directrices de la ISO 27001.

10.11.1 Diagnóstico de infraestructura y análisis de riesgos

Recursos humanos

- Especialista en ciberseguridad: $5.000 USD (1 mes).

- Analistas de TI (2): $8.000 USD (1 mes).
- Especialista en hacking ético: $6.000 USD (1 evaluación).

Tecnología

- Herramientas de monitoreo de red (PRTG, SolarWinds): $3.000 USD (licencias anuales).
- *Software* de pruebas de penetración (Metasploit, Burp Suite): $2.500 USD (licencias anuales).

Materiales

- Plantillas y bases de datos normativas: $500 USD.

Total diagnóstico: $25.000 USD

10.11.2 Definición de requerimientos técnicos y de seguridad

Recursos Humanos

- Consultor en ciberseguridad: $5.000 USD (1 mes).
- Administrador de sistemas: $4.000 USD (1 mes).
- Consultor en políticas de directorio activo: $3.500 USD (1 mes).

Tecnología

- FortiGate 40G (27 unidades): $54.000 USD ($2.000 USD por unidad).
- FortiSwitch de 24 puertos (8 unidades): $8.000 USD ($1.000 USD por unidad).
- FortiAP (10 unidades): $10.000 USD ($1.000 USD por unidad).

Materiales

- Documentación técnica y guías: $1.000 USD.

Total de requerimientos técnicos: $85.500 USD.

10.11.3 Diseño del plan de implementación

Recursos humanos

- Gerente de proyectos: $6.000 USD (1 mes).
- Ingeniero en ciberseguridad: $4.500 USD (1 mes).
- Arquitecto de red: $5.000 USD (1 mes).

Tecnología

- Licencias ISL Online: $3.000 USD (anuales).
- Herramientas de gestión de proyectos (Microsoft Project, Jira): $2.000 USD.

Materiales

- Plantillas y herramientas de planificación: $500 USD.

Total plan de implementación: $21.000 USD

10.11.4 Desarrollo del programa de capacitación y sensibilización

Recursos humanos

- Especialista en formación en ciberseguridad: $4.000 USD (1 mes).
- Diseñador multimedia: $3.500 USD (1 mes).

Tecnología

- Simuladores de ciberseguridad: $2.500 USD.
- Licencias de aprendizaje en línea: $1.500 USD.

Materiales

- Videos educativos, simulaciones y guías: $1.500 USD.

Total de capacitación: $13.000 USD

10.11.5 Establecimiento del sistema de monitoreo y definición de KPI

Recursos humanos

- Analista de seguridad: $4.000 USD (1 mes).
- Especialista en monitoreo de red: $4.000 USD (1 mes).

Tecnología

- UTM FortiGate 100F (2 unidades): $8.000 USD ($4.000 USD por unidad).
- Licencias EDR (400 equipos): $20.000 USD ($50 USD por unidad).
- Licencias XDR SentinelOne (10 servidores): $15.000 USD ($1.500 USD por unidad).
- Licencias EDR para dispositivos móviles (100 unidades): $5.000 USD ($50 USD por unidad).
- QNAP de 30 TB (2 unidades): $12.000 USD ($6.000 USD por unidad).

Materiales

- Manuales y guías de configuración: $500 USD.

Total de monitoreo y KPI: $68.500 USD

10.11.6 Gestión y validación del alcance y entregables

Recursos Humanos

- Patrocinador del proyecto: no aplica (interno).
- Gerente del proyecto: $3.000 USD (1 mes).

Tecnología

- Soluciones de colaboración en la nube con UTM integrado: $5.000 USD.

Materiales

- Documentación centralizada y validación: $500 USD.

Total de gestión y validación: $8.500 USD

Tabla 12. *Distribución total de los recursos*

Categoría	Costo (USD)
Diagnóstico de infraestructura	$25.000
Requerimientos técnicos	$85.500
Plan de implementación	$21.000
Capacitación	$13.000
Monitoreo y KPI	$68.500
Gestión y validación	$8.500
Total	$221.500

Tabla 13. *Matriz de recursos estimada para el proyecto de ciberseguridad*

	Categoría	Recursos Humanos (USD)	Tecnología y Equipos (USD)	Materiales (USD)	Total (USD)
0	Diagnóstico de Infraestructura y Análisis de Riesgos	$19.000	$ 5.500	$500	$25.000
1	Requerimientos Técnicos y de Seguridad	$12.500	$72.000	$1.000	$85.500
2	Plan de Implementación	$15.500	$5.000	$500	$21.000
3	Capacitación y Sensibilización	$7.500	$ 4.000	$1.500	$13.000
4	Monitoreo y KPI	$8.000	$60.000	$500	$68.500
5	Gestión y Validación del Alcance y Entregables	$3.000	$5.000	$500	$8.500
	Total General	$65.500	$151.500	$ 4.500	$221.500

10.12 Estimación de la duración de las actividades

Para el proyecto de planificación de la ejecución del plan de ciberseguridad en Lagobo Distribuciones S. A. S., la estimación de la duración de las actividades se ha realizado considerando un período de ejecución desde el 1 de enero de 2025 hasta el 31 de julio de 2025. Este cronograma asegura que todas las actividades se desarrollen de manera ordenada y con tiempo suficiente para alcanzar los objetivos definidos. La metodología para estimar la duración consiste en:

1. Revisión de la EDT: cada actividad en la Estructura de Desglose del Trabajo (EDT) se analiza para estimar su duración.
2. Juicio de expertos: se consultan especialistas internos y externos para validar las estimaciones.
3. Estimación análoga: se utilizan datos históricos de proyectos similares para ajustar las duraciones.
4. Técnica de tres valores: se calcula la duración considerando los escenarios optimista, probable y pesimista.

Tabla 14. *Actividades y duración estimada*

Actividad principal	Duración estimada	Fecha inicio	Fecha fin
Diagnóstico de Infraestructura y Análisis de Riesgos	40 días laborales	01/01/2025	28/02/2025
Revisión de infraestructura tecnológica	10 días	01/01/2025	12/01/2025
Identificación de vulnerabilidades y amenazas	15 días	13/01/2025	02/02/2025
Evaluación del cumplimiento normativo	10 días	03/02/2025	14/02/2025

Actividad principal	Duración estimada	Fecha inicio	Fecha fin
Elaboración del informe de diagnóstico	5 días	17/02/2025	21/02/2025
Definición de Requerimientos Técnicos y de Seguridad	30 días laborales	03/03/2025	11/04/2025
Determinación de herramientas tecnológicas	10 días	03/03/2025	14/03/2025
Definición de políticas de seguridad	10 días	17/03/2025	28/03/2025
Elaboración del documento de requerimientos	10 días	31/03/2025	11/04/2025
Diseño del Plan de Implementación	30 días laborales	14/04/2025	23/05/2025
Diseño del cronograma de implementación	10 días	14/04/2025	25/04/2025
Priorización de sistemas y fases de ejecución	10 días	28/04/2025	09/05/2025
Desarrollo del plan de implementación	10 días	12/05/2025	23/05/2025
Desarrollo del Programa de Capacitación	40 días laborales	26/05/2025	22/07/2025
Diseño del contenido formativo	10 días	26/05/2025	06/06/2025
Creación de materiales educativos	15 días	09/06/2025	27/06/2025

Actividad principal	Duración estimada	Fecha inicio	Fecha fin
Planificación del cronograma de capacitación	5 días	30/06/2025	04/07/2025
Estrategias para medir la efectividad	10 días	07/07/2025	22/07/2025
Establecimiento del Sistema de Monitoreo y KPI	30 días laborales	01/04/2025	14/05/2025
Diseño del sistema de monitoreo	10 días	01/04/2025	12/04/2025
Identificación de indicadores clave (KPI)	10 días	15/04/2025	26/04/2025
Pruebas iniciales del sistema de monitoreo	10 días	29/04/2025	14/05/2025
Gestión y Validación del Alcance y Entregables	20 días laborales	16/06/2025	12/07/2025
Revisión del alcance por el patrocinador	10 días	16/06/2025	27/06/2025
Validación de los entregables	5 días	30/06/2025	04/07/2025
Consolidación de documentos	5 días	07/07/2025	12/07/2025

En el cronograma propuesto, se distribuyen las actividades de manera equilibrada entre los meses de enero y julio de 2025, priorizando tareas críticas y asegurando un flujo de trabajo continuo. Se han considerado tiempos de buffer para manejar posibles contingencias y garantizar que el proyecto se mantenga dentro de los plazos establecidos.

12.13 Estimación de los costos

La estimación de costos en el proyecto de planificación del plan de ciberseguridad para Lagobo Distribuciones S. A. S. permite determinar el presupuesto necesario para ejecutar todas las actividades y asegurar el cumplimiento de los objetivos estratégicos. Este proceso incluye el cálculo de los costos directos e indirectos asociados a los recursos humanos, tecnología, equipos, materiales y servicios.

La metodología para la estimación de costos es una combinación de enfoques para obtener una estimación precisa, que consiste en: una estimación análoga basada en proyectos previos similares; estimación paramétrica, aplicando datos históricos para determinar costos unitarios; juicio de expertos, consultando a especialistas en ciberseguridad y gestión de proyectos; y estimación por rangos, considerando valores optimistas, probables y pesimistas para las actividades críticas.

Los costos se pueden categorizar así:

- Recursos humanos: el equipo necesario para ejecutar las actividades incluye roles especializados en ciberseguridad, redes, formación y gestión de proyectos. Los costos se calculan con base en tarifas promedio mensuales.
- Tecnología y equipos: incluye hardware (p. ej., FortiGate, switches, puntos de acceso), licencias de *software* (p. ej., EDR, XDR, ISL Online), y dispositivos de almacenamiento (p. ej., QNAP).
- Materiales: cubren materiales educativos, guías técnicas, plantillas y documentación de soporte.
- Servicios: incluyen soporte técnico, capacitación externa, y servicios en la nube como VPN site-to-site seguras.

Tabla 15. *Estimación de costos por actividad*

Actividad Principal	Recursos Humanos (USD)	Tecnología y Equipos (USD)	Materiales (USD)	Servicios (USD)	Total (USD)
Diagnóstico de Infraestructura y Análisis de Riesgos	$19.000	$5.500	$500	$0	$25.000
Definición de Requerimientos Técnicos y Seguridad	$12.500	$72.000	$1.000	$0	$85.500
Diseño del Plan de Implementación	$15.500	$5.000	$500	$0	$21.000
Desarrollo del Programa de Capacitación	$7.500	$4.000	$1.500	$0	$13.000
Establecimiento del Sistema de Monitoreo y KPI	$8.000	$60.000	$500	$0	$68.500
Gestión y Validación del Alcance y Entregables	$3.000	$5.000	$500	$0	$8.500

Tabla 16. *Distribución detallada de tecnología y equipos*

Recurso tecnológico	Cantidad	Costo Unitario (USD)	Costo Total (USD)
FortiGate 40G (Almacenes)	27	$2.000	$54.000
FortiSwitch de 24 puertos	8	$1.000	$8.000
FortiAP	10	$1.000	$10.000
UTM FortiGate 100F	2	$4.000	$8.000
Licencias EDR (400 equipos)	400	$50	$20.000
Licencias XDR SentinelOne (10 servidores)	10	$1.500	$15.000
Licencias EDR (100 dispositivos móviles)	100	$50	$5.000
QNAP 30TB	2	$6.000	$12.000
Herramientas de monitoreo (PRTG, SolarWinds)	1	$3.000	$3.000
ISL Online	1	$3.000	$3.000

Total de tecnología y equipos: $138.000 USD

Tabla 17. *Resumen general de costos*

Categoría	Costo total (USD)
Recursos Humanos	$65.500
Tecnología y Equipos	$138.000
Materiales	$4.500
Servicios	$0
Total general	$200.000

10.14 Presupuesto

La determinación del presupuesto en el proyecto de planificación para la ejecución del plan de ciberseguridad en Lagobo Distribuciones S. A. S. se realiza consolidando las estimaciones de costos obtenidas para todas las actividades, integrando los costos directos e indirectos, y considerando una reserva de contingencia para mitigar riesgos identificados. Este presupuesto es un componente fundamental del plan de dirección del proyecto, permitiendo la gestión financiera efectiva durante la ejecución.

Los objetivos de la determinación del presupuesto son:

- Consolidar las estimaciones de costos realizadas en los procesos previos.
- Proveer un marco financiero para el monitoreo y control de los costos del proyecto.
- Asegurar la disponibilidad de recursos financieros para la ejecución exitosa del proyecto.
- Integrar una reserva de contingencia que permita responder a riesgos y cambios.

El presupuesto está compuesto por costos directos e indirectos. Entre los primeros se encuentran los recursos humanos, que incluyen salarios, tarifas y honorarios para especialistas, consultores y personal de soporte; luego está el ítem de tecnología y equipos como hardware, *software*, licencias, herramientas y dispositivos especializados y por último, los materiales que pueden ser guías educativas, plantillas, documentación técnica y recursos para capacitación.

Por su parte, en los costos indirectos se encuentran los gastos administrativos, soporte técnico adicional y costos operativos asociados al proyecto; la reserva de contingencia; un porcentaje del presupuesto total para mitigar riesgos identificados, y la reserva de gestión (opcional). Además de un monto adicional destinado a abordar riesgos no identificados.

Tabla 18. *Presupuesto consolidado*

Categoría	Costo estimado (USD)
Recursos humanos	$65.500
Tecnología y equipos	$138.000
Materiales	$4.500
Servicios	$0
Reserva de contingencia (10% del total)	$20.000
Total general	$228.000

Tabla 19. *Presupuesto detallado por actividad*

Actividad principal	**Presupuesto (USD)**
Diagnóstico de infraestructura	$25.000
Definición de requerimientos técnicos	$85.500
Diseño del plan de implementación	$21.000
Desarrollo del programa de capacitación	$13.000
Establecimiento del sistema de monitoreo	$68.500
Gestión y validación del alcance	$8.500
Subtotal	$221.500
Reserva de contingencia	$20.000
Total general	$228.000

El presupuesto se distribuye de manera equilibrada en los siete meses que comprende la ejecución del proyecto (enero a julio de 2025). La asignación mensual está alineada con el cronograma de actividades.

Tabla 20. *Distribución del presupuesto por porcentajes*

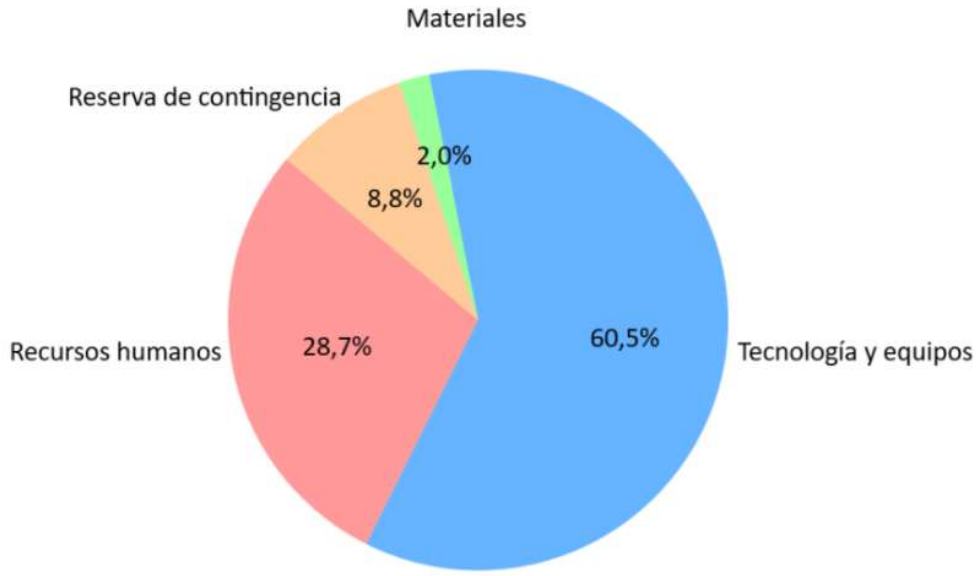
Mes	Porcentaje (%)	Monto (USD)
Enero 2025	15%	$34.200
Febrero 2025	10%	$22.800
Marzo 2025	20%	$45.600
Abril 2025	15%	$34.200
Mayo 2025	20%	$45.600
Junio 2025	10%	$22.800
Julio 2025	10%	$22.800
Total general	100%	$228.000

Las herramientas utilizadas en la determinación del presupuesto son:

a. Estimación por rangos: basada en valores optimistas, probables y pesimistas.
b. Análisis de reservas: para calcular la contingencia del 10%.
c. Reuniones colaborativas: con el equipo del proyecto para validar costos.
d. *Software* de gestión de proyectos: Microsoft Project o Jira para integrar costos al cronograma.

El presupuesto consolidado de $228.000 USD incluye todos los costos necesarios para la ejecución del proyecto, distribuidos en actividades específicas y asignaciones temporales. La integración de una reserva de contingencia permite mitigar riesgos y manejar cambios, garantizando una gestión financiera eficaz durante el proyecto.

Figura 3. *Distribución del presupuesto por categoría*



10.15 Planificación de la calidad

La planificación de la calidad en el proyecto de ciberseguridad para Lagobo Distribuciones S. A. S. asegura que los entregables cumplan con los estándares establecidos y que los procesos del proyecto estén alineados con las mejores prácticas. Este proceso, definido en el capítulo de planificación del PMBOK (7ª edición), permite identificar los estándares de calidad relevantes para el proyecto, documentar cómo se cumplirán y garantizar que los objetivos del proyecto se alcancen de manera eficiente.

Los propósitos de la planificación de la calidad son:

a. Identificar los estándares de calidad aplicables al proyecto.
b. Diseñar actividades para garantizar el cumplimiento de esos estándares.
c. Establecer criterios claros de aceptación para los entregables.
d. Integrar la gestión de la calidad con los procesos de planificación, ejecución y monitoreo.

10.15.1 Enfoque de la planificación de la calidad en el proyecto

Estándares de calidad

- ISO/IEC 27001: para la gestión de seguridad de la información.
- PMBOK 7ª edición: para la dirección estructurada del proyecto.
- NIST Cybersecurity Framework: como referencia técnica en la implementación de ciberseguridad.

Requisitos de calidad del proyecto

- Cumplimiento del alcance definido.
- Entregables que cumplan con los estándares normativos y técnicos.
- Documentación clara y validada.
- Infraestructura tecnológica alineada con las políticas organizacionales.

Planificación de actividades de calidad

La planificación de aseguramiento de la calidad conlleva actividades diseñadas para garantizar que los procesos utilizados en el proyecto son adecuados:

- Revisiones de procesos: validar que las actividades del proyecto siguen los procedimientos definidos.
- Auditorías internas: evaluaciones periódicas del cumplimiento normativo y técnico.
- Capacitación: formación del equipo en estándares aplicables.

Control de la calidad

Las actividades para monitorear los resultados del proyecto y verificar que cumplen con los estándares son

- Pruebas de aceptación: validación de configuraciones técnicas como SD-WAN, EDR y XDR.

- Evaluación de entregables: comparar los resultados con los criterios definidos.
- Revisión de documentación: asegurar que todos los entregables documentales cumplen con los estándares establecidos.

Herramientas y técnicas utilizadas

- Juicio de expertos: consultas con especialistas en ciberseguridad y gestión de calidad.
- Reuniones de planificación: talleres colaborativos para definir los criterios de calidad.
- Listas de verificación: para garantizar que se cumplan los requisitos de calidad en cada etapa.
- Análisis costo-beneficio: evaluar el impacto financiero de cumplir con los estándares de calidad.

Tabla 21. *Matriz de criterios de calidad*

Área	**Criterio de calidad**	**Método de verificación**
Diagnóstico de infraestructura	Informe técnico validado	Auditoría interna
Políticas de seguridad	Alineación con ISO/IEC 27001	Revisión por el equipo de ciberseguridad
Implementación de tecnologías	Configuración correcta de dispositivos y redes	Pruebas de aceptación
Documentación del proyecto	Claridad, completitud y precisión	Revisión técnica
Programa de capacitación	Contenido alineado con los objetivos de aprendizaje	Encuestas y simulaciones

10.15.2 Entregables del proceso de planificación de la calidad

Plan de gestión de la calidad

- Documento que describe cómo se implementarán las políticas y procedimientos de calidad.
- Incluye criterios de aceptación, estándares aplicables y roles responsables.

Matriz de control de calidad

- Registro de actividades específicas para verificar el cumplimiento de los estándares.

Informes de calidad

- Resultados de auditorías, revisiones y pruebas realizadas.

Integración con otros procesos

La planificación de la calidad está estrechamente vinculada con:

- Gestión del alcance: para garantizar que los entregables cumplan los requisitos definidos.
- Gestión del cronograma: para integrar actividades de aseguramiento de calidad dentro del plan del proyecto.
- Gestión de riesgos: para identificar y mitigar posibles fallos en la calidad.
- Gestión de recursos: para capacitar al equipo y asignar expertos en calidad.

La planificación de la calidad en este proyecto establece un enfoque estructurado y alineado con los estándares internacionales para garantizar que los entregables y procesos sean efectivos y cumplan con las expectativas del cliente. Este enfoque asegura que el proyecto se desarrolle con un alto nivel de calidad, reduciendo riesgos y maximizando el valor entregado a Lagobo Distribuciones S. A. S.

10.16 Desarrollo del plan de recursos humanos

El desarrollo del plan de recursos humanos para el proyecto de planificación de la ejecución del plan de ciberseguridad en Lagobo Distribuciones S. A. S. establece la estrategia para identificar, adquirir, desarrollar y gestionar el equipo necesario. Este proceso, alineado con las mejores prácticas descritas en el capítulo de planificación del PMBOK (7ª edición), garantiza que las capacidades y habilidades del equipo cumplan con los requerimientos del proyecto.

Los objetivos del plan de recursos humanos son:

a. Identificar roles y responsabilidades necesarios para el proyecto.
b. Planificar la adquisición de talento especializado en ciberseguridad.
c. Establecer estrategias de desarrollo y capacitación del equipo.
d. Documentar la estructura organizativa del proyecto y los procesos de gestión del equipo.

Por su parte, cada actividad definida en la EDT requiere un equipo de recursos humanos especializado; en la Tabla 22 se muestran los roles necesarios identificados para este proyecto.

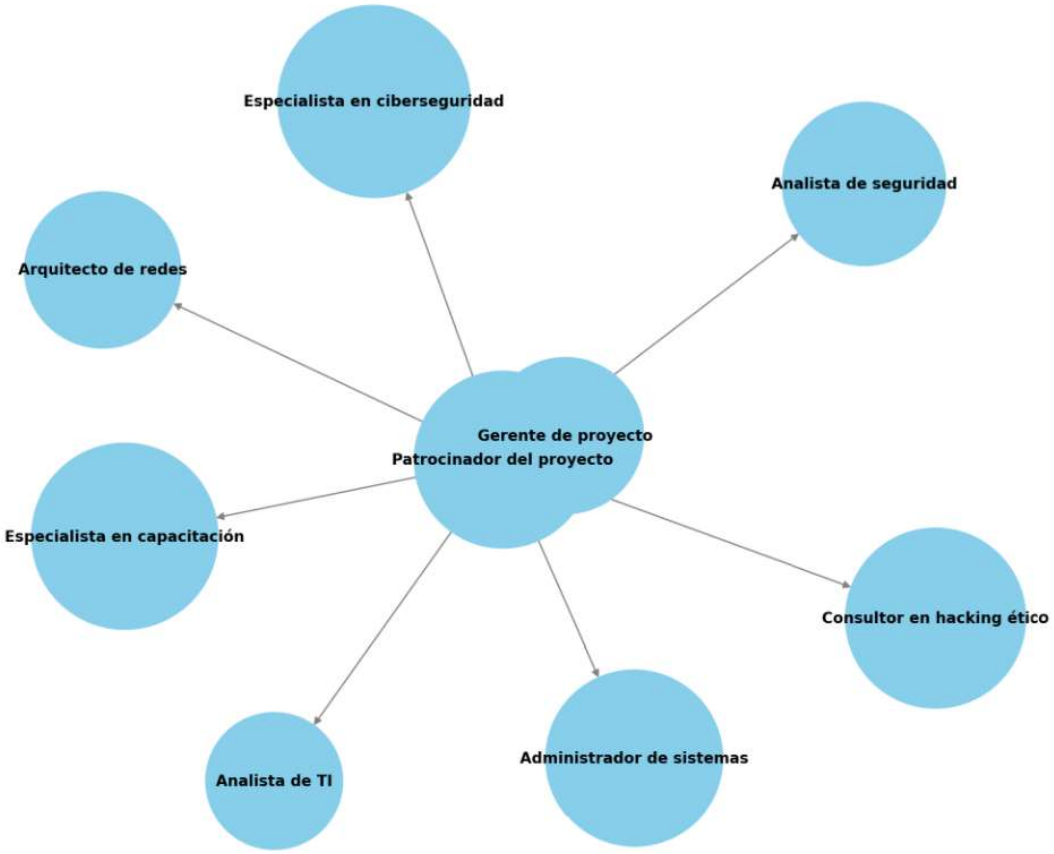
Tabla 22. *Roles y responsabilidades*

Rol	Responsabilidades
Gerente de proyecto	Liderar la planificación, supervisión y control del proyecto.
Especialista en ciberseguridad	Diseñar, implementar y validar soluciones técnicas y políticas de seguridad.
Analista de TI	Evaluar la infraestructura tecnológica y participar en el diagnóstico inicial.
Consultor en hacking ético	Realizar pruebas de penetración y análisis de vulnerabilidades.
Arquitecto de redes	Diseñar e implementar redes SD-WAN y VPN site-to-site.
Especialista en capacitación	Desarrollar y ejecutar el programa de formación en ciberseguridad para el personal.
Administrador de sistemas	Gestionar configuraciones de hardware, *software* y políticas del directorio activo.
Analista de seguridad	Configurar sistemas de monitoreo y evaluar KPI.

10.16.1 Estructura organizacional del proyecto

La estructura organizativa para este proyecto sigue un modelo funcional, donde cada especialista reporta al gerente del proyecto. El gerente coordina con los patrocinadores y asegura que los entregables se cumplan según los estándares definidos.

Figura 4. *Estructura organizacional del proyecto*



10.16.2 Adquisición de talento

El proyecto combina recursos internos de Lagobo Distribuciones S. A. S. y contrataciones externas.

- Internos: analistas de TI, administradores de sistemas, y gerentes de proyecto disponibles dentro de la organización.
- Externos: consultores especializados en hacking ético, arquitectos de redes y especialistas en ciberseguridad.

Desarrollo del equipo

El desarrollo del equipo incluye actividades para garantizar que todos los recursos humanos estén capacitados y alineados con los objetivos del proyecto:

- Capacitación técnica: cursos específicos sobre las herramientas y soluciones de seguridad implementadas (ej., FortiGate, SentinelOne).
- Simulaciones de ciberseguridad: ejercicios prácticos para mejorar las capacidades de respuesta a incidentes.
- Integración del equipo: talleres de trabajo colaborativo para alinear expectativas y roles.

Herramientas y técnicas utilizadas

- Juicio de expertos: consultar líderes de áreas técnicas para identificar competencias clave.
- Análisis de habilidades: evaluar las capacidades actuales del equipo para determinar brechas.
- Talleres de planificación: sesiones colaborativas para definir roles, responsabilidades y expectativas.
- Matrices RACI: herramienta para clarificar las responsabilidades de cada miembro en actividades específicas.

Tabla 23. *Matriz RACI (responsable, aprobador, consultado, informado)*

Actividad	Gerente de proyecto	Especialista en ciberseguridad	Analista de TI	Hacking ético	Arquitecto de redes
Diagnóstico de infraestructura	A	R	R	C	C
Definición de requerimientos técnicos	A	R	C	C	C
Diseño del plan de implementación	A	R	C	C	R
Desarrollo del programa de capacitación	A	R	C	C	C
Establecimiento del sistema de monitoreo	A	R	C	C	R

Gestión del equipo

La motivación del equipo debe aplicarse para el éxito del proyecto a través de las siguientes estrategias:

- Reconocimientos: incentivos no financieros como certificados de participación y reconocimiento interno.

- Oportunidades de desarrollo: participación en proyectos futuros de ciberseguridad dentro de la empresa.
- Evaluación del desempeño
- Indicadores clave: monitoreo de la contribución individual y el cumplimiento de los objetivos asignados.
- Revisión periódica: evaluaciones semanales durante las reuniones de avance.

Entregables del plan de recursos humanos

- Plan de adquisición de recursos: detalla los roles necesarios y el cronograma de contratación.
- Plan de capacitación: actividades de desarrollo para garantizar que el equipo tenga las habilidades requeridas.
- Matriz RACI: herramienta para gestionar responsabilidades.
- Estructura organizativa: visualización jerárquica de los roles en el proyecto.

El plan de recursos humanos garantiza que el proyecto cuente con un equipo calificado y comprometido, alineado con los objetivos estratégicos y los estándares de calidad. Este enfoque asegura que las actividades se realicen de manera eficiente, maximizando el uso de recursos internos y externos.

10.17 Planificación de las comunicaciones

La planificación de las comunicaciones en el proyecto de ciberseguridad para Lagobo Distribuciones S. A. S. garantiza el flujo eficiente de información entre todas las partes interesadas, promoviendo la transparencia y la toma de decisiones informadas. Este proceso, alineado con los principios del capítulo de planificación del PMBOK (7ª edición), define cómo se recopilará, generará, almacenará y difundirá la información del proyecto.

Los objetivos de planificar las comunicaciones son:

- Asegurar que los interesados reciban la información adecuada, en el momento correcto y con el nivel de detalle necesario.
- Minimizar malentendidos mediante canales de comunicación claros y efectivos.
- Facilitar el seguimiento y la coordinación entre los diferentes equipos involucrados.

Los componentes del plan de comunicaciones considerados para este proyecto son:

- Identificación de las necesidades de información
- Se realiza un análisis de los interesados para determinar sus necesidades de comunicación, considerando:
- Patrocinadores: información estratégica sobre el progreso del proyecto.
- Equipo del proyecto: detalles técnicos y actualizaciones operativas.
- Proveedores externos: especificaciones y requisitos técnicos.
- Usuarios finales: programas de capacitación y sensibilización.

Los métodos de comunicación que resultan útiles para para este proyecto incluyen:

- Reuniones cara a cara: para discusiones estratégicas y validación de entregables.
- Herramientas colaborativas: uso de plataformas como Microsoft Teams y Google Workspace.
- Reportes periódicos: documentos estructurados para informar sobre el avance, riesgos y logros.
- Mensajes instantáneos: para consultas rápidas y resolución de problemas operativos.

Entre las tecnologías y herramientas de comunicación que se pueden utilizar se encuentran:

- Correo electrónico: para notificaciones y actualizaciones formales.
- Videoconferencias: para reuniones con equipos remotos.
- Sistemas de gestión de proyectos: como Jira o Microsoft Project para centralizar información.

Tabla 24. *Matriz de planificación de las comunicaciones*

Interesado	Tipo de información	Método de comunicación	Frecuencia	Responsable
Patrocinador del proyecto	Resumen ejecutivo del progreso	Reuniones y reportes formales	Mensual	Gerente de proyecto
Equipo de ciberseguridad	Detalles técnicos y tareas asignadas	Reuniones técnicas, emails	Semanal	Gerente de proyecto
Proveedores externos	Especificaciones técnicas y requisitos	Correos electrónicos, reuniones	Según necesidad	Especialista en ciberseguridad
Usuarios finales	Información sobre capacitación y sensibilización	Videoconferencias, manuales	Mensual	Especialista en capacitación
Equipo de monitoreo	Reportes de indicadores clave (KPI)	Dashboards, informes periódicos	Quincenal	Analista de seguridad

Se identifican una serie de factores críticos que son claves para el éxito del proyecto, a saber:

- Claridad de mensajes: garantizar que la información sea fácil de entender para todos los interesados.
- Accesibilidad: asegurar que todos los interesados tengan acceso a los canales y herramientas de comunicación.
- Frecuencia adecuada: proporcionar información en los momentos adecuados sin saturar a los interesados.
- Seguimiento y respuesta: asegurar que las consultas y dudas sean atendidas con prontitud.

Del mismo modo, se considera un ciclo de vida de las comunicaciones planeadas en el proyecto:

- Inicio: establecer las necesidades y objetivos de comunicación.
- Planificación: documentar el plan de comunicaciones, incluyendo métodos y frecuencia.
- Ejecución: implementar el plan mediante reuniones, reportes y actualizaciones.
- Monitoreo: evaluar la efectividad del plan y ajustar según sea necesario.

La planificación de las comunicaciones está interrelacionada con otros planes, entre los cuales están:

- Gestión de interesados: asegurar que las necesidades de información de cada parte sean atendidas.
- Gestión de riesgos: informar oportunamente sobre riesgos y sus respuestas.
- Gestión del cronograma: actualizar a los interesados sobre cambios y avances en el cronograma.

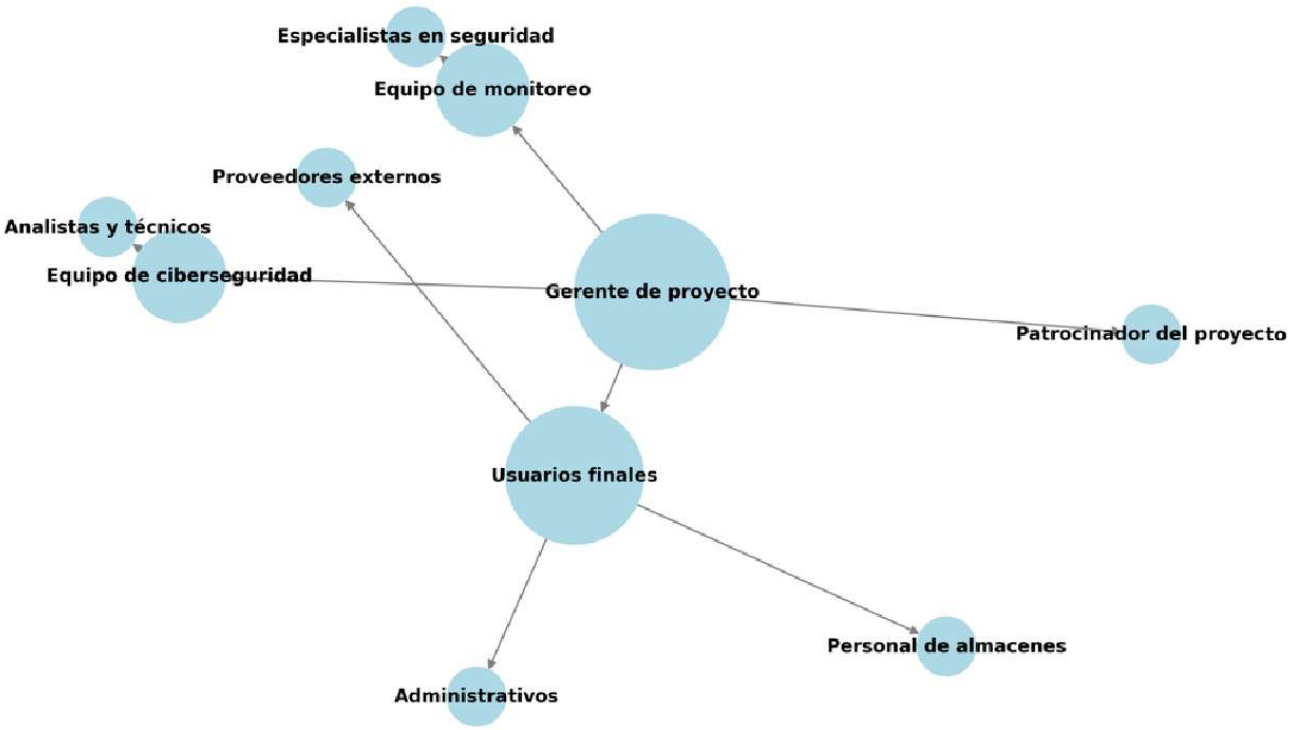
Los entregables del plan de comunicaciones son:

- Plan de gestión de las comunicaciones: documento que detalla las estrategias y procesos de comunicación.

- Calendario de comunicaciones: cronograma con las fechas clave para reuniones, reportes y capacitaciones.
- Plantillas de reportes: diseños estructurados para facilitar la estandarización de la información.

De esta manera, el plan de comunicaciones asegura que toda la información fluya de manera eficiente entre los interesados del proyecto, minimizando malentendidos y facilitando la toma de decisiones informadas. Esta planificación es clave para el éxito del proyecto de ciberseguridad en Lagobo Distribuciones S. A. S.

Figura 5. *Flujo de comunicaciones*



10.18 Planificación de la gestión de riesgos

La planificación de la gestión de riesgos en el proyecto de ciberseguridad para Lagobo Distribuciones S. A. S. implica identificar, analizar, planificar respuestas y monitorear los riesgos que puedan impactar los objetivos del proyecto. Este proceso, alineado con el capítulo de planificación del PMBOK (7ª edición), asegura que el proyecto esté preparado para abordar incertidumbres de manera efectiva. Los objetivos de la planificación de la gestión de riesgos se listan a continuación:

- Identificar posibles riesgos que puedan afectar el proyecto.
- Analizar y priorizar los riesgos según su impacto y probabilidad.
- Diseñar estrategias de respuesta proactivas y reactivas.
- Integrar la gestión de riesgos con otros procesos del proyecto.

El plan de gestión de riesgos debe construirse considerando:

- Entrevistas con expertos.
- Revisión de documentación técnica y normativa.
- Lecciones aprendidas de proyectos anteriores.
- Ejemplos de riesgos específicos para este proyecto:
- Riesgos técnicos: fallos en la implementación de *firewall*s, EDR o SD-WAN.
- Riesgos operativos: falta de capacitación adecuada para los usuarios finales.
- Riesgos externos: ataques cibernéticos mientras se implementa el plan.
- Riesgos organizacionales: cambios en las políticas internas que afecten los procesos.

Además, debe llevarse a cabo el análisis de riesgos tanto cualitativo como cuantitativo. El primero se refiere a la priorización de riesgos según probabilidad e impacto utilizando matrices de riesgos, y el segundo, a las estimaciones numéricas del

impacto financiero o temporal de los riesgos. En este orden, también se diseñan estrategias específicas según el tipo de riesgo, como:

- Evitar: cambiar el plan para eliminar el riesgo (ej., preconfigurar dispositivos antes de la implementación).
- Mitigar: reducir la probabilidad o el impacto (ej., capacitación intensiva para usuarios).
- Transferir: delegar el impacto a un tercero (ej., contratar seguros para la infraestructura crítica).
- Aceptar: aceptar el riesgo y establecer un plan de contingencia.

Sumado a lo anterior, las herramientas y técnicas que se han considerado para la gestión de riesgos son:

- Juicio de expertos: consultar especialistas en ciberseguridad y gestión de proyectos.
- Análisis FODA (Fortalezas, Oportunidades, Debilidades y Amenazas): para identificar riesgos estratégicos.
- Matrices de probabilidad e impacto: clasificar riesgos según su criticidad.
- Diagramas de causa-efecto: para entender la raíz de los riesgos.

Tabla 25. *Matriz de riesgos del proyecto*

Riesgo	Tipo	Impacto	Probabilidad	Estrategia	Plan de respuesta
Fallo en la configuración de *firewall*s	Técnico	Alto	Media	Mitigar	Realizar pruebas piloto previas.
Capacitación insuficiente para usuarios	Operativo	Medio	Alta	Mitigar	Implementar sesiones adicionales.
Ataques cibernéticos durante la implementación	Externo	Alto	Baja	Transferir	Contratar seguros para la red.
Cambios en políticas internas	Organizacional	Medio	Media	Evitar	Involucrar a la alta gerencia.
Escasez de hardware especializado	Logístico	Alto	Baja	Aceptar	Ajustar cronograma de entrega.

10.18.1 Ciclo de gestión de riesgos

Este ciclo tiene varias etapas importantes, de las cuales pueden resultar documentos, resultados de cada subproceso.

1. Planificar: crear el plan de gestión de riesgos.
2. Identificar: detectar riesgos específicos del proyecto.
3. Analizar: evaluar el impacto y la probabilidad de los riesgos.
4. Planificar Respuestas: diseñar estrategias de mitigación o contingencia.
5. Monitorear: revisar y actualizar la lista de riesgos a lo largo del proyecto.

Los documentos que reflejan los resultados de estas etapas del ciclo de gestión de riesgos pueden ser:

1. Plan de gestión de riesgos: documento que describe las estrategias, herramientas y procesos para gestionar los riesgos.
2. Registro de riesgos: lista detallada de todos los riesgos identificados, con su análisis y respuesta planeada.
3. Matriz de probabilidad e impacto: representación gráfica de la priorización de riesgos.
4. Planes de contingencia: estrategias detalladas para abordar riesgos específicos.

Sumado a esto, es posible que se dé la integración con otros planes, por ejemplo: en la gestión del cronograma se hacen ajustes necesarios para manejar riesgos relacionados con tiempos de entrega; en la gestión de los costos se programa una reserva de contingencia para cubrir riesgos financieros, y en la gestión de los interesados se procura mantener informados a los interesados sobre riesgos y respuestas.

La planificación de la gestión de riesgos proporciona un enfoque estructurado para identificar y mitigar los riesgos que puedan impactar el éxito del proyecto. Al integrar estas actividades con otros procesos del proyecto, se mejora la capacidad de respuesta y se garantiza la resiliencia del proyecto de ciberseguridad en Lagobo Distribuciones S. A. S.

10.19 Planificación de las adquisiciones

La planificación de adquisiciones en el proyecto de ciberseguridad para Lagobo Distribuciones S. A. S. implica determinar qué recursos, bienes y servicios se adquirirán externamente, así como desarrollar un plan para gestionar estas adquisiciones. Este proceso, alineado con el capítulo de planificación del PMBOK (7ª edición), asegura que las adquisiciones cumplan con los objetivos del proyecto y se gestionen de manera eficiente. Los objetivos de la planificación de adquisiciones son:

- Identificar bienes, servicios y recursos que no pueden proporcionarse internamente.
- Establecer las especificaciones técnicas y requisitos para cada adquisición.
- Definir un enfoque estratégico para la contratación y selección de proveedores.
- Garantizar que las adquisiciones se alineen con el cronograma, presupuesto y estándares del proyecto.

Se identifican los elementos clave que deben adquirirse para implementar el proyecto:

- Hardware y dispositivos:
  - 27 FortiGate 40G para almacenes.
  - 2 UTM FortiGate 100F para sedes administrativas.
  - 8 switches FortiSwitch de 24 puertos.
  - 10 puntos de acceso inalámbrico FortiAP.
  - 2 dispositivos QNAP de 30 TB para respaldo.
- *Software* y licencias:
  - Licencias EDR para 400 equipos de cómputo y 100 dispositivos móviles.
  - 10 licencias XDR SentinelOne para servidores.
  - ISL Online para sesiones remotas de soporte.
- Servicios:
  - Consultoría en hacking ético.
  - Implementación de VPN site-to-site seguras con proveedores de nube.

La estrategia de adquisición define cómo se seleccionarán y contratarán los bienes y servicios:

- Contratación directa: para proveedores certificados en tecnologías específicas como Fortinet.
- Licitación: para servicios de consultoría y capacitación.
- Contratos marco: para adquisiciones recurrentes, como licencias de *software*.

Cada adquisición debe cumplir con las siguientes especificaciones:

- Hardware: compatibilidad con la infraestructura actual y estándares como ISO/IEC 27001.
- *Software*: licencias válidas para el período del proyecto y alineación con las políticas de seguridad.
- Servicios: experiencia demostrada en ciberseguridad y cumplimiento con normativas locales.

El plan de adquisiciones debe incluir:

- Especificaciones técnicas: requisitos detallados para cada producto o servicio.
- Criterios de selección de proveedores: experiencia, costo, cumplimiento técnico y tiempos de entrega.
- Cronograma de adquisiciones: fechas clave para solicitudes, evaluaciones y entregas.

Tabla 26. *Matriz de adquisiciones*

Elemento	Cantidad	Método de adquisición	Criterios de selección	Proveedor potencial
FortiGate 40G	27	Contratación directa	Compatibilidad, precio, soporte técnico	Proveedor autorizado
UTM FortiGate 100F	2	Contratación directa	Soporte avanzado, integración	Proveedor autorizado
FortiSwitch de 24 puertos	8	Licitación	Capacidad, costo	Distribuidores locales
FortiAP	10	Contratación directa	Compatibilidad, soporte técnico	Proveedor autorizado
QNAP de 30 TB	2	Licitación	Capacidad, seguridad	Distribuidores de TI
Licencias EDR (400 equipos)	400	Contratos marco	Costo por licencia, cobertura	Proveedor de *software*
Licencias XDR SentinelOne	10	Contratos marco	Seguridad avanzada, costo por servidor	Proveedor de *software*
Consultoría en Hacking Ético	1	Licitación	Experiencia, certificaciones	Consultoras especializadas
ISL Online	1	Contratación directa	Usabilidad, costo	Proveedor de *software*

El ciclo de vida de las adquisiciones consiste en:

- Planificación: definir qué adquirir, cuándo y cómo.
- Selección de proveedores: evaluar propuestas y adjudicar contratos.
- Gestión de contratos: supervisar el cumplimiento de los acuerdos.
- Cierre de contratos: confirmar la entrega de bienes y servicios según lo especificado.

Las herramientas y técnicas para planificar adquisiciones son:

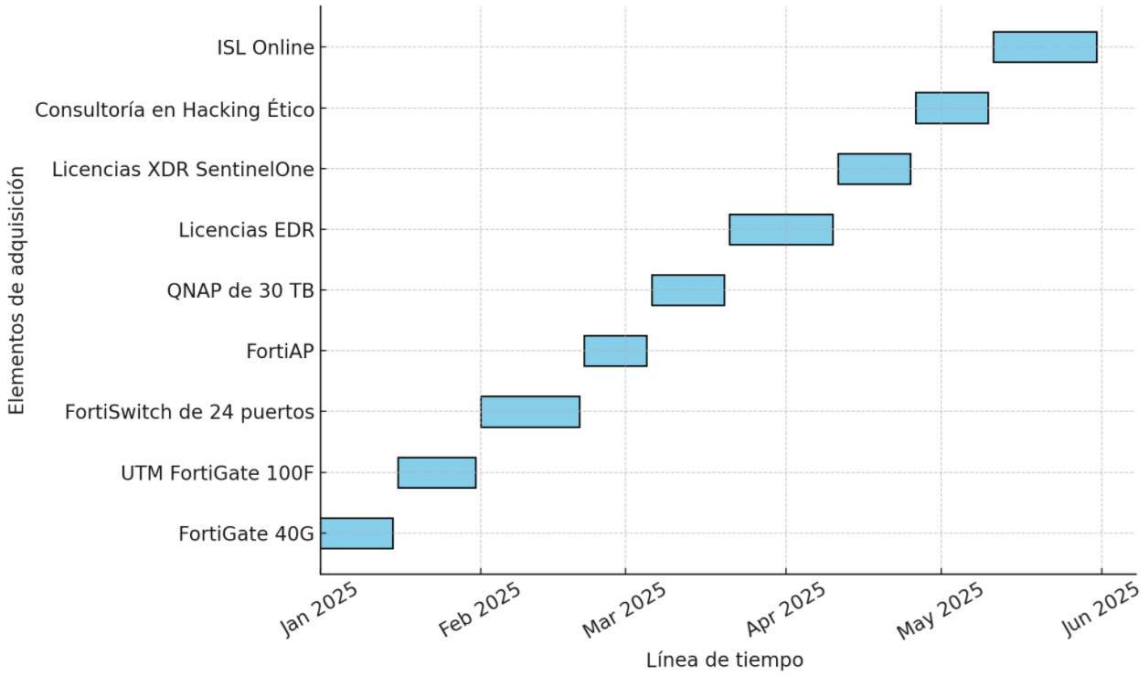
- Juicio de expertos: consultar a especialistas en adquisiciones y ciberseguridad.
- Análisis de mercado: evaluar proveedores potenciales y comparar opciones.
- Criterios de puntuación: asignar puntajes a las propuestas para facilitar la selección.
- Análisis de costo-beneficio: comparar costos frente al valor proporcionado.

Entregables del proceso:

- Plan de gestión de adquisiciones: documento que detalla estrategias, métodos y cronograma.
- Especificaciones de adquisiciones: requisitos técnicos y de selección para cada elemento.
- Criterios de evaluación: parámetros objetivos para seleccionar proveedores.
- Cronograma de adquisiciones: fechas clave para asegurar la sincronización con el proyecto.

El plan de adquisiciones garantiza que los bienes y servicios necesarios sean adquiridos de manera eficiente, cumpliendo con los estándares técnicos y financieros. Este enfoque estructurado facilita la integración de los elementos adquiridos con los procesos internos y asegura el éxito del proyecto de ciberseguridad en Lagobo Distribuciones S. A. S.

Figura 6. *Cronograma de adquisiciones*



11. REFERENCIAS

Abstracta. (2023). *Testing de seguridad en aplicaciones móviles: estándares OWASP*. Abstracta. https://es.abstracta.us/blog/testing-seguridad-aplicaciones-moviles-estandares-owasp/

Alberts, J. D. (2021). OCTAVE Allegro: a Lightweight Approach to Risk Assessment. *IEEE Security & Privacy Magazine, 19*(2), 38-46.

Apache Software Foundation. (s. f.). *Apache Log4j 2*. https://logging.apache.org/log4j/2.x/index.html

Arias, D. (16 de 09 de 2021). *Siguen incrementando los ciberataques en Colombia*. enter.co. https://www.enter.co/empresas/seguridad/siguen-incrementando-los-ciberataques-en-colombia/

AVG. (s. f.). *What is firmware? Definition and examples*. AVG Signal. https://www.avg.com/en/signal/firmware

Casino, F., Dasaklis, T. K., & Patsakis, C. (2019). A systematic literature review of blockchain-based applications: current status, classification and open issues. *Telematics and Informatics*, 36, 55-81. https://doi.org/10.1016/j.tele.2018.11.006

Chen, Y., & Li, S. (2020). Understanding Cyber Attacks in Social Engineering. *Journal of Information Security, 11*(3), 165-182. https://doi.org/10.4236/jis.2020.113009

Cialdini, R. B. (2007). *La psicología de la persuasión*. Paidós.

Cloudflare. (s. f.). *What is a bot?* Cloudflare. https://www.cloudflare.com/learning/bots/what-is-a-bot/

Cooper, A., & Powell, B. (2020). Apache Security Best Practices. *Journal of Web Technologies, 23*(4), 30-45.

CrowdStrike. (s. f.). *Windows NTLM*. https://www.crowdstrike.com/en-us/cybersecurity-101/identity-protection/windows-ntlm

Entrust. (s. f.). ¿Qué es TLS? *Entrust*. https://www.entrust.com/es/resources/learn/what-is-tls

European Central Bank. (s. f.). *TIBER-EU: The European framework for threat intelligence-based ethical red teaming*. https://www.ecb.europa.eu/paym/cyber-resilience/tiber-eu/html/index.en.html

Feldman, D. (2021). Understanding the Evolving Threat Landscape and the Role of Antivirus in Modern Cybersecurity. *Journal of Cybersecurity Research, 12*(1), 23-34. https://doi.org/10.1007/s41125-021-00123-5

Fortinet. (s. f. a). *Ataque de fuerza bruta (Brute Force Attack)*. https://www.fortinet.com/lat/resources/cyberglossary/brute-force-attack

Fortinet. (s. f. b). *¿Qué es XDR (Extended Detection and Response)?* https://www.fortinet.com/lat/resources/cyberglossary/what-is-XDR

Gandomi, A., & Haider, M. (2015). Beyond the hype: big data concepts, spywaremethods, and analytics. *International Journal of Information Management, 35*(2), 137-144. https://doi.org/10.1016/j.ijinfomgt.2014.10.007

Geeknetic. (s. f.). *¿Qué es el Kernel y para qué sirve?* Geeknetic. https://www.geeknetic.es/Kernel/que-es-y-para-que-sirve

GeeksforGeeks. (s. f.). *PHP Tutorial*. https://www.geeksforgeeks.org/php-tutorial/

GitLab. (s. f.). *¿Qué es la prueba de fuzz (fuzz testing)?* GitLab. https://about.gitlab.com/es/topics/devsecops/what-is-fuzz-testing/

Goodfellow, I., Bengio, Y., & Courville, A. (2016). *Deep Learning*. MIT Press.

IBM. (s. f. a). *CVE (Common Vulnerabilities and Exposures)*. https://www.ibm.com/mx-es/think/topics/cve

IBM. (s. f. b). *Kerberoasting*. https://www.ibm.com/think/topics/kerberoasting

IBM. (s. f. c). *Log4Shell*. https://www.ibm.com/es-es/topics/log4shell

IBM. (s. f. d). *Ransomware como servicio (RaaS)*. https://www.ibm.com/es-es/topics/ransomware-as-a-service

International Organization for Standardization (ISO) e International Electrotechnical Commission (IEC). (2013). Information technology — Security techniques — Information security management systems — Requirements. International Organization for Standardization.

International Organization for Standardization (ISO). (2013). ISO/IEC 27001:2013 Information security management systems — Requirements. Geneva, Switzerland: iSO.

Kaspersky. (s. f.). *What is a rootkit?* Kaspersky Resource Center. https://www.kaspersky.com/resource-center/definitions/what-is-rootkit

Kumar, S. (2024). *Algorithms: Big Data, Optimization Techniques, Cyber Security*. De Gruyter.

Lagobo Distribuciones. (2024). Nuestra compañía. https://www.oportunidades.com.co/quienes-somos

Lee, K., & Park, Y. (2018). Bluetooth vulnerabilities and their exploitation. *International Journal of Network Security, 15*(4), 253-265.

Leung, C. (2021). Introduction to Go (Golang) Programming. *Journal of Cloud Development, 15*(3), 29-37. https://doi.org/10.1016/j.jcldev.2021.03.008

LinuxMind. (2024). *Guía completa del SO Zeroshell: cómo funciona, orientación y curiosidades*. LinuxMind. https://linuxmind.dev/2024/05/15/guia-completa-del-so-zeroshell-como-funciona-orientacion-y-curiosidades/

Malwarebytes. (2021). *Braktooth: Bluetooth vulnerabilities crash all the devices*. Malwarebytes. https://www.malwarebytes.com/blog/news/2021/09/braktooth-bluetooth-vulnerabilities-crash-all-the-devices

Microsoft. (s. f.). *¿Qué es MDR (Detección y Respuesta Administrada)?* https://www.microsoft.com/es-es/security/business/security-101/what-is-mdr-managed-detection-response

MIT. (s. f.). *klist – Kerberos credential cache and keytab file utility*. https://web.mit.edu/kerberos/krb5-1.12/doc/user/user_commands/klist.html

NinjaOne. (s. f.). *¿Qué es un controlador de dominio?* https://www.ninjaone.com/es/it-hub/endpoint-management/que-es-un-controlador-de-dominio/

Ortega Candel, J. M. (2021). *Ciberseguridad. Manual práctico*. Ediciones Paraninfo.

Ortiz, J. E., & Semillero en Seguridad Informática Uqbar. (2021). *Backup, la salvación para restaurar sistemas hackeados*. Agencia de Noticias de la Universidad

Nacional de Colombia. https://agenciadenoticias.unal.edu.co/detalle/backup-la-salvacion-para-restaurar-sistemas-hackeados

Parrot Security. (s. f.). *Mimikatz*. GitHub. https://github.com/ParrotSec/mimikatz

Project Management Institute. (2021). *A Guide to the Project Management Body of Knowledge* (PMBOK Guide) (7th Ed.). Project Management Institute.

Quest. (s. f.). *What is KRBTGT and why should you change the password?* https://blog.quest.com/what-is-krbtgt-and-why-should-you-change-the-password

Red Hat. (s. f.). *¿Qué es una API (interfaz de programación de aplicaciones)?* Red Hat. https://www.redhat.com/es/topics/api/what-are-application-programming-interfaces

República de Colombia. (1995). *Ley 222. Por la cual se modifica el Libro II del Código de Comercio, se expide un nuevo régimen de procesos concursales y se dictan otras disposiciones*. Diario Oficial No. 42.156

República de Colombia. (2008). *Ley 1258. Por la cual se crea la sociedad por acciones simplificada*. Diario Oficial No. 47.194.

República de Colombia. (2012). *Ley 1581 de 2012. Por la cual se dictan disposiciones generales para la protección de datos personales*. Diario Oficial N.º 48.587.

Russell, S., & Norvig, P. (2021). *Artificial Intelligence: A Modern Approach* (4th Ed.). Pearson.

Sarker, I. H. (2021). Machine Learning: algorithms, Real-World Applications and Research Directions. *SN Computer Science, 2*(3), 160. https://doi.org/10.1007/s42979-021-00592-x

Selenium. (s. f.). *Selenium Grid Documentation*. https://www.selenium.dev/documentation/grid/

SentinelOne. (s. f.). *Active Directory DCSync Attacks*. https://www.sentinelone.com/blog/active-directory-dcsync-attacks

SentinelOne. (s. f.). *Babuk Ransomware*. https://www.sentinelone.com/anthology/babuk/

Tarlogic. (s. f. a). *Glosario de ciberseguridad*. https://www.tarlogic.com/es/glosario-ciberseguridad/

Tarlogic. (s. f. b). *Shimming*. https://www.tarlogic.com/es/glosario-ciberseguridad/shimming

Trend Micro. (s. f.). *Ransomware*. https://www.trendmicro.com/vinfo/us/security/definition/ransomware